PTO/SB/05 (07-06)
Approved for use through 01/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	CYBS5805CIP
First Inventor	Thierry Brunet de Courssou
Title	GAME TALK SERVICE BUS
Express Mail Label No.	via EFS

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

1. □ **Fee Transmittal Form** (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☑ **Applicant claims small entity status**.
See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages* 60]
Both the claims and abstract must start on a new page
(For information on the preferred arrangement, see MPEP 608.01(a))
4. ☑ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 23]
5. **Oath or Declaration** [*Total Sheets* ______]
a. □ Newly executed (original or copy)
b. □ A copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 18 completed)
i. □ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☑ **Application Data Sheet.** See 37 CFR 1.76
7. □ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
□ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
(if applicable, items a. – c. are required)
a. □ Computer Readable Form (CRF)
b. Specification Sequence Listing on:
i. □ CD-ROM or CD-R (2 copies); or
ii. □ Paper
c. □ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. □ **Assignment Papers** (cover sheet & document(s))
Name of Assignee________________________________
____
10. □ **37 CFR 3.73(b) Statement** *(when there is an assignee)* □ **Power of Attorney**
11. □ **English Translation Document** *(if applicable)*
12. ☑ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
☑ Copies of citations attached
13. □ **Preliminary Amendment**
14. □ **Return Receipt Postcard** (MPEP 503)
(*Should be specifically itemized)*
15. □ **Certified Copy of Priority Document(s)**
(if foreign priority is claimed)
16. □ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. □ Other:________________________________
____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

□ Continuation □ Divisional ☑ Continuation-in-part (CIP) of prior application No.: 10/120,635..............

Prior application information: *Examiner* Mark Alan SAGER *Art Unit:* 3714

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 22430 ***OR*** □ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/ alan young /	Date	2007-08-20
Name (Print/Type)	Alan W. YOUNG	Registration No. (Attorney/Agent)	37,970

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CYBS5805CIP
	Application Number	
Title of Invention	GAME TALK SERVICE BUS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

□ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1

Applicant Authority ● Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Thierry		Brunet de Courssou	

Residence Information (Select One) ● US Residency ○ Non US Residency ○ Active US Military Service

City	Henderson	**State/Province**	NV	**Country of Residence**	US
Citizenship under 37 CFR 1.41(b)	FR				

Mailing Address of Applicant:

Address 1	975 Seven Hills Dr., Apt. 1317		
Address 2			
City	Henderson	**State/Province**	NV
Postal Code	89052	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

**Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).**

□ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22430	
Email Address	alan@younglawfirm.com	Add Email Remove Email

Application Information:

Title of the Invention	GAME TALK SERVICE BUS		
Attorney Docket Number	CYBS5805CIP	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	23	**Suggested Figure for Publication (if any)**	21

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CYBS5805CIP
	Application Number	

Title of Invention	GAME TALK SERVICE BUS

Publication Information:	
□	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
□	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	○ US Patent Practitioner	○ US Representative (37 CFR 11.9)
Customer Number	22430		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	10120635	2002-04-10
Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10120635	non provisional of	60332593	2001-11-23

Additional Domestic Priority Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

			Remove
Application Number	Country[i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			● Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	CYBS5805CIP
	Application Number	
Title of Invention	GAME TALK SERVICE BUS	

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1

If the Assignee is an Organization check here. ☒

Organization Name	CYBERVIEW TECHNOLOGY, INC.		
Mailing Address Information:			
Address 1	Two Palo Alto Square, Suite 500		
Address 2			
City	Palo Alto	**State/Province**	CA
Country	US	Postal Code	94306-2122
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button.

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/ alan young /			Date (YYYY-MM-DD)	2007-08-20
First Name	Alan W.	Last Name	YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

GAME TALK SERVICE BUS

BACKGROUND OF THE INVENTION

Cross-Reference to Related Applications

[0001] This is a continuation-in part of application Serial No. 10/120,635, filed April 10, 2002, which claims the benefit under 35 U.S.C. §119(e) of provisional application Serial No. 60/332,593, filed November 23, 2001, both applications of which are hereby incorporated herein by reference in their entireties.

Field of the Invention

[0002] Embodiments of the present invention relate generally to the field of pay computer-controlled games and entertainment devices, including both games of skills and games of chance. More particularly, embodiments of the present invention relate the field of methods, systems and devices for the automated monitoring and control of a large number of clusters of such pay gaming and entertainment devices.

Description of the Related Art

[0003] Conventional pay entertainment and gaming systems, either of the cash or the cash-less type, are seriously limited due to the technical choices that are typically made to comply with regulatory requirements. Indeed, regulators are mainly concerned with fraud, cheating and stealing, as may occur when legitimate winners are deprived of their just winnings or when illegitimate users receive illegitimate winnings. Because of these security concerns, regulators are reluctant to approve licenses for state-of-the-art "open" multimedia and Internet technologies, opting instead for known but antiquated technology.

[0004] However, the security of such antiquated technology (i.e., technology developed prior to the present advanced multimedia and Internet age) is mostly illusory. Such conventional technologies are only perceived as being more stable and secure because their flaws are not widely publicized. Computer technology being extremely complex, there are always latent imperfections and flaws, which may be exploited by the ill intentioned. This is even truer with antiquated technology, as hacker-crackers have now access to considerable information on software weaknesses as well as sophisticated attack strategies and tools that they may apply to older software.

[0005] Legacy entertainment and gaming systems that are authorized for use in public places are usually aggregates of old technologies bundled together with some PC hardware featuring basic fault tolerance, basic data integrity and ad-hoc security means, together with some LAN networking functionality to enable some primitive centralized auditing. Although some advanced security means have been proposed (such as disclosed in, for example WO 01/41892) that promote off-line gaming security using smart cards, this approach in fact exposes the system to latent unidentified security threats that hacker-crackers or employees will likely eventually exploit. Off-line or semi-on-line systems are totally in the hands of very few people. In short, these systems operate essentially with little means for detecting under-the-radar fraud (to push the analogy farther, finer-grained and smarter radar means would be uneconomical for casino and gaming operators to implement).

[0006] In contrast, lottery and pari-mutual wager systems have evolved to modern fully on-line very-high-capacity mission-critical systems funneling billions of dollars annually while offering significantly greater security means than the security afforded by banks. Since these organizations have come on-line, lawsuits resulting from complaints, flaws and fraud, including internal fraud by employees, have virtually disappeared. However, although pay entertainment and gaming machines based on secure Internet web browser and cash-less payment technology are ideal centralized candidate solutions to equip casinos and like sites, these may rapidly kill the traditional gaming support industry.

[0007] The entertainment and gaming systems lag behind state-of-the-art multimedia PC, gaming console, wireless and interactive TV technologies; consequently these systems are ill prepared to attract the younger player generation accustomed to flashy and networked games.

SUMMARY OF THE INVENTION

[0008] It is therefore an object of this invention to provide an architecture that overcomes the technical lag, security limitations and lack of stability of the prior art. It is a further object of this invention to provide an architecture that overcomes rapid obsolescence of technology. It is yet another object of this invention to provide a flexible architecture that may more easily accommodate the variety of specific regulatory requirements encountered around the world. It is a still further object of this invention to provide specific function peripheral devices with means of secure identification and secure network communication.

[0009] An embodiment of the present invention is a distributed gaming system. The distributed gaming system may include a communication bus; at least one first node, each including a first computer coupled to the communication bus, and at least one second node, each including a second computer coupled to the communication bus. The at least one first node may further include at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:

- publish the at least one high-level function;
- provide the at least one high-level function upon receiving a request to consume the at least one high-level function;
- enable execution of the at least one high-level function upon receiving a request for execution;
- perform a call back upon receiving a request to consume or execute the at least one high-level function, and
- return a reply subsequent to receiving a request for execution of the at least one high-level function.

[0010] The at least one second node may include a second computer coupled to the communication bus, and at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively:

- subscribe to or consume the published or provided at least one high-level function;
- request that the at least one first node execute the at least one high-level function;
- accept the reply subsequent to receiving a reply from the at least one first node, and
- accept the call-back upon receiving a call-back from the at least one first node.

[0011] The first service oriented software may be configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call. The first service oriented software may be configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a HTTP request. The first service oriented software may be configured to enable execution of the at least one high-level function upon receiving a request for execution via a

HTTP request. The first service oriented software may be configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call. The first service oriented software may be configured to return a HTTP reply subsequent to receiving a HTTP request for execution of the at least one high-level function.

[0012] The service oriented protocol is the Service Oriented Architecture Protocol (SOAP), for example. The communication bus may include loosely coupled and/or tightly coupled nodes. The loosely coupled nodes may include nodes coupled via Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and/or satellite link, for example. The tightly coupled nodes may include nodes coupled via inter-process communication, USB, Bluetooth, RS-232, RS-422 and/or IEEE1394 Firewire, for example. The at least one high-level function may include a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and/or an outcome determination function, to name but a few of the possible high-level functions. The at least one first node may include a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and/or an automatic teller machine, for example.

[0013] The at least one second node may include, for example, a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and/or an automatic teller machine. The first and/or second service oriented protocol may include asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and/or UDDI, for example. Security over the communication bus may be provided by implementing the IPSec protocol, the VPN tunneling protocol and/or the SSL protocol, for example.

[0014] The at least one second node may include a gaming machine. The at least one second node may be included inside a gaming machine. The at least one first node may include a gaming machine. The at least one first node may be included inside a gaming machine. The at least one second node may include a gaming machine played by a player and may be configured to execute at least one function call during a game session. The at least one second node may be included inside a gaming machine played by a player and may be configured to execute at least one function call during a game session. The at least one first node may be configured for load balancing with another one of the at least one first node. The negotiating of service messages on the communication bus may include at least one of, for example, naming, discovery, message routing, publishing eventing, subscribing eventing, message transformations, workflows, and communication recovery from nodes powering-off then on again.

[0015] According to another embodiment thereof, the present invention is a distributed gaming system that may include a communication bus; a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.

[0016] The first gaming machine may be further configured to perform a call back upon receiving a request to consume or execute the at least one high-level function, and return a reply and wherein the second gaming machine is further configured to accept the reply subsequent to receiving the call-back from the first gaming machine. The distributed gaming system may further include a service-oriented device coupled to the communication bus, the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine, for example. The service oriented device may be configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function.

[0017] According to another embodiment thereof, the present invention is a method for distributed gaming over a communication bus. The method may include steps of, for example, providing a first gaming machine and coupling the first gaming machine to the communication bus; publishing, by the first gaming machine, a first high-level function over the communication bus; providing a node coupled to the communication bus; receiving, from the node, a request to subscribe to the published first high-level function; accepting the subscription request; initiating a gaming session on the first gaming machine, and responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus.

[0018] The receiving step may be carried out with the node including a second gaming machine. The receiving step may be carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and/or an automatic teller machine, for example. The high-level function may include at least one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and/or an outcome determination function. The method may further include a step of receiving, from the node, a request that the first gaming machine executes the high-level function. A step may be carried out of the first gaming machine performing a call back upon receiving the request to consume or execute the high-level function. The second providing step may be further carried out with the node being configured to selectively publish, subscribe, provide, execute and request that the first gaming machine execute the high level function.

[0019] According to yet another embodiment thereof, the present invention is a method for distributed gaming over a communication bus. The method may include providing a first node and coupling the first node to the communication bus; publishing, by the first node, a high-level function over the communication bus; providing a first gaming machine coupled to the communication bus; receiving, from the first gaming machine, a request to subscribe to the published high-level function; accepting the subscription request; initiating a gaming session on the first gaming machine, and responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus.

[0020] The receiving step may be carried out with the first node including a second gaming machine. The receiving step may be carried out with the node including an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device and/or an automatic teller machine, for example. The high-level function may include a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and/or an outcome determination function, for example. The method may further include a step of receiving, from the first gaming machine, a request that the node execute the first high-level function. A step may be carried out of the node performing a call back upon receiving the request to consume or execute the high-level function. The second providing step may be further carried out with the first gaming machine being configured to selectively publish, subscribe, provide, execute and request that the node execute the high level function.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Figure 1 is a diagram of a gaming system in accordance with an embodiment of the present invention.

[0022] Figure 2 is a diagram of an exemplary cash gaming machine in accordance with an embodiment of the present invention.

[0023] Figure 3 is a diagram of an exemplary cash-less gaming machine in accordance with an embodiment of the present invention.

[0024] Figure 4 is a diagram of an exemplary entertainment machine in accordance with an embodiment of the present invention.

[0025] Figure 5 is a diagram an exemplary PVU (Payment Verification Unit) in accordance with an embodiment of the present invention.

[0026] Figure 6 is a diagram of an exemplary compact PVU in accordance with an embodiment of the present invention.

[0027] Figure 7 is a diagram depicting an exemplary Automatic PVU (APVU) or “Smart Cashier” in accordance with an embodiment of the present invention.

[0028] Figure 8 is a diagram depicting a tightly coupled configuration of a gaming machine in accordance with an embodiment of the present invention.

[0029] Figure 9 is a diagram depicting a modular software architecture of a gaming machine in accordance with an embodiment of the present invention.

[0030] Figure 10 is a diagram depicting a loosely coupled software configuration of a gaming machine in accordance with an embodiment of the present invention.

[0031] Figure 11 is a diagram depicting a virtual configuration of the software architecture of a gaming machine in accordance with an embodiment of the present invention.

[0032] Figure 12 is a diagram depicting an extended virtual configuration of the software architecture of a gaming machine in accordance with an embodiment of the present invention.

[0033] Figure 13 is a diagram depicting a number of Internet-ready, specialized devices coupled to an APVU, according to an embodiment of the present invention.

[0034] Figure 14 is a diagram depicting partial processing by central server(s) 112 in accordance with an embodiment of the present invention.

[0035] Figure 15 is a diagram depicting a central server system, according to an embodiment of the present invention.

[0036] Figure 16 is a diagram depicting processing of gaming machine functions by PCs within a central server system, in accordance with an embodiment of the present invention.

[0037] Figure 17 is a diagram depicting each remote gaming machine connected to an individual PC or computer server located within a central server system 112, in accordance with an embodiment of the present invention.

[0038] Figure 18 is a diagram depicting a central server system that includes a server farm for performing operating system and applications boot to the individual PCs of a central server from a central storage facility, in accordance with an embodiment of the present invention.

[0039] Figure 19 is a diagram depicting a simplified Plug and Play protocol, in accordance with an embodiment of the present invention.

[0040] Figure 20 is a diagram depicting asynchronous notification of events, in accordance with an embodiment of the present invention.

[0041] Figure 21 illustrates a view of the service based gaming system according to an embodiment of the present invention, including a plurality of nodes arranged such as to offer one service publisher and multiple service subscribers.

[0042] Figure 22 illustrates a view of the service based gaming system according to an embodiment of the present invention, including a plurality of nodes arranged such as to offer multiple service publishers and one service subscriber.

[0043] Figure 23 illustrates a view of the service based gaming system according to an embodiment of the present invention, including a plurality of nodes arranged such as to offer multiple service publishers and multiple service subscribers.

[0044] Figure 24 illustrates a view of the service based gaming system according to an embodiment of the present invention, including a plurality of nodes, wherein each node is arranged such as to offer a one service publisher, multiple service publishers, one service subscriber and/or multiple service subscribers.

[0045] Figure 25 illustrates a view of the service based gaming system according to an embodiment of the present invention, including a plurality of nodes, wherein each node is arranged such as to offer one service publisher, multiple service publishers, one service subscriber and/or multiple service subscribers and wherein the communication network is pictured as a service bus that may include loosely coupled and/or tightly coupled nodes.

DETAILED DESCRIPTION OF THE INVENTION

[0046] Reference will now be made in detail to the construction and operation of preferred implementations of the present invention illustrated in the accompanying drawings. The following description of the preferred implementations of the present invention is only exemplary of the invention. Embodiments of the present invention are not limited to these implementations, but may be realized by other implementations.

[0047] Figure 1 illustrates a gaming system 100 according to an embodiment of the present invention. The system 100 may include a plurality of gaming machines 200, 300; one or a plurality of gaming machines clusters 106 located in the same site or in geographically dispersed locations; a plurality of Payment Verification Units 500 (hereafter, "PVU"), at least one such PVU 500 being associated with each gaming machines cluster 106, and one or more central server(s) 112. Instead of or in addition to the PVU 500, a compact PVU 600 (Figure 6) and/or an automated PVU or APVU 700 may be associated with individual gaming machines 200, 300 and/or cluster(s) 106. The clustering of gaming machines may be carried out according to geographical location, type of gaming machine, regulatory requirements, type of application and/or any criteria for grouping the gaming machines in a physical or logical cluster 106. The gaming machines 200, 300, PVUs 500, 600 or 700 and central server(s) 112 are networked together within a wide area network 102 (which may include, for example, the Internet).

[0048] The gaming system 100 may further include one or a plurality of entertainment machines. Alternatively, the entertainment machines 400 may be substituted for all or some of the gaming machines 200, 300. Within the context of the present inventions, gaming machines 200, 300 include machines that enable the player to plays games of chance while entertainment machines 400 include machines that enable the player to play games of skill, to watch entertainment materials or to even participate in interactive entertainment sessions with groups of players or other individual players. Monetary payouts from games of skills and entertainment machines 400 are usually illegal and prizes may commonly be awarded in the form of longer play sessions or ranking into a higher skill level.

[0049] Central server(s) 112 may be located on the same premises as the gaming machines 200, 300, entertainment machines 400 and PVUs 500, 600, 700 or elsewhere. A plurality of servers 112 may be used in various configurations. For example, the server(s) 112 may be located on same premises for fault tolerance backup, located on different premises for disaster tolerance backup, located on same or different premises for load balancing and/or configured in a hierarchical structure, whereby a hierarchically-higher server 112 provides consolidated services for one or a plurality of hierarchically-lower servers 112.

[0050] Figure 2 illustrates a gaming and identification verification machine 200 that accepts and redeems cash. It is to be understood that the gaming machine 200 is but one possible implementation of such gaming machines and that embodiments of the present invention are not limited thereto. Indeed, the system 100 may include any mix of any gaming and/or entertainment machines of most any kind. The gaming and identification verification machine 200 may include a display 202, a coin acceptor 204, a banknote acceptor 206, a coin hopper 210, a gaming machine identification (hereafter, "ID") device 212 and a plurality of user interaction means 208, which may include buttons, trackballs and/or joysticks, for example. The gaming machine ID device 212 is commonly used for identifying players that subscribe to a loyalty program to benefit from advantages and promotions offered by the gaming operator. Figure 3 illustrates an exemplary cash-less gaming machine 300 that does not accept or redeem cash. It is to be understood that the gaming machine 300 is but one possible implementation of such a cashless gaming machine and embodiments of the present invention are not limited thereto. For cash-less operation, a gaming device ID device(s) 304, 306 is/are necessary. The gaming machine ID device 304, 306 may include a magnetic card reader, a SmartCard reader and writer, a barcode reader, a ticket printer, a biometric reader, a touch-screen, keyboard or keypad to enable players to enter a PIN (Personal Identification Number) and/or a "Pay" button. The gaming machine identification device 304, 306 may further include an ID token reader to read other forms of advanced ID devices such as ID buttons, ID key-chains (such as disclosed, for example in commonly assigned US design patent entitled "Personal Communicator and Secure ID Device" patent number D441,765 issued on May 8, 2001) as well as secure communication means for securely communicating with, for example, personal wallets, hand held PCs or computer wrist-watch via infra red, magnetic field, capacitive charges or RF (Bluetooth, IEEE 802.11, etc.) for player identification purposes. According to one embodiment of the present invention, a player initially establishes a player account with the central server(s) 112 and receives a player ID card or ID token bearing the player's account number and other relevant information. Alternatively, gaming machine 200, 300, may include a printer 314 (Figure 3) to provide the player with a printed ticket 312 including a human and/or a machine-readable ID code. Alternatively, the printed ticket 312 may be provided by the PVU 500, 600 or 700 and read by the gaming machine 200, 300 via a ticket reader 316. Alternatively still, the player may register a biometric feature such as fingerprint, voiceprint and/or face print, and a PIN to be entered whenever confirmation of identity is required. All of these ID devices may allow the player to remain anonymous; in that case, the player's personal information is not requested and the assigned or chosen ID is associated with a numbered account instead of a personal account. Wager debits and prize credits are controlled by the central server(s) 112. Players may redeem any account balance by pressing the "Pay Button" (which may halt the current gaming session) and by claiming the funds from a cashier that is connected with the central server(s) 112. A machine coded (e.g., bar coded) printed ticket 312 may be generated by the gaming machine 200, 300 as additional means for claiming the funds or to begin a new game session on another gaming machine 200, 300 by causing the ticket reader 316 of the other gaming machine 200, 300 to scan the machine code on the printed ticket 312.

[0051] Electronic purses such as those based on the SmartCard technologies may also be used, either in on-line or off-line modes, although off-line operation is to be avoided to preclude latent and under-the-radar fraud, especially from inside employees.

[0052] Figure 4 illustrates a cash-less entertainment machine 400 including the following identification and payment means: a magnetic card reader or a SmartCard reader/writer 404, a ticket printer 412 for printing a ticket 410, a touch-screen 402 (and/or a keyboard or keypad) to enter a Personal Identification Number "PIN" and one or more buttons 406, 408, at least one of which may be a “Pay” button. It is to be understood that the gaming machine 400 shown in Figure 4 is but one possible implementation of such an entertainment machine and that embodiments of the present invention are not limited thereto. The entertainment gaming machine 400 may further include a biometric reader such as voice recognition (for example), to enable media-less identification means. The entertainment machine 400 may be configured for cash-less and/or for cash payment. Such entertainment machines 400 may have more than one screen, may allow for 3D, 360-degree vision and/or immersive vision, may include advanced interactive controls, force feed-back, motion feed-back, motion control, immersive sound and/or any technology that enhances the player's entertainment sensory experiences.

[0053] Moreover, the entertainment machines 400 and/or gaming machines 200, 300 may further include a video camera to allow for face-to-face action, face ID recognition, creation of avatars (movable three-dimensional images that may be used to represent a person or part thereof - such as a head - in cyberspace) and the like. Incorporating functionality for identifying players based upon recognition of their facial features in the entertainment machines 400 and/or the gaming machines 200, 300 would allow any pre-registered person to be immediately greeted and his or her account retrieved as soon as he or she stands by the entertainment machine 400 and/or the gaming machine 200, 300. Alternatively still, entertainment machines 400 may enable the player to participate in a game of chance while offering the player a superb multimedia and sensorial experience.

[0054] Because of the technical similarities and potential functional overlap between gaming machines 200, 300 and entertainment machines 400, the term “gaming machine”, as used herein below will collectively refer to both gaming machines 200, 300 and entertainment machines 400 and/or any variant or combinations thereof.

[0055] Figure 5 illustrates a payment verification unit or PVU 500, according to an embodiment of the present invention. The PVU may include a computer 502 connected to the network 102 with the gaming machines and/or the central server(s) 112 and a ticket printer 504. The ticket printer 504 may include an integrated printer for printing tickets or receipts 506 that include a human and/or machine readable code imprinted thereon and code reader 508 for reading the code(s) imprinted on the ticket 506. The PVU 500 may also include, for example, a magnetic card reader 510, a SmartCard reader 512, a biometric reader 514 (such as a fingerprint reader, for example), a display 520 and input devices such as a keyboard 518 and/or a mouse 516.

[0056] When a player wishes to redeem the credit available in his or her account, the player may consult a nearby cashier equipped with a PVU 500 who may identify the player's account using one of the ID media provided by the player, query the central server(s) 112 for payment authorization, and proceed with payment. When processing the payment authorization, smart pattern analysis software may be used to detect possible fraud resulting from counterfeiting whereby (for example) the player would deposit some cash funds for credit to his or her account, play very small wager amounts then claim the totality of the balance at another cashier. In that case, there is a high probability that the coins or notes remitted by the player may be counterfeits or originate from suspicious origin. The PVU 500 may also be used for crediting the player's account when the player remits cash to play on one of the cash-less gaming machines.

[0057] Figure 6 illustrates a compact version of the PVU 500, according to another embodiment of the present invention. The PVU 600 may include an enclosure 602, a data display 616 (which may include a touch screen), a magnetic card 606, a smart card reader 608, a printed ticket exit 612 through which a printer (internally mounted, not shown) dispenses printed tickets or receipts, an optical reader 610 and/or a speaker 604, for example. The optical reader 610 may include a barcode reader or most any machine vision system. The printer and the optical reader 610 may draw, for example, from aspects of the printers and scanners disclosed in commonly assigned Patent No. 6,710,895, issued March 23, 2004, and/or Patent No. 6,732,920, issued May 11, 2004, both patents of which are hereby incorporated herein by reference in their entireties.

[0058] Figure 7 illustrates an embodiment of an automated PVU or APVU 700, which dispenses with the need for a human cashier. The APVU 700 may include an internal computer connected to the network 102 with the gaming machines and/or the central server(s) 112, a coin acceptor 722, a note acceptor 720, a coin dispenser/hopper 718, a SmartCard or magnetic card dispenser 704, a note dispenser 714, a ticket printer 710 for printing a ticket 712, a magnetic card reader 702, a SmartCard reader/writer 706, a barcode reader 708, display with touch-screen 726, a keypad 724, a video camera 728 and/or a UL 291 certified cash safe 716, for example. The UL 291 certified cash safe 716 prevents robbery of the cash stored inside the APVU 700. The APVU 700 may further include biometric ID readers, ID token readers to read other forms of advanced ID devices such as ID buttons, ID key-chains, etc. as well as secure communications means for communicating with personal wallets, hand held PCs or computer wrist-watch via infra red, magnetic field, capacitive charges or RF (Bluetooth, IEEE 802.11, etc.) for identification purposes.

[0059] When a player wishes to redeem the credit available in his or her account, the player may consult a nearby APVU 700 or “smart-cashier” who will identify the player's account using one of the ID media provided by the player, query the central server(s) 112 for payment authorization, then proceed with cash payment via the coin hopper 718 and note dispenser 714, for example. When processing the payment authorization, smart pattern analysis software may be used to detect possible fraud. The APVU 700 may also allow the player to credit directly his or her account by remitting cash via the note acceptor 720, the coin acceptor 722 or alternatively via Electronic Fund Transfer ("EFT") with his or her bank account, to play one of the gaming machines. Any of the ID media may be used to allow the player to play on any of the gaming machines connected to the network 102.

[0060] Figure 8 illustrates a typical tightly coupled configuration that may be used with the present gaming machines. The gaming machine main processing platform may be built on a PC or equivalent hardware platform 801 that communicates with the central server(s) 112 and the PVU 500, 600, 700 via a network link. In addition to the PC platform, operating system, low level software, power supply, the main enclosure and any physical intrusion security, a gaming machine according to an embodiment of the present invention may include payment and identification devices, high-level application software modules, network communication means for enabling the gaming machine to exchange data with external devices (such as the central server(s) 112 and the PVU 500, 600, 700). The present gaming machine may also include an internal true RNG 808 (Random Number Generator) or means for receiving random combinations via the network 102 from external devices.

[0061] A hardware RNG is extremely desirable in order to ensure maximum entropy of encryption of the secret keys such that the encrypted keys are formed of true random bits, thereby rendering a brute force attack thereon to its maximum theoretical level of difficulty. An embedded true RNG based on diode noise, for example, enables systematic use of the highest encryption strength for the encryption algorithms and key length allowed by government. Flaws in RNGs and badly chosen encryption keys are responsible for highly publicized cracked systems. Although 128-bit encryption such as RSA, 3DES, etc. requires a considerable theoretical computer power to crack, a badly chosen encryption key may result in the secret keys being cracked within hours. There is a need to provide the gaming machines and external sources of random numbers coupled to the present gaming machines with almost "Military Defense Class" security. Virtual private Networks (VPNs), Secure Socket layer (SSL) and other secure communication protocols that rely on locally generated encryption keys are solutions that are widely available today. The resilience of such encryption protocols to attack depend on the quality of the encryption keys or their maximum entropy, such as discussed in Schneider, Secrets and Lies: Digital Security in a Networked World, Wiley& Sons, Inc. © 2000, pages 102-106, which is incorporated herein by reference.

[0062] The present gaming machine may also include one or more player video displays 802 driven directly by a multimedia controller within the gaming machine or driven externally thereto, one or more non-video displays 804 such as status indicators, digital indicators, mechanical indicators, blinking lights illuminations and the like and one or more player interactive controls 806 such as a one-arm bandit handle, push-buttons, trackballs or a joystick. As shown, the payment and identification devices of the present gaming machines may include a coin acceptor 810, a coin dispenser or hopper 812, a bill or note acceptor 814, a bill dispenser 816, a smart card reader and writer 818, a smart card dispenser 820, a bar or other machine readable code reader 822, a ticket printer 824, a magnetic card reader 826, a biometric ID reader 828 and/or other devices, generically referenced at 830. The payment and identification devices may advantageously be coupled to the platform 801 via RS232/ RS485 or similar connections.

[0063] The payment and identification devices listed above are collectively referenced herein as "specialized devices" herein below and may not all be present in a given gaming machine configuration. For example, a gaming machine may only be configured for cash-less payment using voice ID; in that case, only a microphone and touch-screen (and/or display and keypad) need be present. Moreover, the list of specialized devices above is not limitative, as new specialized devices may become available such as interfaces with personal wallets, contact-less smart cards or ID tokens, for example. Any such specialized devices may readily be incorporated within the present gaming machines. It is to be noted that the purpose for listing a significant number of specialized devices is not to recommend equipping gaming machine with each listed specialized device, but rather to teach the benefits of designed-in modularity, as is discussed in detail herein below. Furthermore, the same architecture may be advantageously applied to the APVU 700 (Automated Payment Verification Unit or Smart-Cashier).

[0064] In legacy gaming machines, the connection between specialized devices and the processing hardware is rather ad-hoc, as a wide variety of interfaces are encountered such as RS232, RS422, Parallel, via dedicated add-on board, etc. More recent specialized devices are now capable of providing a Universal Serial Bus ("USB") interface. However, all of these devices require that special software (software device drivers) that understands the inner characteristics of the hardware be developed. Software device drivers are well known to be difficult to develop and to introduce computer instabilities and limitations, especially when there is a large number of devices that may give rise to resource sharing conflicts.

[0065] As shown in Figure 8, the high-level software application modules for a gaming machine according to an embodiment of the present invention may include an audit engine 832, an authentication engine 834, a business engine 836 and/or a video entertainment/game engine 838. The audit engine 832, as a passive observation layer, transparently intercepts all the important events and all regulatory critical parameters associated with the operation of the specialized devices such as cash/cash-out or submitted identification information, the serial numbers of all connected devices and generates a non-modifiable reference audit log 840 that may consulted by the central server(s) 112 or the PVU 500, 600, 700. In addition, the audit engine 832 compares all devices connected to the gaming machine with a map of authorized regulatory configurations and may alert responsible personnel and/or regulators whenever non-valid device configurations are encountered, such as may occur after replacing devices or relocation of the gaming machine. The audit engine 832 may include instantly accessible non-volatile data storage, which data storage may be locally or remotely located (accessible via network 102). This would allow resolving data coherence and correctness in case of power failure, interruption, virus infection and/or software crash so as not jeopardize the accuracy of the game record keeping. For example, the audit engine 832 allows resolving conflicts wherein a record indicates a win and a payout amount although a power interruption has prevented the full payout from occurring. Moreover, the audit engine 832 may keep very specific accounting data as required by a given jurisdiction to meet locally applicable gambling regulations. For example, the audit engine 832 may keep a log of each drawn random number combination for audit purposes.

[0066] The audit engine 832 may keep audit trails separately for all of the different forms of monetary value that may be accepted by modern gaming machines such as, for example, audit trails of all wagers found in the coin and currency cash boxes. In gaming machines equipped with coupon readers, audit trail of the currency box may contain bar coded coupons of varying amounts in addition to cash. In the case of cashless wagers (e.g., those placed from player charge accounts or using some form of electronic money), as there is no currency in either of the coin or currency cash boxes, the audit trail may include relevant information exchanged during the player identification process, retrieval of the balance held in the central server(s) 112, the wager debits and the prize credits, for example.

[0067] The authentication engine 834 may include functionality to consult a Certificate Authority (which may be located on a server on the network 102 or on a computer network connected thereto), certify the authenticity of the identification presented, authorize a given operation, ensure data integrity of data exchanged, securely time-stamp the operation (to ensure non-repudiation of the operation) and/or revoke illegal identifications, for example.

[0068] The business engine 836 handles the games rules and the associated bookkeeping and may be subject to regulatory requirements. The business engine 836 handles the business aspects of the game and/or entertainment provided, controls wagers and maintains the prize matrix. This software application module customarily requires extensive testing by an independent laboratory to receive the certification mandated by local regulatory requirements. The regulatory requirements essentially insure that funds are reliably disbursed to legitimate players and insure that funds are not acquired by other individuals because of flaws, cheating and/or stealing.

[0069] The business engine 836 may include a transaction engine 842 for online operation with the central server(s) 112. In the case of game of chance, the video / entertainment / gaming engine 844 receives the current draw from one or more random number generators 808 located inside the gaming machine or outside the gaming machine (see reference numbers 902 and 904 in Figure 8), in accordance with local regulatory requirements. In case of games of skills, the gaming engine 844 receives the bonus from the business engine 836 in accordance with a given skill strategy, which may also require certification by a regulatory body and compliance with local regulatory requirements. An example of skill strategy may be rapidity, precision, ability to reach a given score, intelligence, memory, ability to focus on critical events amongst less critical events, etc. The business engine 836 may have received the applicable regulatory certification as illustrated by the star-shaped stamp 846.

[0070] The video / entertainment / game engine 844 communicates with the business engine 836 to translate the business rules into an attractive interactive experience for the player. Indeed, the video / entertainment / game engine 844 handles the player user interface, the multimedia interactive and entertainment and game graphics, sound, motion feedback and video streaming. The video / entertainment / game engine 844 may include a library 838 that offers a variety of entertainment multimedia, game multimedia and video streaming to suit the player's taste and expectations, as well as to accommodate a given strategy formulated by the game operator. For example, the engine 844 and library 838 may implement the methods and systems disclosed in commonly assigned Patent No. 6,921,331, issued July 26, 2005, which patent is hereby incorporated herein by reference in its entirety.

[0071] The central server(s) 112 provides on-line control of the gaming machines, the PVU 500, 600 and APVUs 700. An advantageous embodiment of the present invention is for the central server(s) 112 to instantly capture all the critical events occurring within the entire gaming system 100, including for example when each coin is inserted in the coin acceptor 810, noting its value as well as each coin rejection event. Further operation of the gaming machine may be prevented upon failure of the network 102. This principle is the basis of operation of large lottery systems, whereby thousands of terminals are deployed in remote areas. Such a model has proven to be extremely successful at avoiding fraud, including fraud committed by employees having access to sensitive data such as program source code. Performance is not an issue, as central server(s) 112s may use a farm of Intel Pentium® (for example) –based servers and a transactional protocol such as described in commonly assigned application Serial No. 09/862,165, filed May 21, 2001, which application is hereby incorporated herein by reference in its entirety, may handle tens of thousands of transactions per second with a guaranteed latency for each individual transaction no greater than 200 milliseconds.

[0072] Figure 9 illustrates a modular configuration that may be applied to a gaming machine according to an embodiment of the present invention, in which the gaming machine includes the same elements as described above but arranged in a modular fashion with their software Application Programming Interfaces or APIs clearly identified. Moreover, Secure APIs or S-APIs are also employed when data and programming security are essential. As represented in Figure 9, the constituent elements of the present gaming machines communicate with one-another only via their associated APIs or S-APIs.

[0073] It is to be noted that APIs not only define the exchange of information between the adjacent modules but also define how one module may provide services that may be consumed by the other. In this manner, one module may be made to control another module.

[0074] The specialized devices may be configured to possess the necessary embedded processing resources to control the entire operation of the device and to communicate with high-level application software via a clearly defined API or S-API. In Figure 9, the capability to control the hardware is represented by the elements named "Driver"; consequently, the low level details necessary to operate the specialized device are not made available to the high-level software module. According to embodiments of the present invention, the device drivers may form part of the embedded software of the specialized devices or may form part of the software of the platform 801 (such as a PC or other computing platform), so as to offer an API to the audit engine 832. Each specialized device may also be configured to supply its identity to the central server(s) 112; this is represented by the element named "ESN", which is an acronym for Electronic Serial Number. It is advisable to rely on secure means of authentication that may cooperate with the authentication engine 834 to ensure that the ESN is not associated with an illegal specialized device. Embodiments of the specialized devices may include secure ESN (secure serial numbers) that may be seeded with, e.g., a X509 certificate or a secret private key via a configuration step such as embedded smart card modules and TPM (Trusted Platform Module of the Trusted Computing Group). The authentication engine 834 may advantageously maintain a registry of authorized devices and may dispatch alerts to prevent illegal devices from operating. The player video displays 802, other player displays 804 and player interactive controls 806 are preferably modular devices capable of communication via a clearly defined API. Moreover, the audit engine 832 may read and record the serial numbers of each device connected to or coupled with the gaming machine.

[0075] According to embodiments of the present invention, some or all of the specialized devices may have their hardware aggregated such as to present only one coupling interface. For example, video displays 802, non-video displays 804, interactive controls 806 and card reader 818 may be aggregated into a single specialized device mounted in, on or coupled to the gaming machine. For example a player tracking device running Windows CE may be loosely coupled via the communication network to a high-level software module running in the central server, the high-level software module implementing a player tracking management function.

[0076] Figure 10 shows another configuration of a gaming machine according to another embodiment of the present invention, showing how components once having a clearly defined APIs may be controlled instead by components via a LAN (Local Area Network) and/or a WAN (Wide Area Network) 1002 via Remote Procedure Calls “RPCs.” A more modern control model is object-oriented, whereby a module may offer network services for consumption by other modules. Widely used standards for such object-oriented models include, for example, Distributed Common Object Module ("DCOM", developed by Microsoft Corporation) and Simple Object Access Protocol "SOAP", a vendor independent protocol based on eXtensible Markup Language ("XML").

[0077] SOAP forms the foundation layer of the Web services stack for providing a service oriented messaging framework, featuring a basic messaging framework that more abstract layers can build on. SOAP is a protocol for exchanging XML-based messages over computer networks using the HTTP/HTTPS stack, notably the following two methods: HTTP-request (or GET) and HTTP-response (or POST). There are several different types of messaging patterns in SOAP, but by far the most common is the RPC pattern, in which one network node (the client) sends to another node (the server) a request message for a service to be provided (the request may contain input parameters), and the server subsequently sends to the client a response message containing the return (which may contain output parameters) in accordance with the provided service. A node is a device that is connected as part of a computer network. For example, a node may be or include a computer, a personal digital assistant, a cell phone, a router, a switch, a hub, a server, a workstation, a handheld PC, gaming machine, specialized device or ATM.

[0078] SOAP is the successor of XML-RPC. SOAP originally stood for Simple Object Access Protocol, and lately also Service Oriented Architecture Protocol, but is now simply SOAP. The SOAP specification is currently maintained by the XML Protocol Working Group of the World Wide Web Consortium. SOAP is encapsulated in the Microsoft WCF – Windows Communication Foundation available in ".NET Framework 3.0" and later versions.

[0079] In a preferred embodiment, abstract layers may be build on SOAP for providing a service oriented architecture (SOA) such as a game service bus, whereby the game service bus provides a publish-and-subscribe message bus. A bus, according to embodiments of the present invention, is a service messaging engine based on, for example, standards such as SOAP, RPC, Microsoft Remoting, CORBA, RSS and/or Microsoft WCF (Windows Communication Foundation of .NET Framework 3.0).

[0080] The game service bus according to embodiments of the present invention provides high level applications and specialized devices with a uniform set of mechanisms for negotiating service messages on the communication bus such as naming, discovery, message routing, publish and subscribe eventing, message transformations, workflows, communication recovery from nodes powering-off then on again, and so on. The game service bus may be deployed within a casino property via private Intranet or across casino properties via public Internet (using secure communication means such as VPN, SSL or IPSec, for example). Microsoft "Biztalk Services" (www.biztalk.net) may advantageously be used to quickly deploy a service bus across properties. Biztalk Services is an Internet Service Bus, i.e. a fabric that interconnects distributed applications.

[0081] The service bus framework (or fabric) allows participating communicating end points (or nodes) to publish services or subscribe to services in a simple high level fashion, enabling the devices to understand one-another, thus to "talk" to one another. The "talking together" paradigm is rather appropriate as it emphasizes the value that the service bus brings to a complex distributed casino gaming system that may include thousands of devices manufactured by dozens of vendors.

[0082] According to an embodiment of the invention, a casino progressive Jackpot server may advantageously be built on the game service bus framework, whereby the progressive Jackpot is a service provider to gaming machines that subscribe to the services offered by the Jackpot service provider. The jackpot grows progressively as each spin/hand played on a connected gaming machine adds a small credit to the running jackpot total. Several casinos may join together to form an inter-casino progressive jackpot that can generate very large sums. In this example, a progressive Jackpot high level application service may be hosted on a server and published across the network. Each participating gaming machine may subscribe to the published progressive Jackpot service, may contribute to the jackpot at every spin/hand played and may claim the jackpot if the winning jackpot combination is drawn.

[0083] According to embodiments of the present invention, each gaming machine may publish its accounting meters via the game talk service bus and then authorized management servers, workstations, mobile handhelds and peer gaming machines may register to receive all or a subset of the accounting meters each time they are updated, at a predetermined interval or upon the occurrence of a predefined event, for example.

[0084] The ticket printer in each gaming machine may, according to further embodiments of the present invention, publish its printing services via the game talk service bus. Authorized management servers, workstations, mobile handhelds and/or peer gaming machines, for example, may then register to print a ticket. For instance, a promotional central server may print a free meal ticket for the player currently playing on the gaming machine he or she is currently playing on, either as a random bonus, or because the play profile of the player meets predetermined criteria for the awarding of such a meal ticket. Likewise, a floor manager carrying a wireless mobile handheld and observing a player may print on the player's gaming machine printer a free trial coupon for a new game that has just been released and that may suit the player's playing style, style as observed by the floor manager.

[0085] According to further embodiments of the present invention, a central logistic support server may subscribe to the printers' services (a printer being installed in each gaming machine) for a paper low or paper jam alert, and the technician closest to the gaming machine having the necessary repair skill or paper supply may receive instantly an SMS message on his location-finder equipped mobile phone to attend to the problem. The central logistic support server and the location-finder equipped mobile phones may be supplied by a third-party vendor specialized in automated geo-localized logistic support or geo-localized services for large factories, such as car manufacturing plans, airplane manufacturing plans, airports, harbor facilities, for example. The central casino management system may also subscribe independently to the printers' alerts for general accounting purposes.

[0086] Each gaming machine, according to still further embodiments, may publish player tracking services that (a) reads the player tracking card inserted in a card reader specialized device, (b) displays player tracking information on at least one of the player display (e.g. via a dedicated video display, via pop-up overlapping windows over a player video display, via a sliding overlapping windows over a player video display, via alpha-blended outlined data, icons or sprites over a player video display, or any other mechanisms to overlay information over a player video display), and (c)interacts with the player (e.g. via a touch-screen, a keypad, a pointing device, a joystick, biometric input). A central player tracking management system (that may advantageously leverage on intelligence data retrieved from the casino property hospitality network and servers) may subscribe to the player tracking services (offered on each gaming machine) in order for the central player tracking high level applications to interact directly with a player at the gaming machine.

[0087] According to an embodiment of the invention, client-side player tracking services may be offered by a specialized device including, for example, (a) an embedded computer controller running Windows CE, (b) a touch-screen video display, (c) a card reader (or any other means of player identification such as smartcard reader, PIN entry, pseudo+password entry, biometric identification, etc.), (d) a network interface for communicating over the game talk service bus and (e) controlling software to provide the client-side player tracking software services.

[0088] In a service oriented architecture such as SOAP, IBM SOA and a game service bus, the term publishing a service (or services) encompasses within its scope the functionality of providing a service (or services), and the term subscribing to a service (or services) encompasses within its scope the functionality of consuming or invoking a service (or services). The binding term is associated with the capability for allowing the publisher/provider to perform an asynchronous callback to the subscriber/consumer when a subscribed service (or services) is/are available (data update for example). The term publishing a service (or services) includes within its scope the functionality of exposing a service (or services).

[0089] In a service oriented architecture (based on SOAP, CORBA, IBM SOA and Web-services, for example), services may be discovered using service discovery protocols. Service discovery protocols are network protocols which allow automatic detection of devices and services offered by these devices on a computer network. There are many service discovery protocols including, for example, DNS Service Discovery (DNS-SD), Service Location Protocol (SLP), Simple Service Discovery Protocol (SSDP) as used in Universal Plug and Play (UPnP), Universal Description, Discovery and Integration (UDDI) for Webservices, Jini for Java objects, Bluetooth Service Discovery Protocol (SDP), WS-Discovery (Web Services Dynamic Discovery), Internet Storage Name Service (iSNS), Web Proxy Autodiscovery Protocol and Dynamic Host Configuration Protocol, to name but a representative few.

[0090] At least the high-level engines 832, 834, 836, and 844 may communicate with the central server(s) 112 and/or the PVU 500, 600, 700.

[0091] The RNG (random number generator) located within the gaming machine 808 preferably behaves in the same manner as a specialized device and, therefore, has the same networking, API and secure communication characteristics, requirements and behaviors. The gaming machines may selectively receive random numbers for the game draw from different sources 902 904 to accommodate the various regulatory requirements mandated by given states or given countries. As represented in Figs. 8 and 9, the sources for such random numbers may be internal to the gaming machine as shown at 808 (wherein the RNG is configured as a specialized device), may originate from a RNG generator 902 internal or coupled to the PVU 500, 600 or APVU 700 and/or from a RNG generator or generators 904 internal or coupled to the central server(s) 112. According to one embodiment of the present invention, a RNG generator may be provided for each gaming machine 200, 300, 400, each PVU 500, 600, 700 and for each central server 112. For example, a single or a plurality of RNG generators 904 coupled to the central server(s) 112 may provide random number combinations to a large number of geographically distributed gaming machines. Also, a single or multiple RNG generators 902 coupled to the PVU 500, 600 or APVU 700 may provide random number configurations for selected gaming machines at a single location, within a cluster 106 and/or to several clusters 106, as shown in Figure 1. This configuration offers a great degree of flexibility and allows the present gaming system to meet most any applicable regulatory requirement relating to the RNG generators.

[0092] It is to be noted that all the modern technologies for offering network services and consuming network services via wired or wireless networks have very high security protection using advanced security techniques such as authentication, encryption, Secure Sockets Layer ("SSL"), Public Key Infrastructure ("PKI"), Kerberos, True Random Number Generators (for generating secret keys with maximum entropy), hopping keys (constantly changing keys), 128-bit Wired Equivalent Privacy ("WEP") algorithm, etc. In addition, a Virtual Private Network ("VPN") tunnel may be used for secure inter-module communication. For example, a VPN tunnel may be established between the bill dispenser 816 specialized device and the central server(s) 112, or one or more software modules located on the central server(s) 112. A preferred embodiment of the present invention is to use the IPSec communication encryption standard that can be conveniently applied as a system wide policy.

[0093] Moreover, a “Network Access Point” component 1004 may be introduced that simply allows the APIs of the specialized devices to be directly supported and controlled over the network 102, 1002. These Network Access Points 1004 are sometimes called “IP Converters”. Examples of such network access points or IP converters include the USB to Ethernet converter from Inside Out Networks (www.IONetworks.com) and the RS232 to Ethernet from Moxa Technologies (www.moxa.com). Ideally, an Ethernet interface would be directly embedded on processing hardware that controls the specialized device.

[0094] An embodiment of the present invention includes the use of the IP protocol for intercommunication between each of the modules shown in Figure 9. Other existing or future protocols may also be used such as, for example, IPX from Novel; however, the IP protocol is universally used for the Internet and many communicating products and components support it. The payment and identification devices may be coupled to the Network Access Point or IP Converter 1004 by an RS232, RS485, USB, I2C, 802.11, Blue Tooth, Ethernet, Fire Wire or most any standardized interface.

[0095] An embodiment of the present invention includes automatic binding of specialized devices with the central server(s) 112 following their activation for example after power-on or reset. Figure 19 shows a simplified diagram wherein a specialized device coupled to the central server(s) 112 by network 102 sends, following its activation, broadcast packets over the network 102 indicating its availability. The broadcast packet may contain data identifying the specialized device and describing its location and capabilities. The server 112 that needs to communicate with this specialized device then enters into a binding protocol in order to establish bi-directional communication. A preferred embodiment for the automatic binding is the Universal Plug and Play standard proposal led by Microsoft, although other binding protocols may be used.

[0096] According to another embodiment of the present invention, the specialized devices may be configured to offer asynchronous notification of events directly to the central server(s) 112 over a communication network, such as shown at 102, for example. Figure 20 shows a simplified diagram wherein a specialized device, coupled to the central server(s) 112 by a network, sends asynchronous notifications packets to the central server(s) 112 following an event being received by the specialized device or an event generated by the specialized device. For asynchronous notification of events, the server(s) 112 may register (subscribe) with the specialized devices for the list of events that are of interest. Then, the event notification process running in the specialized device may produce a call back to the server(s) 112 (thus the name callback) in order to pass details on the event information when it occurs. A mechanism to un-register (unsubscribe) may be provided wherein the server(s) may inform the specialized device to stop sending asynchronous notification of events. A preferred embodiment of the asynchronous notification of events is the callback feature of COM+, DCOM, REMOTING technologies from Microsoft and the callback capability of SOAP, although other technologies may be implement within the context of embodiments of the present invention.

[0097] Figure 11 shows another embodiment of the present invention, in which the present gaming system is network-centric. In Figure 11, the network 1102 is the centerpiece thus allowing all the elements internal to as well as external to the gaming machine to interact with one another over the network 102. This wheel and spoke network topology brings great flexibility benefits, as detailed herein under, as it allows virtually any configuration to be chosen for assembling the present gaming machines. For example, the business engine 836 may be located within the gaming machine, within the PVU 500, 600, 700 or within the central server(s) 112. Likewise, the video/entertainment/games engine 844 may also be located within the gaming machine, within the PVU 500, 600, 700 or within the central server(s) 112. The same holds true for the audit engine 832. The video/entertainment/games engine 844 may support real time MPEG compression. For example, the broadband channel between the LAN/Wan 1102 and the video/entertainment/games engine 844 may accommodate video streams encoded using the MPEG4 compression standard (for example) at 100/1000Mbits/sec, enabling high quality graphics and video to be rendered on the player video displays 802 of the gaming machine(s).

[0098] Moreover, the technologies for offering and consuming services over a network such as network 1102 work equally well without any network; consequently the high-level software modules may remain unchanged whether or not a network exists inside the gaming machine for inter-module communication. Thus, the same high-level software modules may be used whether the gaming machine relies on a tightly coupled configuration as shown in Figure 8 or on a loosely coupled configuration as shown in Figs. 10 and 11.

[0099] The flexibility to configure a gaming machine in a variety of ways and avoid modifying high-level software modules (especially certified modules) is immensely valuable for a company that produces gaming machines to the global market, as regulatory requirements vary significantly from country to country and from state to state. Moreover, a manufacturer may more readily leverage on advanced integrated software development platforms such as Microsoft .NET to promote significant re-use of code across the product line, accelerate development time, improve code quality, facilitate code maintenance and upgrade and reduce development cost.

[0100] Figure 12 represents an extension of Figure 11, in which the specialized devices are directly capable of network communication using, for example, technology developed for smart IP peripherals, according to a still further embodiment of the present invention. Smart IP peripherals are commonly called Internet Appliances. According to an embodiment of the invention, the specialized devices may each be controlled by a processor capable of supporting an operating system such as Microsoft Windows CE, Microsoft Embedded XP or Embedded Linux; IP networking may be carried out via a wired or wireless link. With such advanced operating system, applications may be loaded from the network. Therefore, applications need not be stored locally within the specialized device, thereby avoiding software upgrade issues. Indeed, application software may be loaded into the gaming machines 200, 300, 400, any specialized device thereof from a remote server 112 and/or from a PVU 500, 600, 700. Similarly, application software may be loaded into the PVUs 500, 600, 700 and/or into any specialized devices therein from a remote server 112. Moreover, the entire operating system of the present gaming machine may be replaced over the network 1202. The operating system may be booted from the network 1202 using PXE (Preboot Execution Environment), for example.

[0101] Figure 13 represents the APVU 700 equipped with IP-Ready specialized devices. These specialized devices are preferably interchangeable with the IP-Ready specialized devices that equip the present gaming machine. Therefore, the APVU's specialized devices may interact directly with the central server(s) 112 via network services, thus benefiting of the same advantages as the gaming machine. As shown, the APVU 700 may incorporate hardware and corresponding software modules for a microphone 1302, a sound system 1304, a video camera 728, a display 1308, a keypad 1310, an alarm system 1312, a active security system 1314 for the internal safe, a power supply 1316 and an Uninterruptible Power Supply ("UPS"). Network Services, as referred to herein, relate to service-oriented architectures such as Microsoft DCOM, Common Object Request Broker Architecture (CORBA), Microsoft .NET and Sun Java 2 Platform, Enterprise Edition (J2EE), for example. Microsoft .NET and Sun J2EE are also commonly referred as “Web Services” and offer a universal solution over the Internet using XML, SOAP, Web Services Description Language (WSDL) and Universal Description, Discovery and Integration (UDDI) standardized technologies. UDDI nodes enables developers to publish web services and enables their software to search for and bind to services offered by others.

[0102] Network Services deliver loose coupling services between service requestors and service providers. Service requestors “consume” services provided by services providers. Publication of service descriptions play a central role to enable service requestors to discover available services and bind to them. The service descriptions allow service requestors to bind to the service provider. The service requestor obtains service descriptions through a variety of techniques, from the simple "e-mail me the service description" approach to techniques such as Microsoft DISCO and sophisticated service registries like UDDI.

[0103] Network services offer a network distributed objects/services infrastructure for transparent activations and accessing of remote objects/services. Objects are typically the EGD’s peripherals such as a note acceptor, and the services are the functions performed by the peripheral that are accessible externally via the IP network such as the value of the banknote entered. The central server is typically a service requestor. Peripherals are commonly service providers as well as service requestors (consuming services provided by the central server). In the same way, the central server is a services requestor and a services provider.

[0104] For embodiments of the present invention, Microsoft DCOM is a currently preferred technology, as DCOM support is already integrated into Microsoft Windows CE and Embedded XP, although embodiments of the present invention may be readily configured using other technologies, as those of skill in this art may appreciate. In the long term, Microsoft .NET web services over a private IP network (or VPN over Internet) may become the preferred technology, as it offers flexible and dynamic discovery of Net/Web services. The notion of a private or non-operator UDDI node is critical to the emergence of a dynamic style of a service-oriented architecture. As of this writing, Microsoft has announced support of .NET web services in Windows CE.NET.

[0105] Figure 14 illustrates a possible configuration that leverages on a virtual configuration architecture in which partial processing may be carried out at the central server(s) 112 (i.e., the gaming machines 200, 300, 400, the PVUs 500, 600, 700 may offload all or a part of their processing to the central servers 112. In this case, the audit engine, the authentication engine and the business engine software modules 832, 834, 836 may be located externally to the gaming machines, such as in the central server(s) 112, noting that the modules securely interact with one another precisely via their APIs, as defined in Figure 9. That is to say, the specialized devices located in the present gaming machine interact directly with the audit engine 832 located in the central server(s) 112 via network services. In the same manner, the video/entertainment/ games engine 844 located in the gaming machine interacts directly with the business engine 836 located in the central server(s) 112. The specialized devices and the video entertainment/games engine 844 located inside the gaming machine do not communicate or interact with one another.

[0106] The advantages of the configuration described above include significantly increased data integrity (fully on-line system, fault/disaster tolerant central server(s) 112), significantly strengthened fraud control (fully on-line system, centralized audit log, centralized code execution, quality code, centralized authentication), significantly increased stability (server class operating system, quality code, fault tolerant central server(s) 112), immediate code upgrade capability, accurate and instantly available audit (all the gaming machine critical events are instantly logged in the centralized audit log 840). Moreover, the hardware necessary to support the execution the video entertainment/games engine software module may be a very economical yet extremely multimedia capable game console such as Microsoft Xbox® or Sony PlayStation®, for example.

[0107] Figure 15 illustrates the trend in server hardware to increase the processing power per square foot of floor space. As shown, computer cabinets are available in multiples of the standardized "U" size and 42U high cabinets are commonly used for computer servers. 1U-size "pizza box like" servers are very popular with Internet service providers, which form factor allows 42 computer servers to be stacked on top of one another in a 42U size cabinet, as shown at 1502. Already, computer suppliers are packing twice and even 4-times this density, whereby 2 and 4 computer servers are integrated in a 1U rack, thus offering 84 and 168 computer servers 112 per 42U cabinet, as shown at reference numerals 1504 and 1506, respectively.

[0108] An alternative to the 1U pizza size form factor servers is the "blade" size factor whereby a complete server 112 may be integrated on a narrow board or blade. One presently proposed configuration allows 9 (reference numeral 1508) or 10 blade servers to be logged into a

3U size rack as shown on the right side of Figure 15. These racks may then be stacked, as shown at 1510. The complete server fits on a small board that may be very easily accessed for replacement or upgrade. Higher density dense servers are being developed that make use of very low power processing components such as fitted in laptops and hand held PCs, to help resolve the heat dissipation problem. It is to be noted that each of the servers discussed above may include a complete computer with CPU, memory, disk, network interface, and optionally full graphics. Large server farms that have on the order of 10,000 servers employ this type of dense server technology.

[0109] According to one embodiment of the present invention, each server shown in Figure 15 corresponds to a central server 112 and may be associated with and connected to a remotely located gaming machine. Preferably, each server 112 shown in Figure 15 is configured for multimedia graphics, generating 3D video and data streams encoded according to an MPEG standard, for example. In this manner, the central servers 112 may be constructed of an array of inexpensive servers, such as off the shelf PCs. Indeed, according to another embodiment of the present invention, the video stream shown to the player is generated (in MPEG4 format, for example) and streamed to the gaming machine over a broadband connection.

[0110] Figure 16 illustrates another embodiment of the present invention in which the execution of all the high-level software modules may be carried out at the central server(s) 112, including the video entertainment/game engine module 844. For this, a high-speed network 1602 is required to bring the video signal to the gaming machine, which may then be fitted with a simple video receiver. Each remote gaming machine may be connected to and associated with an individual server 112 within the central server system or farm of server 112. Other player displays and interactive control may also be controlled directly by the central server(s) 112 via network services.

[0111] Suitable means of transmitting such a video signal to the present gaming machine may include, for example, cable or wireless TV, HDTV or digital TV broadcast whereby each gaming machine is tuned to receive a separate predetermined frequency corresponding to the image to be displayed to the player, high quality video streaming such as MPEG2, MPEG4, or other emerging digital video standards via Fast Ethernet such as 100Mbps, 1000Mbps and upcoming higher bandwidth protocols, a fiber optic network, a wireless network such as IEEE 802.11b (11Mbps), 802.11a (54 & 72 Mbps @ 5 GHz), 802.11g (54 Mbps @ 2.4GHz) and upcoming higher bandwidth protocols. It is to be noted that the means of video transmission and reception listed above, whether based on TV technology or media streaming technology, are already fairly economical and it is believed that the associated costs will continue to decrease rapidly.

[0112] Figure 17 illustrates another embodiment of the present invention, in which a server (an individual PC, for example) located in a 42U Bay (for example) is associated with each gaming machine at the central server(s) 112. The server 112 associated with each gaming machine would then execute all or part of the software modules (audit engine 832, the authentication engine 834, the business engine 836 and the video entertainment/game engine 844) of the gaming machine. Interaction between the gaming machines and the central server(s) 112 is via network appropriate services as detailed above.

[0113] In particular, intensive video rendering to the player may be best if generated by an individual server at the central site and then the generated video signal may then be transmitted to the gaming machine. In this manner, there is considerable power to generate very advanced and attractive graphics for the player. Real-time translation to video streaming such as MPEG2 or MPEG4 may require hardware acceleration that may be carried out by a separate dedicated integrated circuit or alternatively may be directly integrated within the graphic processing unit of the server associated with the gaming machine.

[0114] Devices to receive high quality video information from the central server(s) 112, decode it and display it on a TV screen or a video display monitor are readily available. These devices use advanced electronic components developed for the latest generation Internet ready set top boxes and interactive TV systems. For example, such devices may be drawn from the devices and systems disclosed in commonly assigned application Serial No. 09/932,282, filed August 17, 2001, which application is hereby incorporated herein by reference in its entirety.

[0115] According to further embodiments of the present invention, each of the gaming machines may be configured to selectively offload computations to the farm of computer servers over the communication network. This may be done in a one-to-one manner whereby a computer server is entirely allocated to a given gaming machine, in a one-to-many manner whereby several computer servers are allocated to one gaming machine, or in a many-to-one manner whereby one computer server is allocated to several gaming machines.

[0116] Figure 18 shows another embodiment of the present invention in which the operating system and/or applications of each server 112 (collectively referenced by numeral 1806) may be booted from a central data storage such as a Storage Area Network (SAN) device 1804 coupled to the network 1802. This approach is commonly used for large server farms, as it enables each server 112 to obtain the same software image from a central repository (SAN 1804). Consequently, software upgrades are immediate. The PXE (Preboot Execution Environment) standard may be advantageously adopted to enable booting of the operating system within each of the server computers 112 via the network 1802. In this manner, each server 112 boots and loads the same software image from a centralized network accessible storage 1804.

[0117] The video rendering and distribution approach described above whereby the intensive graphics operations are performed at the central server(s) 112 has considerable benefits for the gaming machines, notably:

a. Low cost computer hardware (no CPU intensive graphics operation, no expensive graphics accelerator);

b. Stability and reliability as the gaming machine computer platform (hardware and software) are simple and do not need to be upgraded;

c. Future proofing (prevents obsolescence), as no software or hardware upgrades are required to accommodate extremely resource intensive multimedia advances such as future generations of advanced graphics animation, voice recognition, face recognition, avatar creation, etc. Moreover, selection of a given microprocessor architecture, operating system platform and supplier do not impact the future capabilities of the gaming machine, and

d. the video encoding, transmission, reception and decoding means may use low cost and mass-produced economical TV and streaming media components.

[0118] Moreover, this approach is ideally suited for offering wireless mobile gaming machines that players may take to the bar, the restaurant, the swimming pool, their hotel room, etc.

[0119] According to one embodiment of the present invention, Microsoft DCOM may be advantageously used; DCOM support is already integrated into Microsoft Windows CE and Embedded XP. In the long term, Microsoft .NET web services over a private IP network (or VPN over Internet) may become the preferred technology, as it offers flexible and dynamic discovery of Net/Web services. The notion of a private or non-operator UDDI node is critical to the emergence of a dynamic style of a service-oriented architecture. As of this writing, Microsoft has announced support of .NET web services in Windows CE.NET. These network technologies are encapsulated in the Microsoft WCF – Windows Communication Foundation available in ".NET Framework 3.0" and later versions.

[0120] Figure 21, 22, 23, 24 and 25 illustrate views of a service based gaming system in which SOAP is used, according to embodiments of the present invention. In the figures, a node may be or include a computer, personal digital assistant, cell phone, router, switch, hub, server, workstation, handheld PC, gaming machine, specialized device, an ATM or other device or process having the requisite processing functionality.

[0121] Figure 21 illustrates a view of the service based gaming system according to an embodiment of the present invention including a plurality of nodes 2104, 2106, 2108, 2110, 2112 and 2114 arranged such as to offer one service publisher 2128 and multiple service subscribers 2130, 2132, 2134, 2136 and 2138. The network 2102 is representative of a physical communication medium that may be loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, Bluetooth, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2116, 2118, 2120, 2122, 2124 and 2126 may be included in each node to allow the communication of services. The publisher 2128 may publish (or provide) services that one or a plurality of subscribers (or consumers) may consume, over the network 2102. The services provided by the publishing node 2104/2128 may be (a) high level functions such as from a business application server, a bonusing server, a customer loyalty server, a progressive jackpot server and a player tracking server, or (b) services from a specialized device, e.g. a network connected printer, a network connected bill acceptor, a player tracking combo (video display + touch-screen + card reader) and devices connected to a network bridge USB to Ethernet or RS232 to Ethernet. The services provided by the publishing node 2104/2128 may be consumed independently by multiple subscribing nodes 2106/2130, 2108/2132, 2110/2134, 2112/2136 and/or 2114/2138.

[0122] Figure 22 illustrates a view of a service based gaming system, according to an embodiment of the present invention. As shown, the service based gaming system may include a plurality of nodes 2204, 2206, 2208, 2210, 2212 and 2214 arranged such as to offer multiple service publishers 2228, 2230, 2232, 2234 and 2236 and one service subscriber 2238. The network 2202 is representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, Bluetooth, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2216, 2218, 2220, 2222, 2224 and 2226 may be included in each node to allow the communication of services. The services provided by the publishing node 2204/2228, 2206/2230, 2208/2232, 2210/2234 and/or 2212/2236 may be (a) high level functions such as from a business application server, a bonusing server, a customer loyalty server, a progressive jackpot server and a player tracking server, or (b) services from a specialized device, e.g. a network connected printer, a network connected bill acceptor, a player tracking combo (video display + touch-screen + card reader) and devices connected to a network bridge USB to Ethernet or RS232 to Ethernet. The services provided by the publishing nodes 2204/2228, 2206/2230, 2208/2232, 2210/2234 and 2212/2236 may be consumed independently by one subscribing node 2214/2238; for example, network connected printers installed in gaming machines may publish a range of services and a maintenance server may subscribe to, e.g., a paper jam alert and the paper low alert services such that the maintenance server may forward a job order to a technician on his or her mobile device.

[0123] Figure 23 illustrates a view of a service based gaming system according to another embodiment of the present invention that may include a plurality of nodes 2302, 2304, 2306, 2308, 2310, 2312, 2314, 2316 and 2318 arranged such as to offer multiple service publishers 2336, 2340, 2346 and 2350 and multiple service subscribers 2338, 2342, 2344 and 2348. As described relative to Figs. 21 and 22, the network 2302 may be representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, Bluetooth, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2320, 2322, 2324, 2326, 2328, 2330, 2332 and 2334 may be included in each node to allow the communication of services.

[0124] Figure 24 illustrates a view of a service based gaming system according to an embodiment of the present invention. As shown, the service based gaming system of Figure 24 may include a plurality of nodes 2404, 2406 and 2408, wherein each node is arranged such as to offer one or more of: one service publisher, multiple service publishers, one service subscriber and multiple service subscribers. The network 2402 is representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, Bluetooth, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2410, 2412 and 2414 may be included in each node to allow the communication of services. For example, node 2404 may include a central media server that may be configured to publish, for example, music content 2416, advertising video content 2418, promotional video content 2420 and a live TV feed 2422 to authorized participating nodes in the distributed gaming system. Node 2406 may include, for example, a billboard in a bar section wherein one network connected streaming plasma display 2424 may subscribe to the live video TV feed 2422 and the network connected ambience audio system may subscribe to the music content 2416. Node 2408 may include, for example, a gaming machine wherein an instance of a media player process 2430 may subscribe to the live video TV feed 2422 and another instance of a media player process 2432 may subscribe to the advertising video content 2418, and the video contents may be displayed simultaneously on the video gaming display or displays through a separate video window or 3D viewport. The gaming machine 2408 may publish 2428 its gaming meters using the GSA G2S protocol (Game Standard Association Game-to-System protocol), and any authorized node may subscribe to receive the gaming meters such as a casino management system (whose primary function is to satisfy regulatory accounting), a game download server, a security server, a marketing server, a player tracking server and/or a maintenance server, for example.

[0125] Figure 25 illustrates a view of the service based gaming system according to an embodiment of the present invention. As shown, the present service based gaming system may include a plurality of nodes, and each node may be arranged such as to offer one or more of the following: (a) one service publisher, (b) multiple service publishers, (c) one service subscriber and (d) multiple service subscribers. The communication network labeled "network bus" 2502 may include loosely coupled and tightly coupled nodes carrying network services via the SOAP stack. Node 2504 may include, for example, a USB printer specialized device located within an

ATM for publishing printing services in the ATM. Node 2508 may include, for example, a technician Wi-Fi handheld mobile device subscribing to alerts to repair jammed printers or bill acceptors. Node 2510 may include, for example, a billboard subscribing to a Keno server (not shown) that displays the published results of that Keno server.

[0126] In the illustrations of Figure 21, 22, 23 24 and 25, the service discovery is not shown but may include any service discovery protocol as discussed previously, such as UDDI and SSDP. UDDI (Universal Description, Discovery and Integration) is a platform-independent, XML-based registry for businesses worldwide to list themselves on the Internet. UDDI is an open industry initiative, enabling businesses to publish service listings and discover each other and define how the services or software applications interact over the Internet. UDDI may also be applied in an Intranet network. SSDP (Simple Service Discovery Protocol) is the basis of the discovery protocol of Universal plug-and-play. SSDP provides a mechanism through which network clients can use to discover network services. Clients can use SSDP with little or no static configuration. SSDP provides multicast discovery support, server-based notification, and discovery routing. SSDP uses XML UDP unicast and multicast packets to advertise their services.

[0127] Nodes may be added and removed to the network; new services will be discovered and bound automatically, and services that are no longer available will be detected and their associated binding will be terminated. Nodes may be provided by any supplier complying with the service bus protocol. In the figures, the SOAP stack is the network service, but as may be readily inferred by persons of skill in the distributed network architecture arts, any other network service stack offering similar capability may be used, including the associated service discovery scheme.

[0128] Embodiments of the present invention offer a modular architecture for an on-line gaming system that may readily accommodate the wide variety of regulatory requirements encountered around the world. The strongest open security standards may be used. The very complex software code is located in the high-level software modules that may advantageously be developed using an advanced unified integrated development environment (such as, for example, Microsoft .NET). The various elements may be arranged in a tightly coupled configuration, loosely coupled configuration or in a mixture of tightly and loosely coupled configuration without requiring the high-level software modules to be entirely redesigned, retested and re-certified. In most cases, the high-level software modules may be re-used without modification thus saving enormous cost and development, validation and testing time. A gaming system may be constructed using a wide variety of computer hardware and software platforms, and make use of the latest multimedia technologies to attract the younger generation of players used to flashy and networked games. IP-Ready specialized devices using Internet appliance technologies offer tremendous benefit as the gaming machines, entertainment machines and payment verification units become a simple shell; the devices may be fully managed by the central server(s) 112. An advantageous embodiment of the invention is one in which the processing of all the high-level software modules, including graphics rendering, is carried out by the central server(s) 112, which relies on a server-class operating system and fault tolerant computing platform. Consequently, embodiments of the present invention provide an architecture that overcomes the technical lag, security limitations and lack of stability of the prior art.

[0129] Rapidity changing technologies, such as advanced multimedia graphics and biometric recognition that require continual increase in processing power are, according embodiments of the present invention, processed at the central server(s) 112. The present gaming machine, according to one embodiment thereof, only requires means of receiving and displaying high quality video images and means for sending locally captured biometric data (such as voice or video image of player) to the central server(s) 12. Wireless mobile gaming machine may be readily constructed. The central server(s) 112 (constructed with advanced server blades in one embodiment of the present invention) may be readily upgraded at any time by plugging in new replacement blades. Moreover, it is likely that entire server blades will soon fit on a single integrated circuit. One or more servers 112, therefore, may fit on a single integrated circuit. The present gaming machines do not require costly upgrades to take advantage of such multimedia advances. Consequently, embodiments of the present invention provide an architecture that overcomes rapid obsolescence of technology. The devices, methods and systems disclosed herein provide a flexible architecture that enables international suppliers to readily accommodate the variety of specific regulatory requirements encountered around the world.

[0130] Embodiments of the present invention also offer a modular architecture for an on-line gaming system that may readily accommodate the wide variety of regulatory requirements encountered around the world. The strongest open security standards may be used. The very complex software code is located in the high-level software modules that may advantageously be developed using an advanced unified integrated development environment (such as, for example, Microsoft .NET). The various elements may be arranged in a tightly coupled configuration, loosely coupled configuration or in a mixture of tightly and loosely coupled configuration without requiring the high-level software modules to be entirely redesigned, retested and re-certified. Similarly, a subset of the specialized devices may have its hardware aggregated such as to present only one coupling interface. Embodiments of video displays 802, non-video displays 804, interactive controls 806 and card reader 818 may be aggregated into a single specialized device mounted in the gaming machine, for example a player tracking device running Windows CE that is loosely coupled via the communication network to a high-level software module running in the central server, the high-level software module implementing a central player tracking management function. In most cases, the high-level software modules may be re-used without modification, thereby affording significant saving in costs and development, validation and testing time. A gaming system may be constructed using a wide variety of computer hardware and software platforms, and make use of the latest multimedia technologies to attract the younger generation of players used to flashy and networked games. IP-Ready specialized devices using Internet appliance technologies offer tremendous benefit as the gaming machines, entertainment machines and payment verification units become a simple shell; as the devices may be fully managed by the central server(s) 112. An advantageous embodiment of the invention is one in which the processing of all the high-level software modules, including graphics rendering, is carried out by the central server(s) 112, which relies on a server-class operating system and fault tolerant computing platform. Consequently, embodiments of the present invention provide an architecture that overcomes the technical lag, security limitations and lack of stability of the conventional gaming systems.

WHAT IS CLAIMED IS:

1. A distributed gaming system, comprising:

a communication bus;

at least one first node, each including a first computer coupled to the communication bus;

at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:

publish the at least one high-level function;

provide the at least one high-level function upon receiving a request to consume the at least one high-level function;

enable execution of the at least one high-level function upon receiving a request for execution;

perform a call back upon receiving a request to consume or execute the at least one high-level function, and

return a reply subsequent to receiving a request for execution of the at least one high-level function;

at least one second node, each including a second computer coupled to the communication bus, and

at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively:

subscribe to or consume the published or provided at least one high-level function;

request that the at least one first node execute the at least one high-level function;

accept the reply subsequent to receiving a reply from the at least one first node, and

accept the call-back upon receiving a call-back from the at least one first node.

2. The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call.

3. The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a HTTP request.

4. The distributed gaming system of claim 1, wherein the first service oriented software is configured to enable execution of the at least one high-level function upon receiving a request for execution via a HTTP request.

5. The distributed gaming system of claim 1, wherein the first service oriented software is configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call.

6. The distributed gaming system of claim 1, wherein the first service oriented software is configured to return a HTTP reply subsequent to receiving a HTTP request for execution of the at least one high-level function.

7. The distributed gaming system of claim 1, wherein the service oriented protocol is the Service Oriented Architecture Protocol (SOAP).

8. The distributed gaming system of claim 1, wherein the communication bus includes loosely coupled and/or tightly coupled nodes.

9. The distributed gaming system of claim 8, wherein the loosely coupled nodes include nodes coupled via at least one of Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and satellite link.

10. The distributed gaming system of claim 8, wherein the tightly coupled nodes include nodes coupled via at least one of inter-process communication, USB, Bluetooth, RS-232, RS-422 and IEEE1394 Firewire.

11. The distributed gaming system of claim 1, wherein the at least one high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and an outcome determination function.

12. The distributed gaming system of claim 1, wherein the at least one first node includes one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine.

13. The distributed gaming system of claim 1, wherein the at least one second node includes at least one of a gaming machine, an entertainment machine, a payment verification unit, a

specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

14. The distributed gaming system of claim 1, wherein the first service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI.

15. The distributed gaming system of claim 1, wherein the second service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI.

16. The distributed gaming system of claim 1, wherein security over the communication bus is provided by implementation of at least one of the IPSec protocol, the VPN tunneling protocol and the SSL protocol.

17. The distributed gaming system of claim 1, wherein the at least one second node includes a gaming machine.

18. The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine.

19. The distributed gaming system of claim 1, wherein the at least one first node includes a gaming machine.

20. The distributed gaming system of claim 1, wherein the at least one first node is included inside a gaming machine.

21. The distributed gaming system of claim 1, wherein the at least one second node is a gaming machine played by a player and is configured to execute at least one function call during a game session.

22. The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine played by a player and is configured to execute at least one function call during a game session.

23. The distributed gaming system of claim 1, wherein the at least one first node is configured for load balancing with another one of the at least one first node.

24. The distributed gaming system of claim 1, wherein the negotiating of service messages on the communication bus include at least one of naming, discovery, message routing, publishing eventing, subscribing eventing, message transformations, workflows, and communication recovery from nodes powering-off then on again.

25. A distributed gaming system, comprising:

a communication bus;

a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and

a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.

26. The distributed gaming system of claim 25, wherein the first gaming machine is further configured to perform a call back upon receiving a request to consume or execute the at

least one high-level function, and return a reply and wherein the second gaming machine is further configured to accept the reply subsequent to receiving the call-back from the first gaming machine.

27. The distributed gaming system of claim 25, further including a service-oriented device coupled to the communication bus, the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine, the service oriented device being configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function.

28. A method for distributed gaming over a communication bus, comprising:

providing a first gaming machine and coupling the first gaming machine to the communication bus;

publishing, by the first gaming machine, a first high-level function over the communication bus;

providing a node coupled to the communication bus;

receiving, from the node, a request to subscribe to the published first high-level function;

accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus.

29. The method of claim 28, wherein the receiving step is carried out with the node including a second gaming machine.

30. The method of claim 28, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

31. The method of claim 28, wherein the high-level function includes at least one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

32. The method of claim 28, further comprising a step of receiving, from the node, a request that the first gaming machine executes the high-level function.

33. The method of claim 28, further comprising a step of the first gaming machine performing a call back upon receiving the request to consume or execute the high-level function.

34. The method of claim 28, wherein the second providing step is further carried out with the node being configured to selectively publish, subscribe, provide, execute and request that the first gaming machine execute the high level function.

35. A method for distributed gaming over a communication bus, comprising:

providing a first node and coupling the first node to the communication bus;

publishing, by the first node, a high-level function over the communication bus;

providing a first gaming machine coupled to the communication bus;

receiving, from the first gaming machine, a request to subscribe to the published high-level function;

accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus.

36. The method of claim 35, wherein the receiving step is carried out with the first node including a second gaming machine.

37. The method of claim 35, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

38. The method of claim 354, wherein the high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

39. The method of claim 35, further comprising a step of receiving, from the first gaming machine, a request that the node execute the first high-level function.

40. The method of claim 35, further comprising a step of the node performing a call back upon receiving the request to consume or execute the high-level function.

41. The method of claim 35, wherein the second providing step is further carried out with the first gaming machine being configured to selectively publish, subscribe, provide, execute and request that the node execute the high level function.

ABSTRACT

A service-oriented bus for distributed gaming systems allowing gaming machines, servers, workstations, mobile PCs, handheld devices and automatic telling machines to talk together over a network. The game service bus provides a publish-and-subscribe message bus over a private network within a gaming property and/or over the public Internet across several properties. The service bus framework allows participating communicating end points to publish services or subscribe to services in a simple and standardized high level fashion, thereby enabling the devices to understand one-another, thus “talk” together. The “talking together” paradigm is rather appropriate, as it emphasizes the value that the service bus brings to a complex distributed casino gaming system that may include thousands of devices manufactured by dozens of vendors. Gaming machines may talk together in a peer-fashion over the service bus, which is well suited for multiplayer gaming. The service-oriented bus allows third party ultra-specialized vendors to offer dazzling plug-in services directly on the casino floor, such as automated geo-localized logistic support and other geo-localized services.

\\Ylfserver\ylf\CLIENTS\JMG\CYBS\5805\CIP\5805CIP PA.docx

S1/23

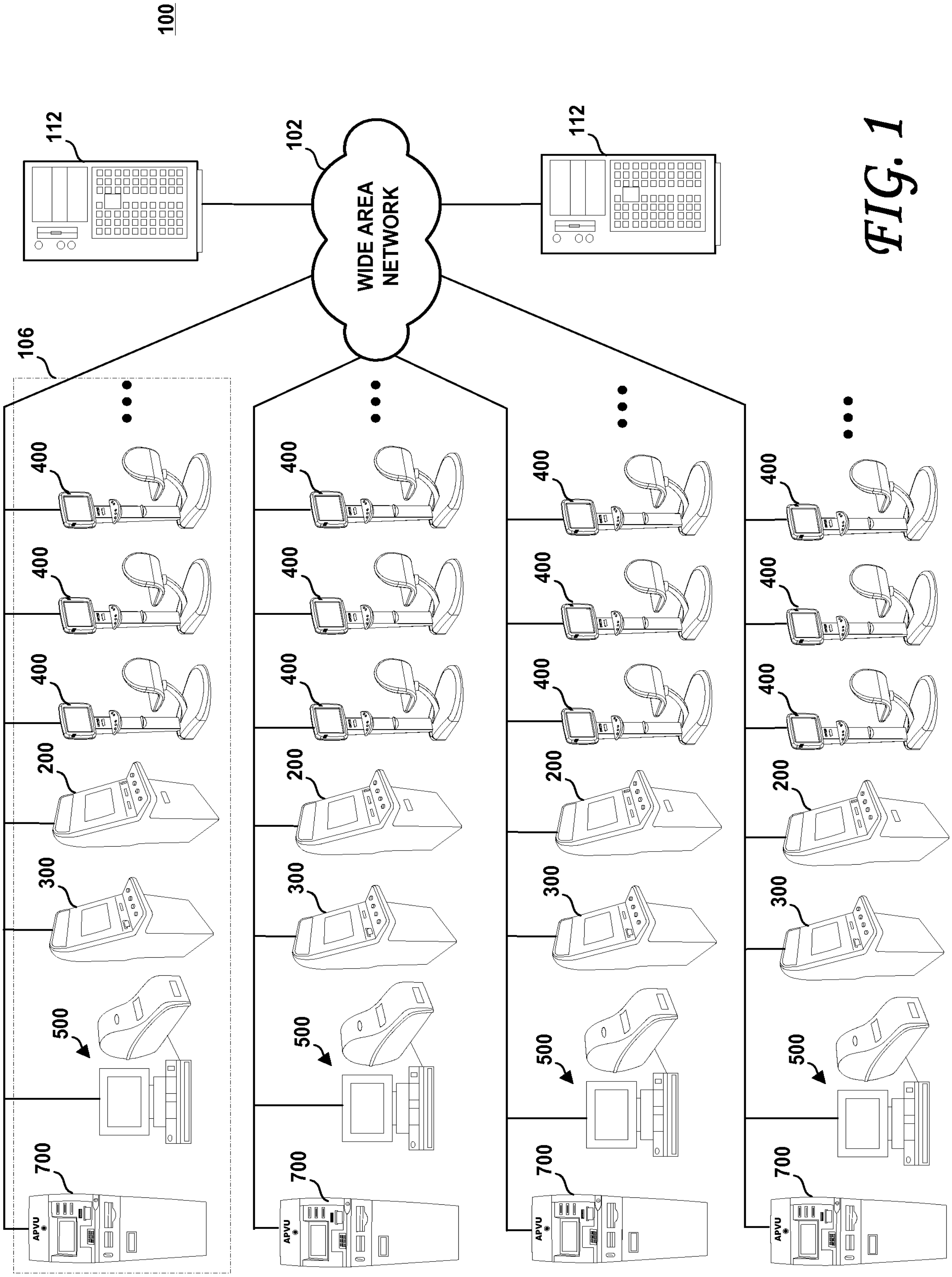

100
112
102
WIDE AREA NETWORK
112
106
400
400
400
200
300
500
700
APVU

FIG. 1

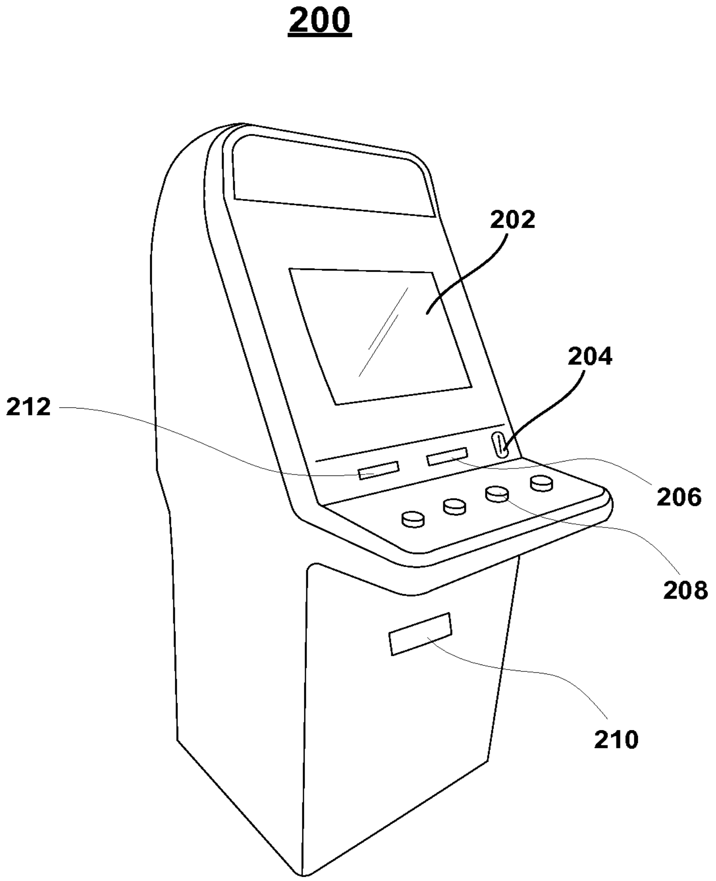


FIG. 2

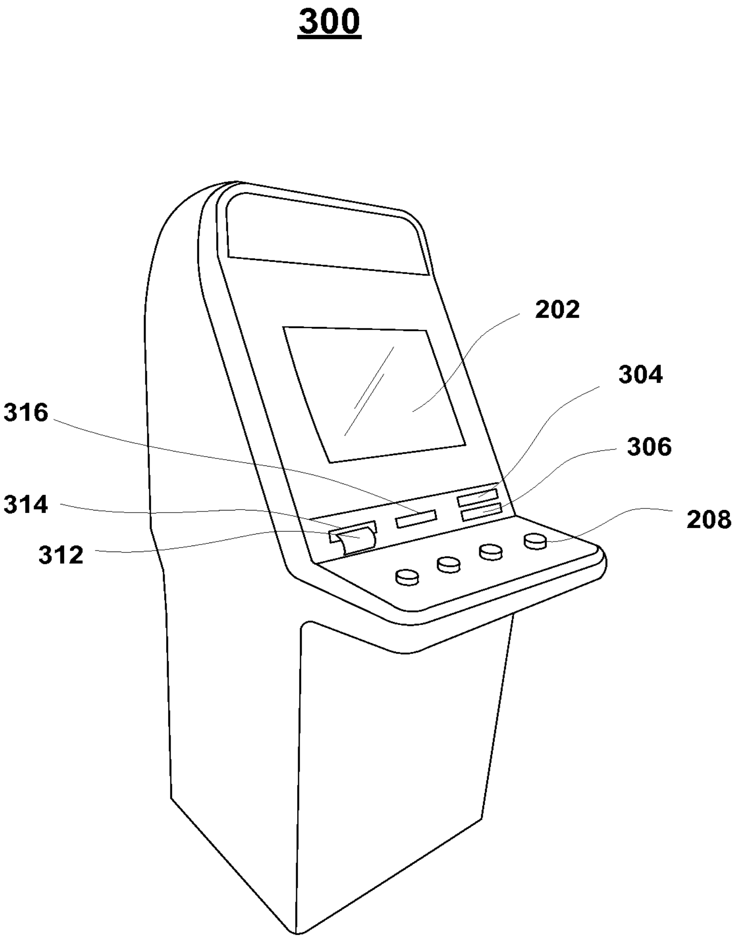


FIG. 3

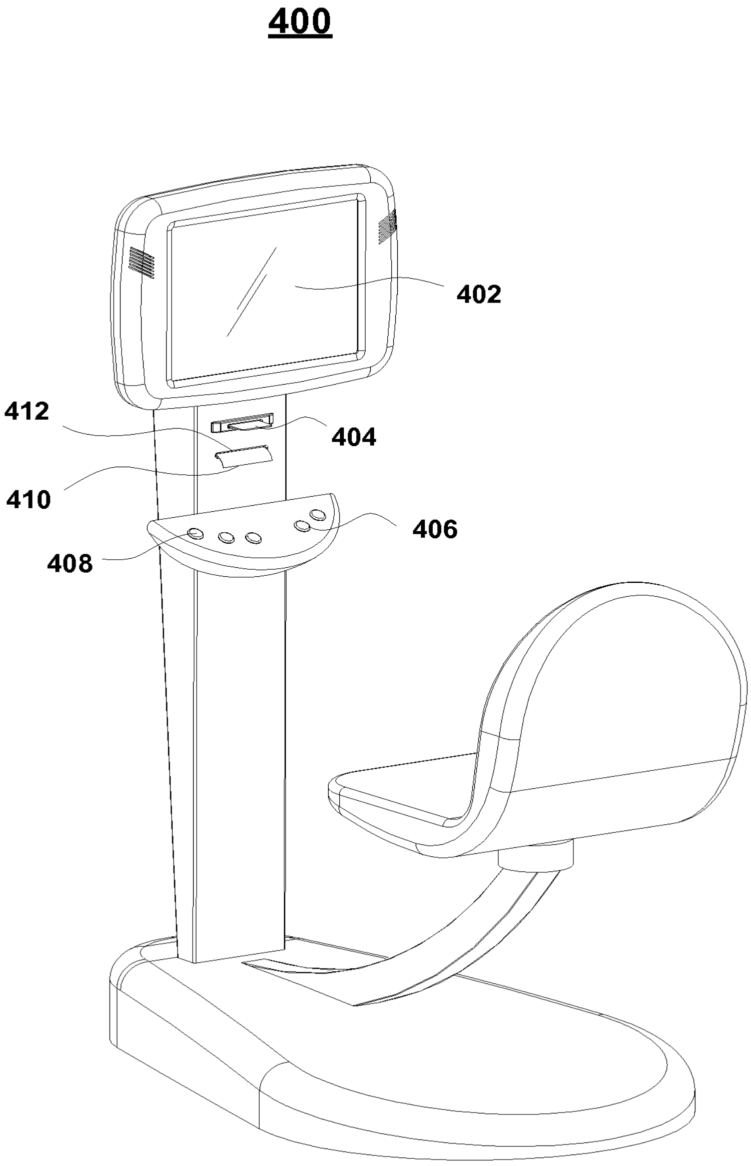


FIG. 4

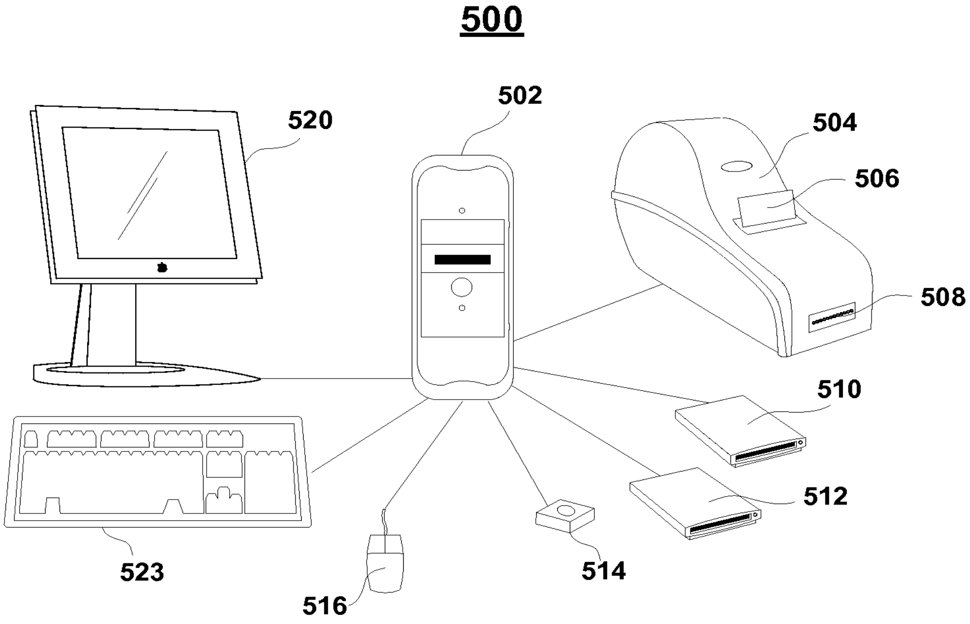

500
520
502
504
506
508
510
512
514
516
523

FIG. 5

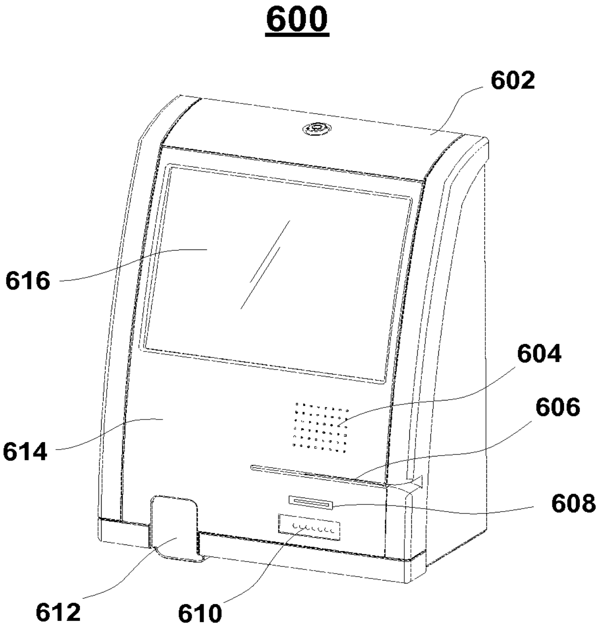

600
602
616
604
606
614
608
612
610

FIG. 6

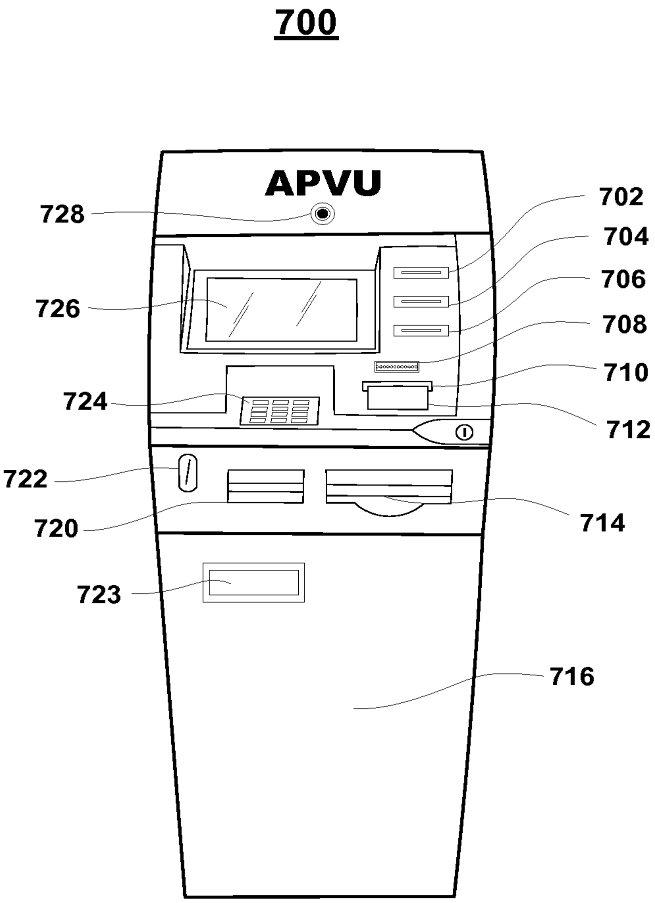
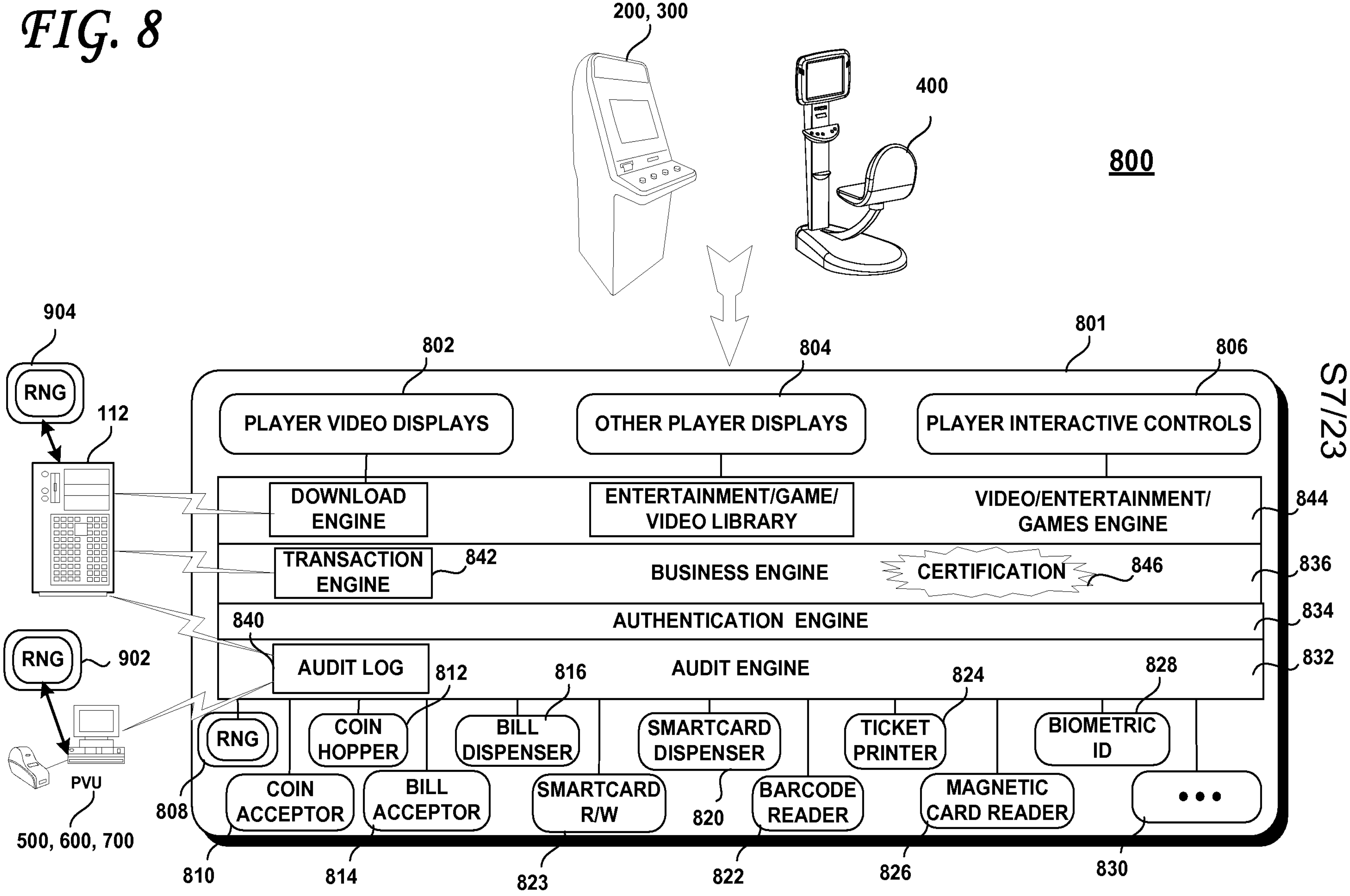


FIG. 7

FIG. 8


200, 300
400
800
904
RNG
112
802
804
801
806
PLAYER VIDEO DISPLAYS
OTHER PLAYER DISPLAYS
PLAYER INTERACTIVE CONTROLS
DOWNLOAD ENGINE
ENTERTAINMENT/GAME/ VIDEO LIBRARY
VIDEO/ENTERTAINMENT/ GAMES ENGINE
844
TRANSACTION ENGINE
842
BUSINESS ENGINE
CERTIFICATION
846
836
840
AUTHENTICATION ENGINE
834
RNG
902
AUDIT LOG
812
816
AUDIT ENGINE
824
828
832
RNG
COIN HOPPER
BILL DISPENSER
SMARTCARD DISPENSER
TICKET PRINTER
BIOMETRIC ID
PVU
808
COIN ACCEPTOR
BILL ACCEPTOR
SMARTCARD R/W
820
BARCODE READER
MAGNETIC CARD READER
•••
500, 600, 700
810
814
823
822
826
830

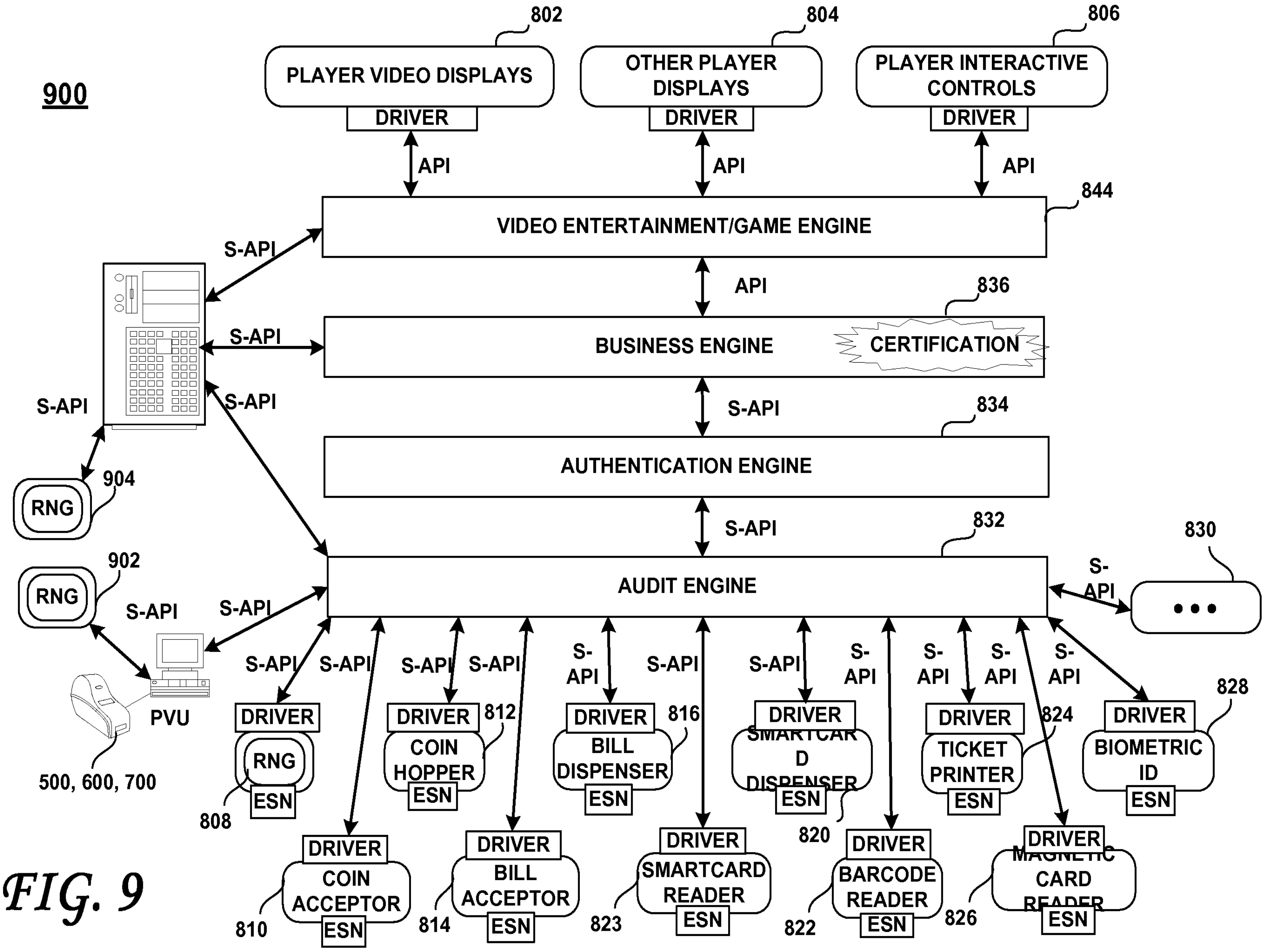
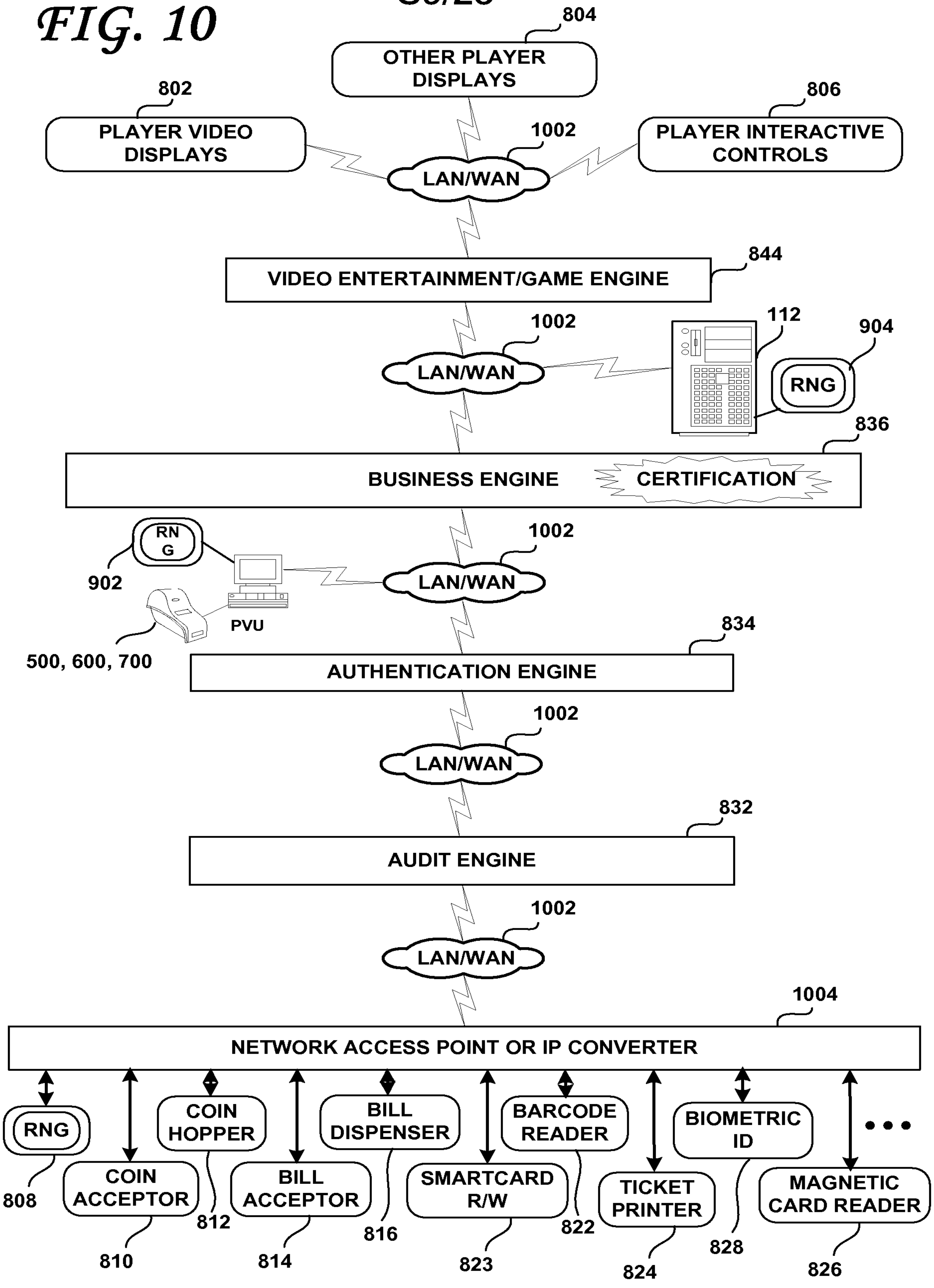

900
802
PLAYER VIDEO DISPLAYS
DRIVER
API
804
OTHER PLAYER DISPLAYS
DRIVER
API
806
PLAYER INTERACTIVE CONTROLS
DRIVER
API
844
VIDEO ENTERTAINMENT/GAME ENGINE
API
836
BUSINESS ENGINE
CERTIFICATION
S-API
834
AUTHENTICATION ENGINE
S-API
832
AUDIT ENGINE
S-API
S-API
S-API
S-API
904
RNG
902
RNG
S-API
S-API
PVU
500, 600, 700
830
S-API
S-API
DRIVER
RNG
ESN
808
S-API
DRIVER
COIN ACCEPTOR
ESN
810
S-API
DRIVER
COIN HOPPER
ESN
812
S-API
DRIVER
BILL ACCEPTOR
ESN
814
S-API
DRIVER
BILL DISPENSER
ESN
816
S-API
DRIVER
SMARTCARD READER
ESN
823
S-API
DRIVER
SMARTCARD DISPENSER
ESN
820
S-API
DRIVER
BARCODE READER
ESN
822
S-API
DRIVER
TICKET PRINTER
ESN
824
S-API
DRIVER
MAGNETIC CARD READER
ESN
826
S-API
DRIVER
BIOMETRIC ID
ESN
828

FIG. 9

FIG. 10


804
OTHER PLAYER DISPLAYS
802
PLAYER VIDEO DISPLAYS
1002
LAN/WAN
806
PLAYER INTERACTIVE CONTROLS
VIDEO ENTERTAINMENT/GAME ENGINE
844
1002
LAN/WAN
112
904
RNG
836
BUSINESS ENGINE
CERTIFICATION
RN G
902
1002
LAN/WAN
PVU
500, 600, 700
834
AUTHENTICATION ENGINE
1002
LAN/WAN
832
AUDIT ENGINE
1002
LAN/WAN
1004
NETWORK ACCESS POINT OR IP CONVERTER
RNG
808
COIN ACCEPTOR
810
COIN HOPPER
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMARTCARD R/W
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826
• • •

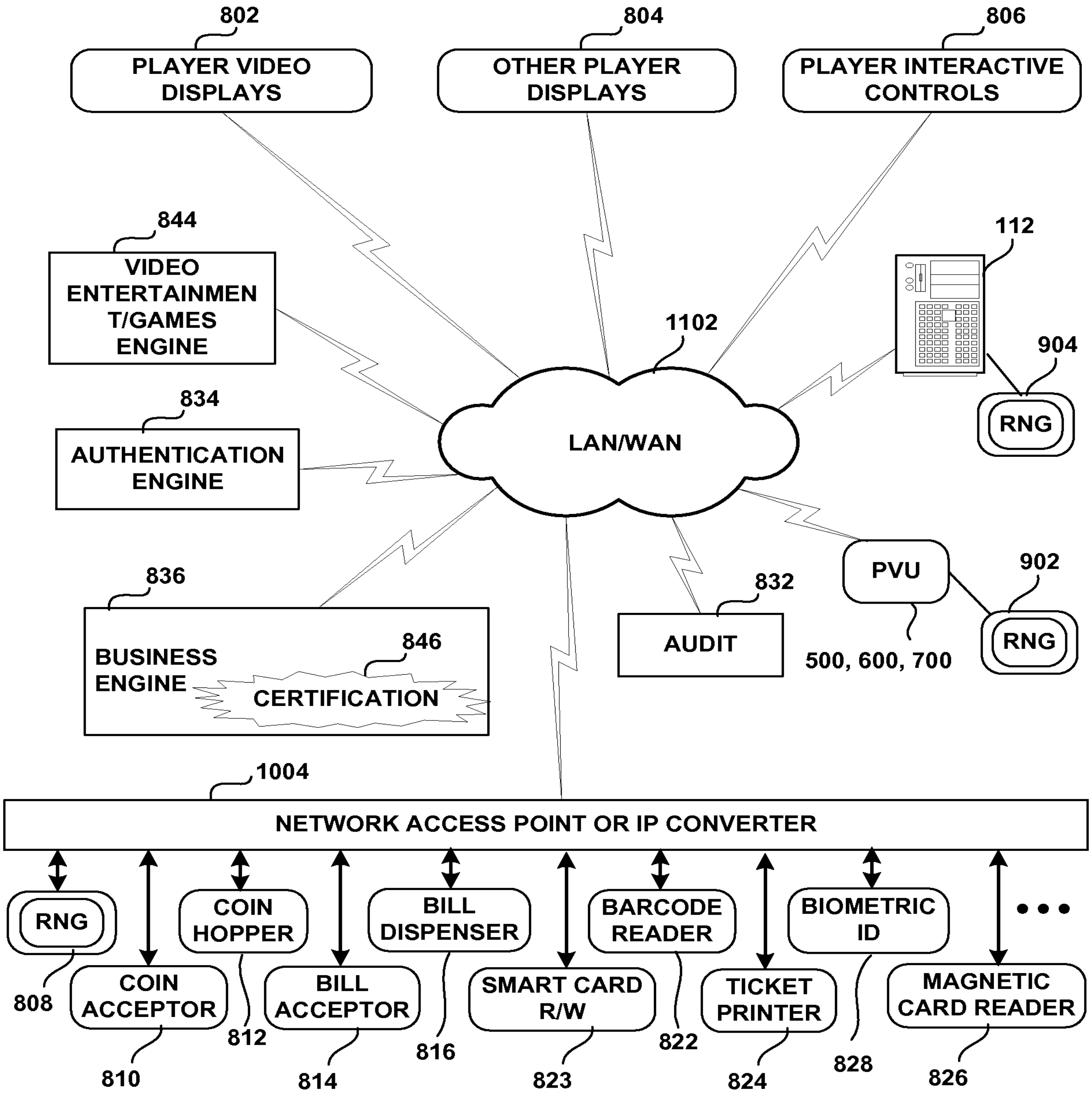

802
PLAYER VIDEO DISPLAYS
804
OTHER PLAYER DISPLAYS
806
PLAYER INTERACTIVE CONTROLS
844
VIDEO ENTERTAINMEN T/GAMES ENGINE
112
1102
904
RNG
834
AUTHENTICATION ENGINE
LAN/WAN
836
BUSINESS ENGINE
846
CERTIFICATION
832
AUDIT
PVU
500, 600, 700
902
RNG
1004
NETWORK ACCESS POINT OR IP CONVERTER
RNG
808
COIN ACCEPTOR
810
COIN HOPPER
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMART CARD R/W
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826
• • •

FIG. 11

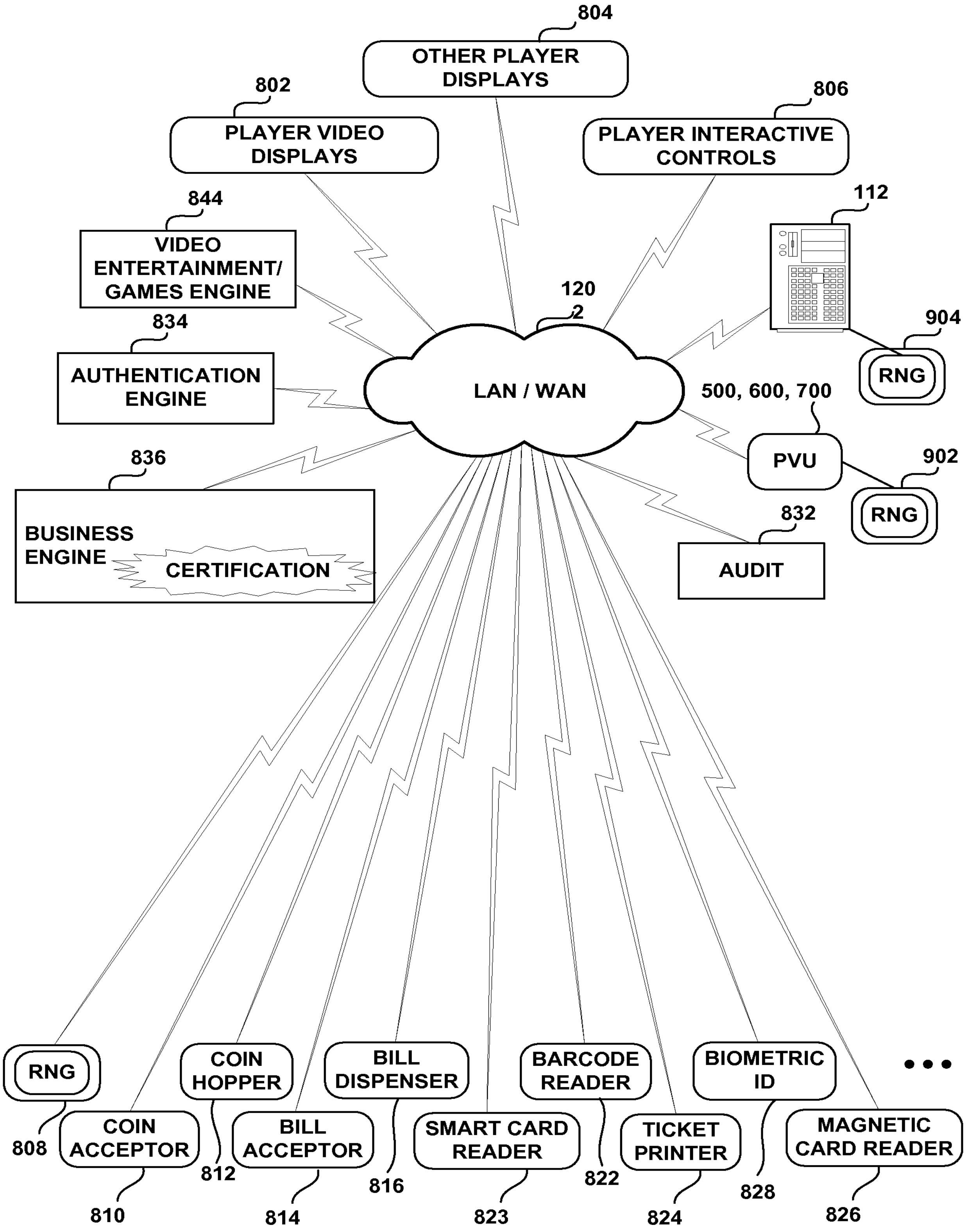

804
OTHER PLAYER DISPLAYS
802
PLAYER VIDEO DISPLAYS
806
PLAYER INTERACTIVE CONTROLS
112
844
VIDEO ENTERTAINMENT/ GAMES ENGINE
120
2
834
AUTHENTICATION ENGINE
LAN / WAN
904
RNG
500, 600, 700
PVU
902
RNG
836
BUSINESS ENGINE
CERTIFICATION
832
AUDIT
RNG
808
COIN ACCEPTOR
810
COIN HOPPER
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMART CARD READER
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826
• • •

FIG. 12

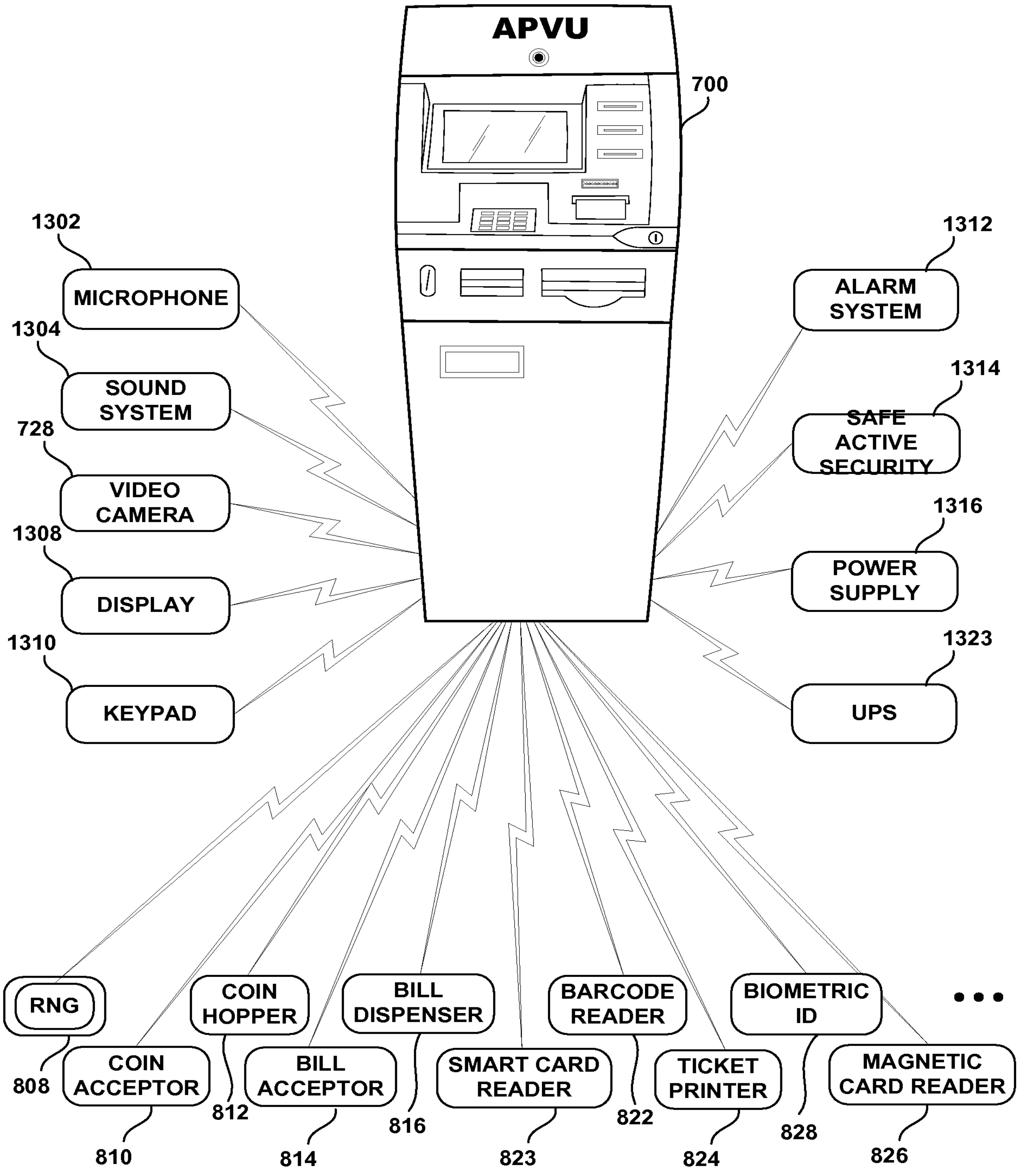

APVU
700
1302
MICROPHONE
1304
SOUND SYSTEM
728
VIDEO CAMERA
1308
DISPLAY
1310
KEYPAD
1312
ALARM SYSTEM
1314
SAFE ACTIVE SECURITY
1316
POWER SUPPLY
1323
UPS
RNG
808
COIN ACCEPTOR
810
COIN HOPPER
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMART CARD READER
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826
• • •

FIG. 13

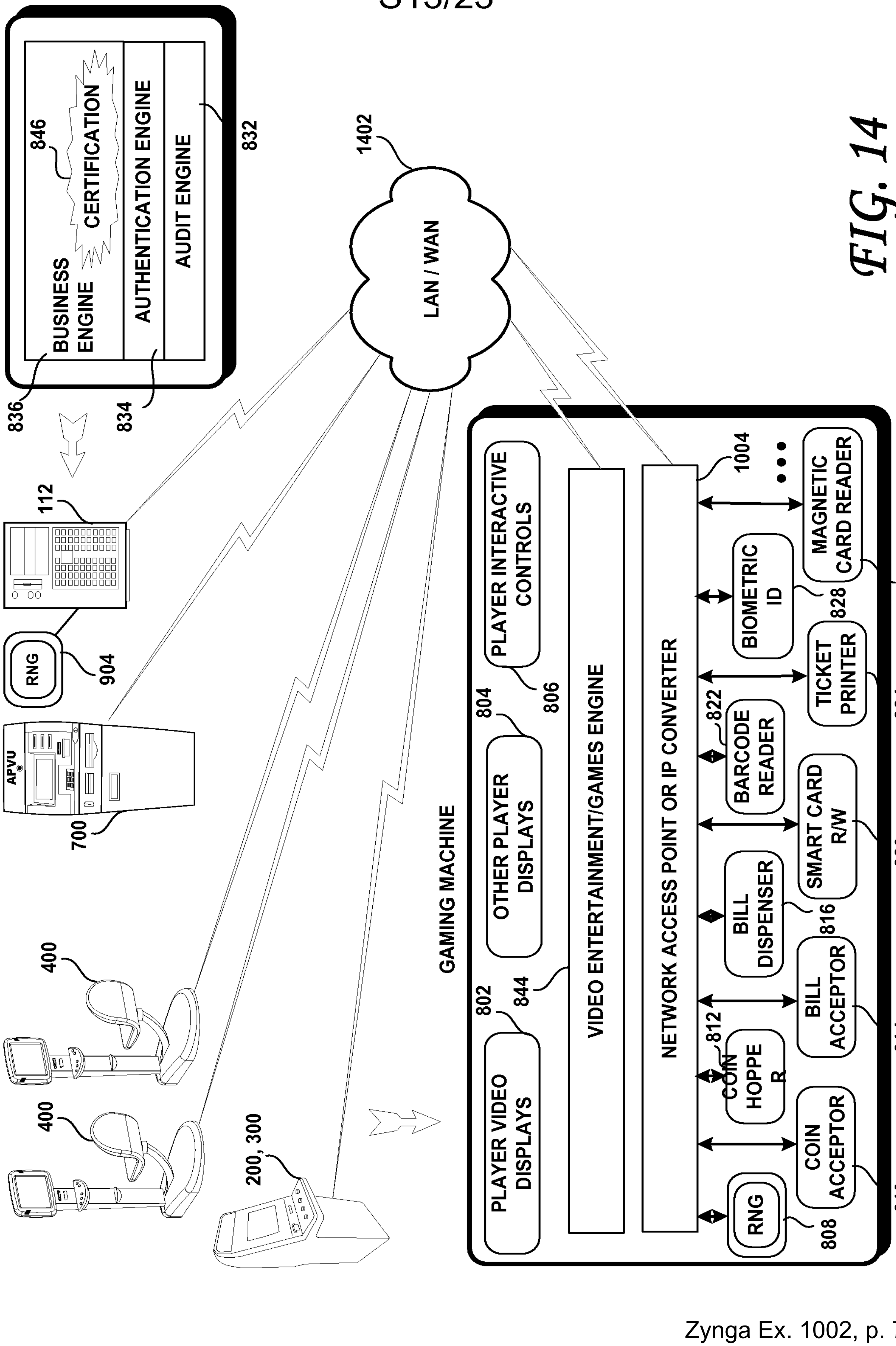

BUSINESS ENGINE
CERTIFICATION
AUTHENTICATION ENGINE
AUDIT ENGINE
836
834
846
832
1402
LAN / WAN
112
RNG
904
APVU
700
400
400
200, 300
GAMING MACHINE
PLAYER VIDEO DISPLAYS
802
844
OTHER PLAYER DISPLAYS
804
PLAYER INTERACTIVE CONTROLS
806
VIDEO ENTERTAINMENT/GAMES ENGINE
NETWORK ACCESS POINT OR IP CONVERTER
1004
RNG
808
COIN ACCEPTOR
810
COIN HOPPE R
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMART CARD R/W
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826

FIG. 14

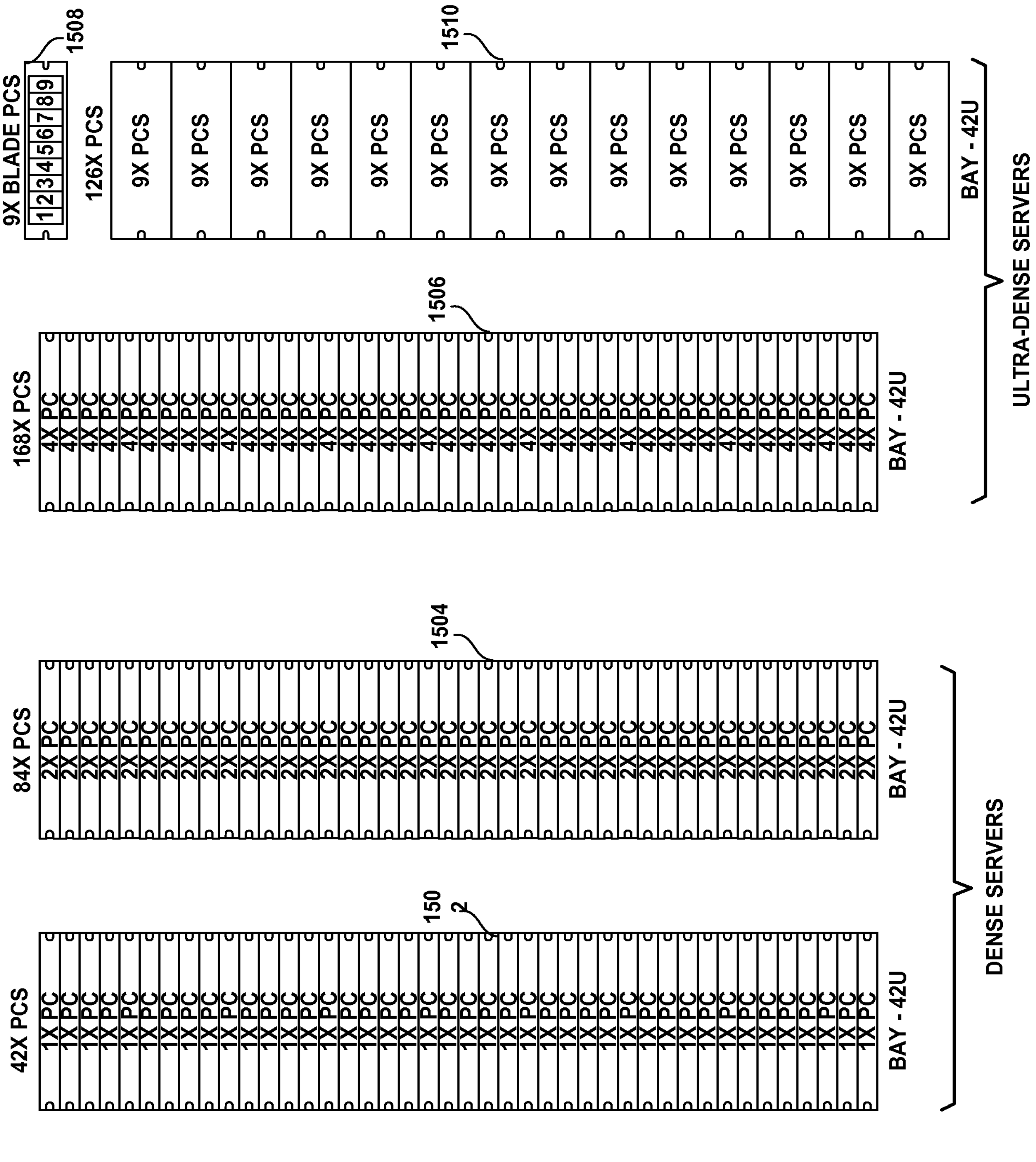

9X BLADE PCS
1 2 3 4 5 6 7 8 9
1508
126X PCS
1510
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
9X PCS
BAY - 42U
ULTRA-DENSE SERVERS
168X PCS
1506
4X PC
BAY - 42U
84X PCS
1504
2X PC
BAY - 42U
42X PCS
150
2
1X PC
BAY - 42U
DENSE SERVERS

FIG. 15

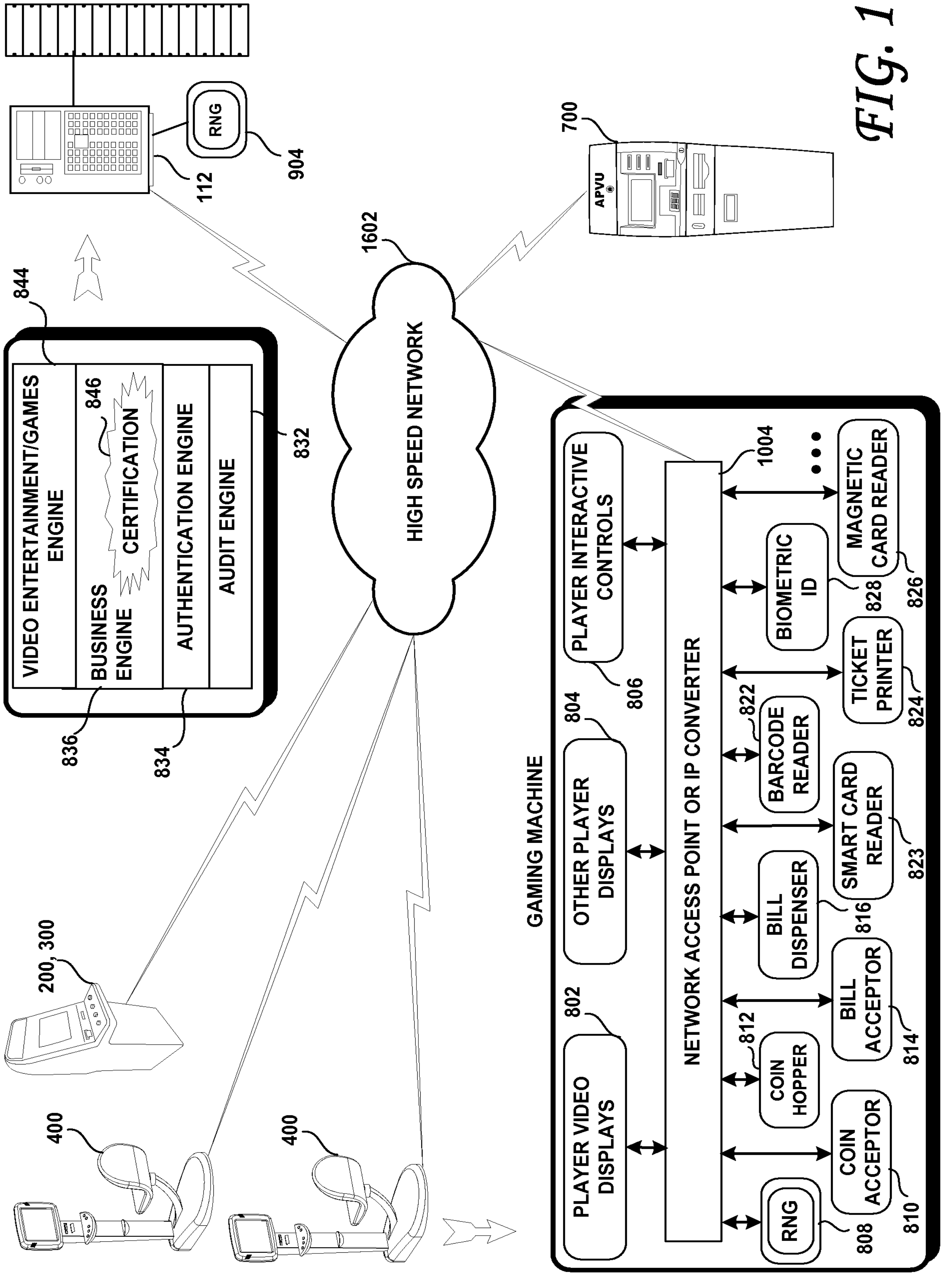

112
RNG
904
844
VIDEO ENTERTAINMENT/GAMES ENGINE
BUSINESS ENGINE
846
CERTIFICATION
AUTHENTICATION ENGINE
AUDIT ENGINE
832
836
834
1602
HIGH SPEED NETWORK
700
APVU
200, 300
400
400
GAMING MACHINE
PLAYER VIDEO DISPLAYS
802
OTHER PLAYER DISPLAYS
804
PLAYER INTERACTIVE CONTROLS
806
NETWORK ACCESS POINT OR IP CONVERTER
1004
RNG
808
COIN ACCEPTOR
810
COIN HOPPER
812
BILL ACCEPTOR
814
BILL DISPENSER
816
SMART CARD READER
823
BARCODE READER
822
TICKET PRINTER
824
BIOMETRIC ID
828
MAGNETIC CARD READER
826

FIG. 16

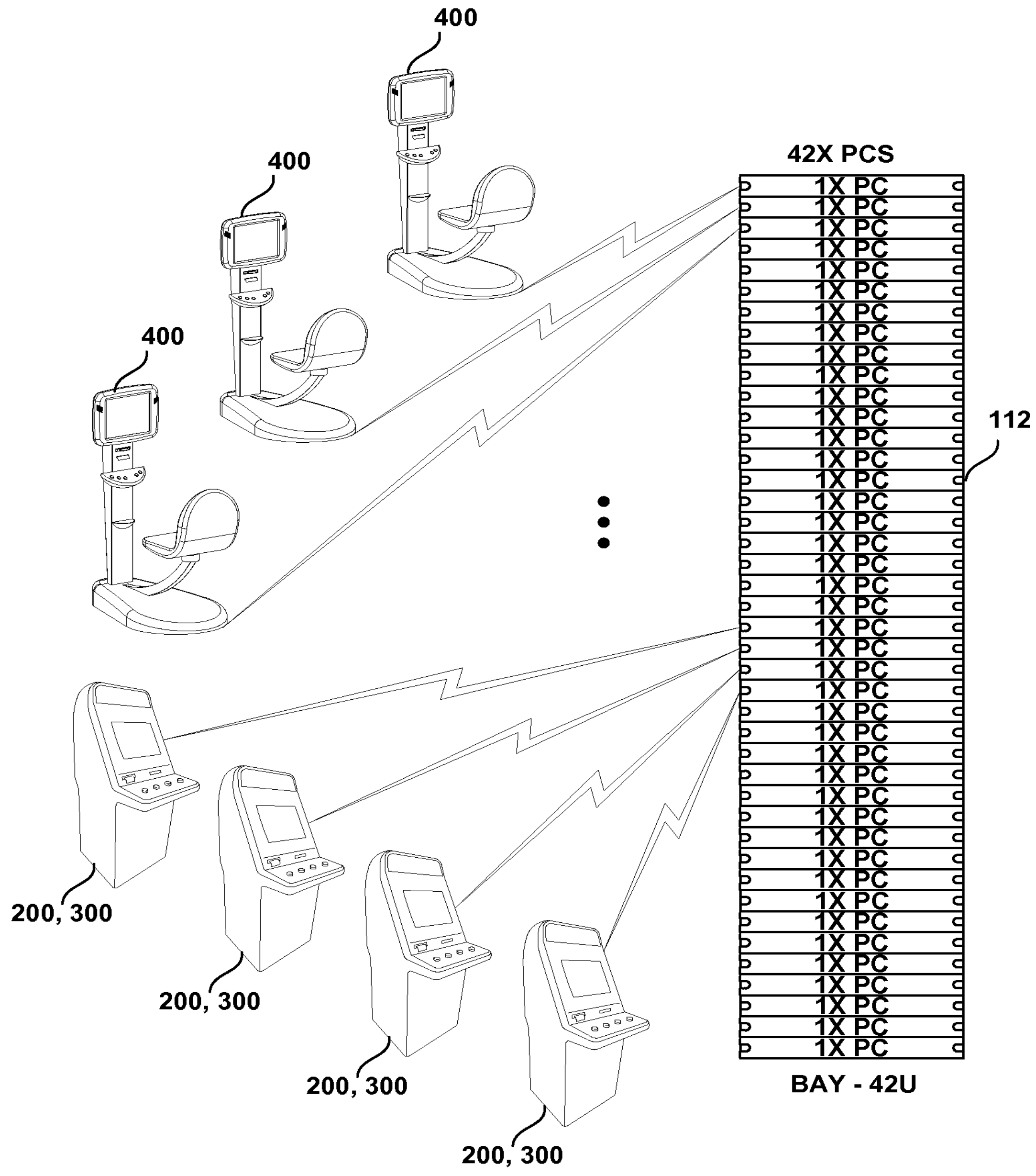

400
400
400
42X PCS
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
1X PC
112
BAY - 42U
200, 300
200, 300
200, 300
200, 300

FIG. 17

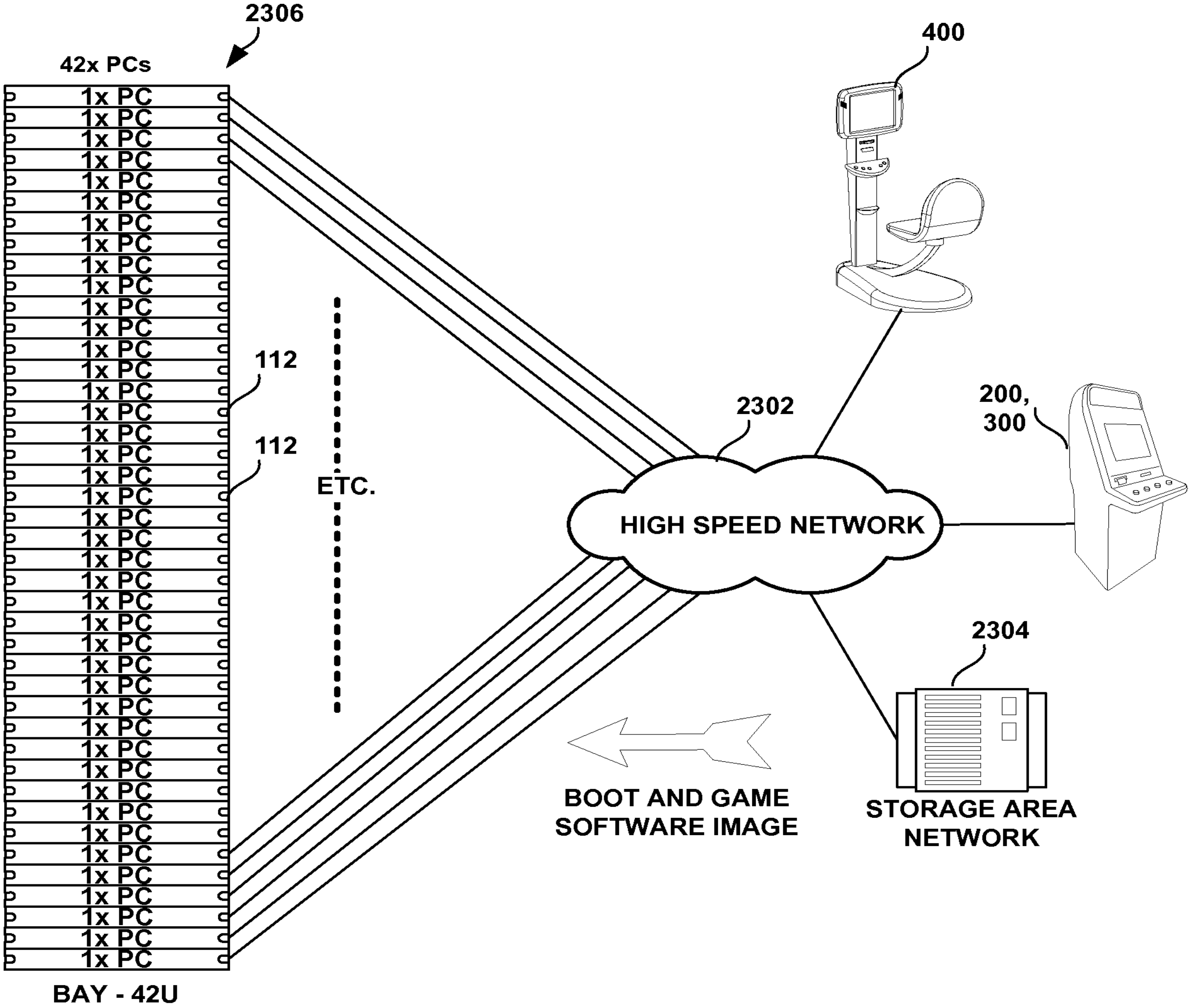

2306
42x PCs
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
1x PC
112
112
ETC.
BAY - 42U
400
2302
HIGH SPEED NETWORK
200,
300
2304
STORAGE AREA
NETWORK
BOOT AND GAME
SOFTWARE IMAGE

FIG. 18

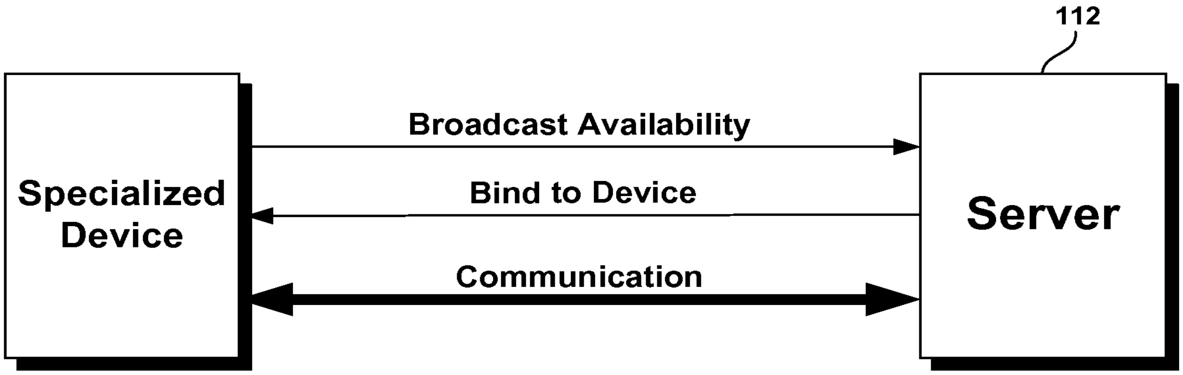

112
Specialized Device
Broadcast Availability
Bind to Device
Communication
Server

FIG. 19

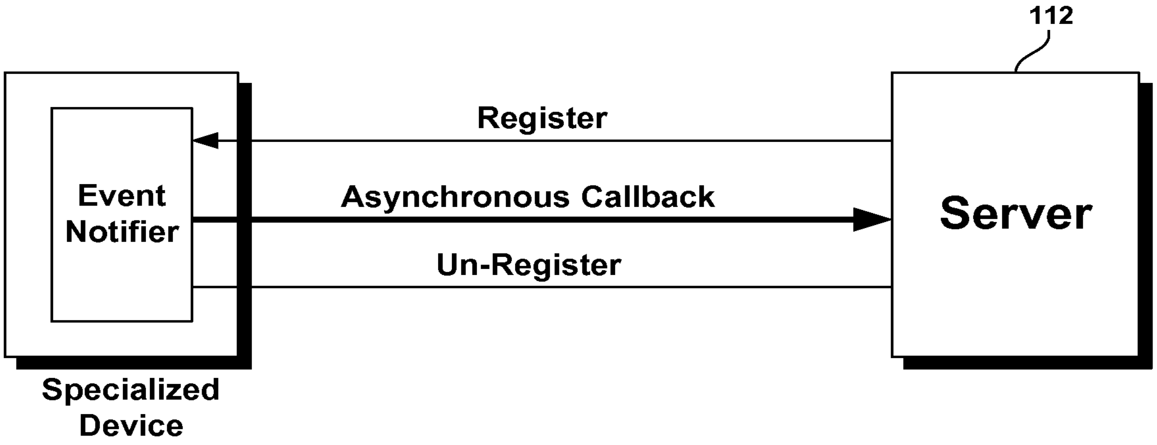

112
Event Notifier
Register
Asynchronous Callback
Un-Register
Server
Specialized Device

FIG. 20

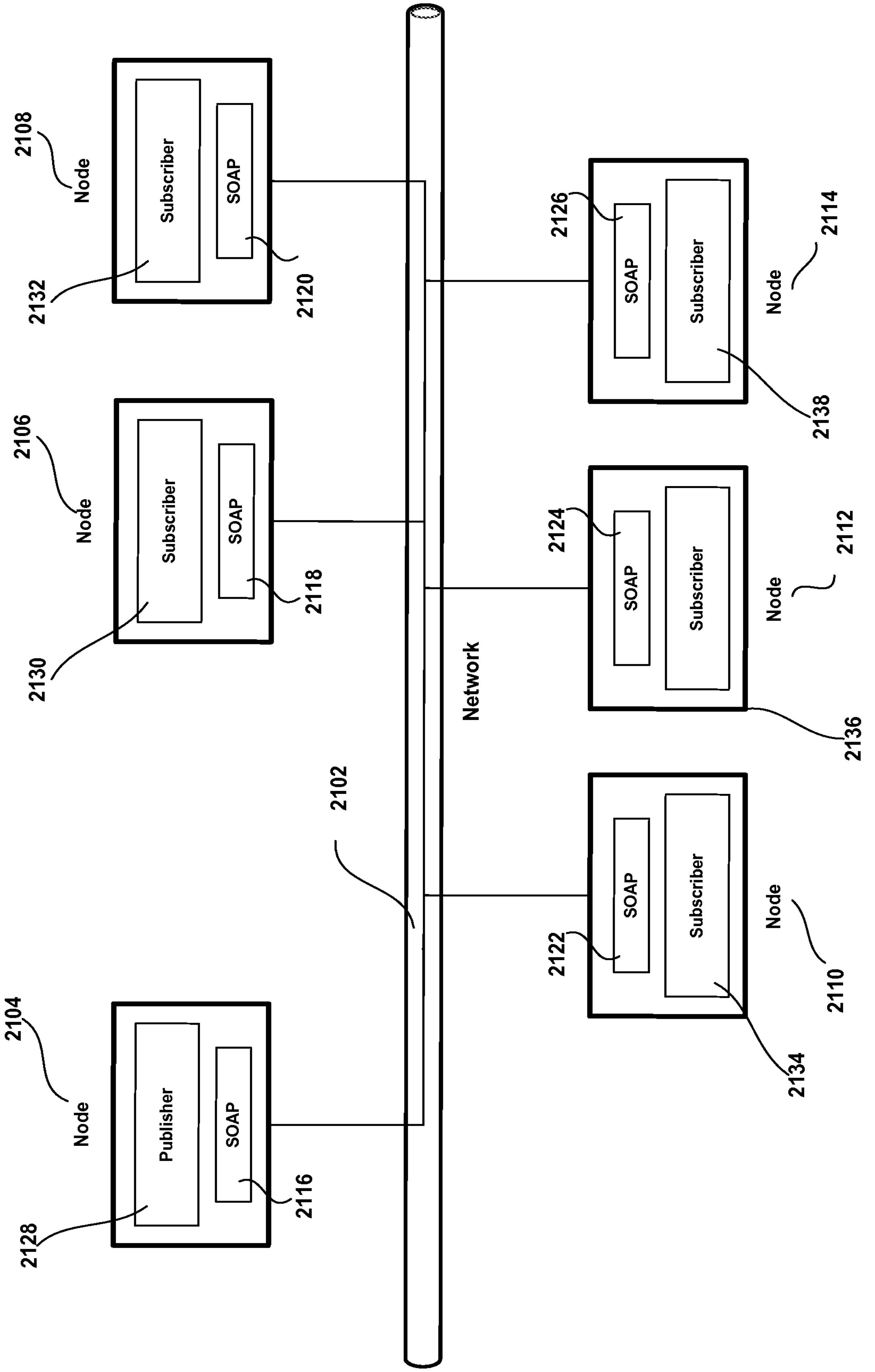

2104
Node
Publisher
SOAP
2116
2128
2106
Node
Subscriber
SOAP
2118
2130
2108
Node
Subscriber
SOAP
2120
2132
2102
Network
2122
SOAP
Subscriber
Node
2110
2134
2124
SOAP
Subscriber
Node
2112
2136
2126
SOAP
Subscriber
Node
2114
2138

FIG. 21

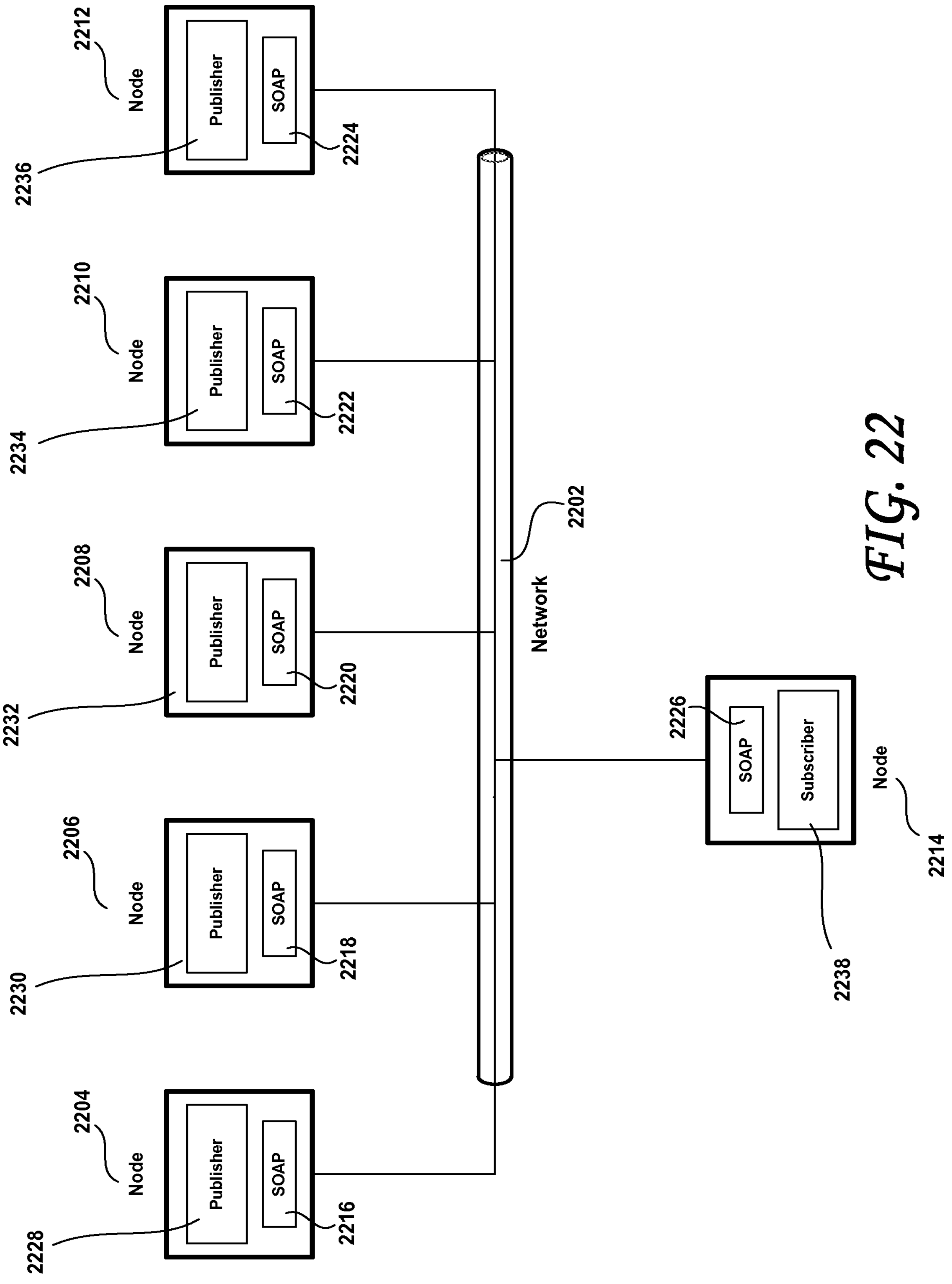

Node
2204
Publisher
SOAP
2228
2216
Node
2206
Publisher
SOAP
2230
2218
Node
2208
Publisher
SOAP
2232
2220
Node
2210
Publisher
SOAP
2234
2222
Node
2212
Publisher
SOAP
2236
2224
Network
2202
2226
SOAP
Subscriber
Node
2214
2238

FIG. 22

S21/23

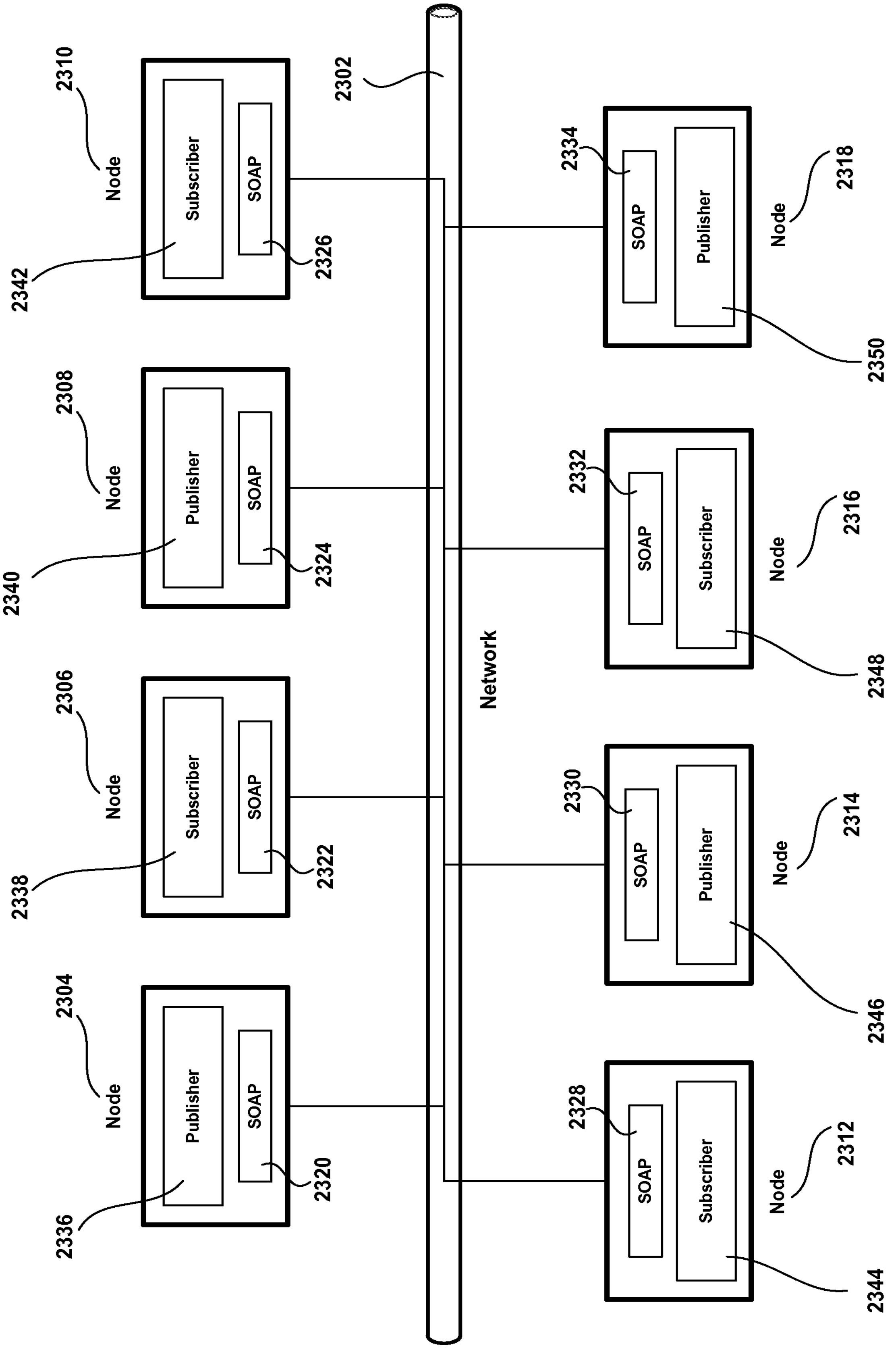

2302
Network
Node
2304
Publisher
2336
SOAP
2320
Node
2306
Subscriber
2338
SOAP
2322
Node
2308
Publisher
2340
SOAP
2324
Node
2310
Subscriber
2342
SOAP
2326
Node
2312
Subscriber
2344
SOAP
2328
Node
2314
Publisher
2346
SOAP
2330
Node
2316
Subscriber
2348
SOAP
2332
Node
2318
Publisher
2350
SOAP
2334

FIG. 23

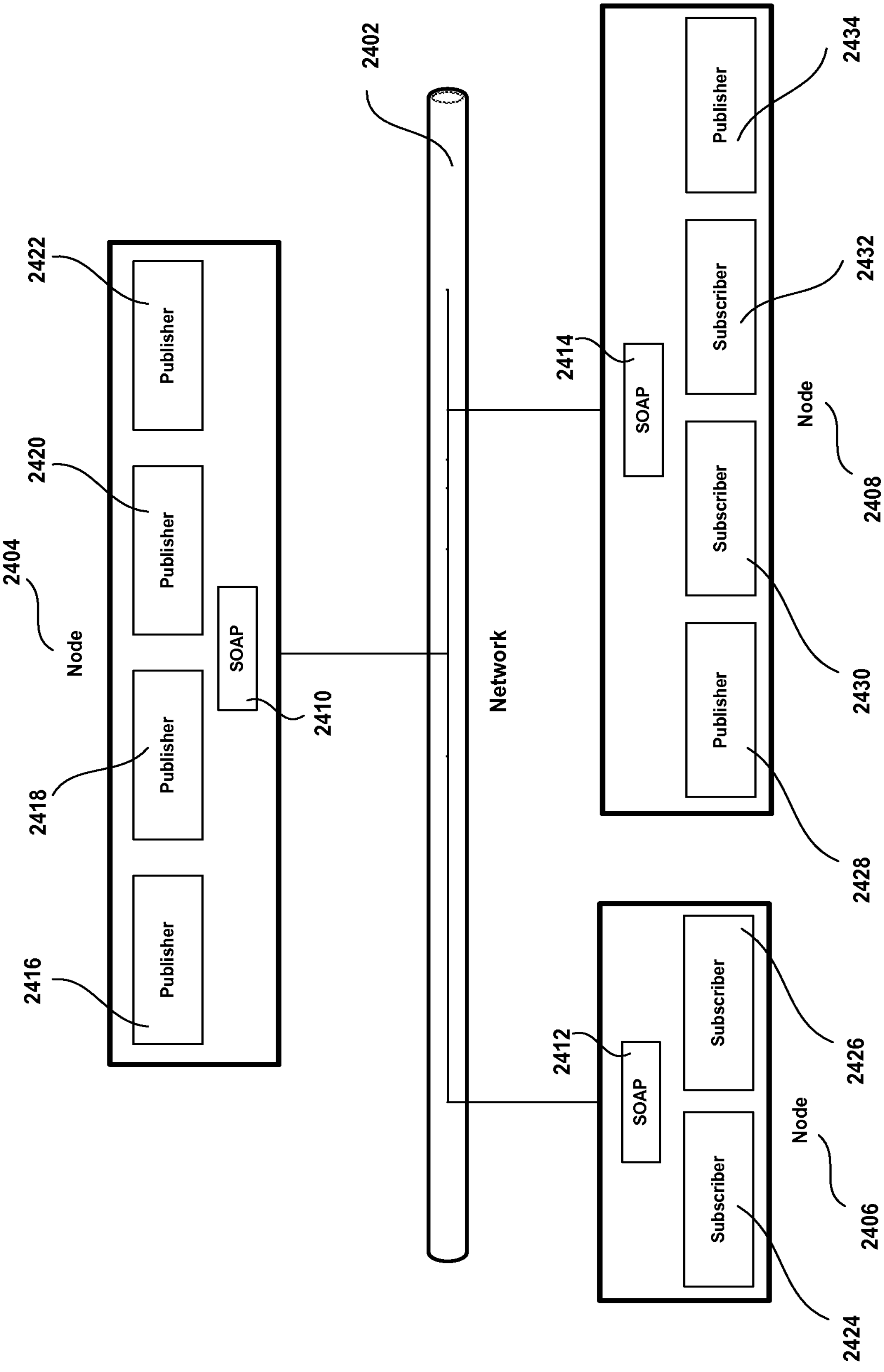

2404
Node
2416
Publisher
2418
Publisher
2420
Publisher
2422
Publisher
SOAP
2410
2402
Network
2412
SOAP
2414
SOAP
2406
Node
Subscriber
Subscriber
2424
2426
2408
Node
Publisher
Subscriber
Subscriber
Publisher
2428
2430
2432
2434

FIG. 24

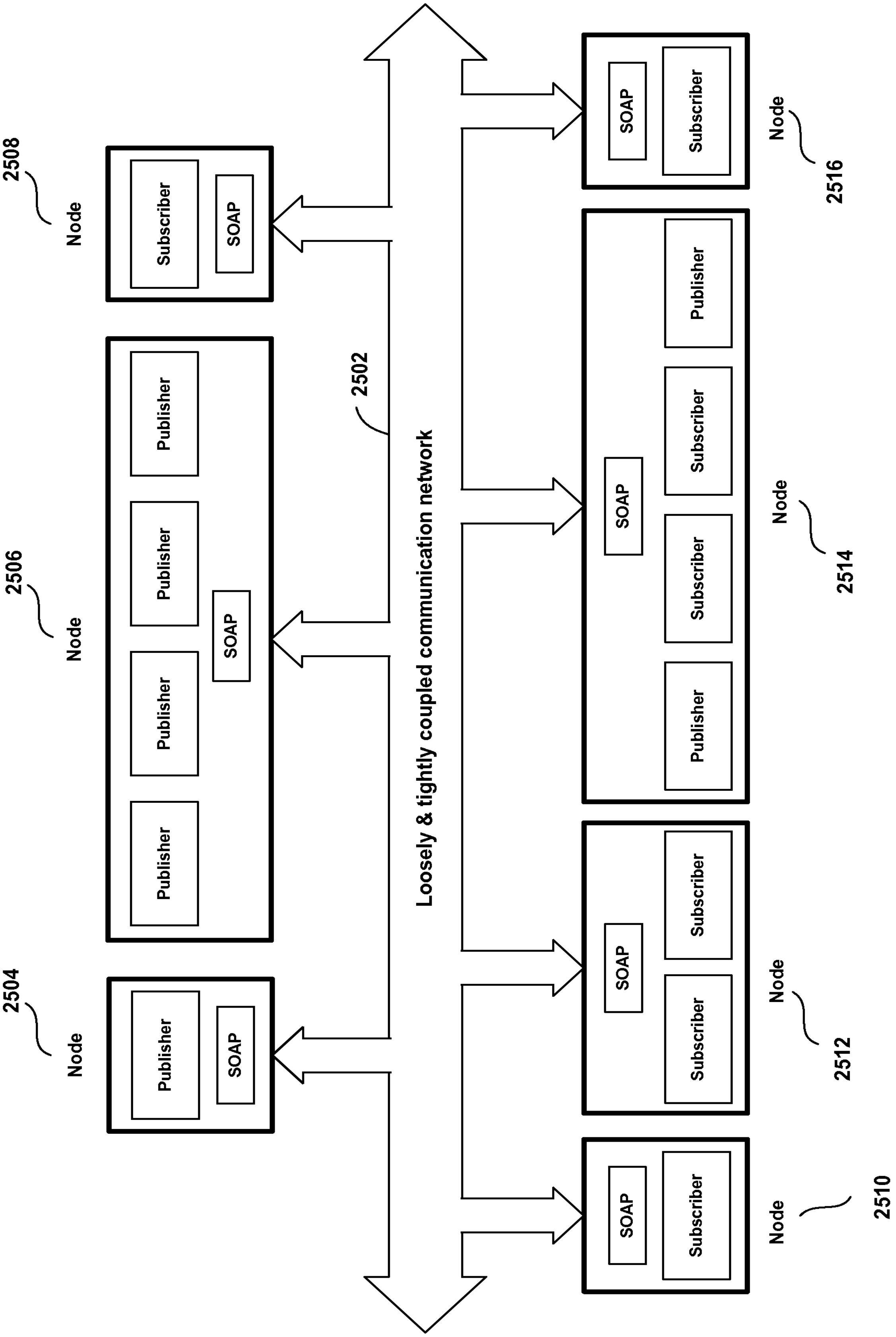

2508
Node
Subscriber
SOAP
2506
Node
Publisher
Publisher
Publisher
Publisher
SOAP
2504
Node
Publisher
SOAP
2502
Loosely & tightly coupled communication network
Node
2516
SOAP
Subscriber
Node
2514
SOAP
Publisher
Subscriber
Subscriber
Publisher
Node
2512
SOAP
Subscriber
Subscriber
Node
2510
SOAP
Subscriber

FIG. 25

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Filer:	Alan W. Young/Nita Miller
Attorney Docket Number:	CYBS5805CIP

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Claims in excess of 20	2202	21	25	525
Independent claims in excess of 3	2201	1	100	100
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1050**

Electronic Acknowledgement Receipt

EFS ID:	2104151
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	21-AUG-2007
Filing Date:	
Time Stamp:	02:08:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$1050
RAM confirmation Number	4232
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)

1		5805CIPPA.pdf	827349 d0fa4c5072f49e00bc50271d35dd5088 50da4e8d	yes	87

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal of New Application	1	1
Application Data Sheet	2	4
Specification	5	55
Claims	56	63
Abstract	64	64
Drawings	65	87

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	8550 aec694160b71a5e73149c9a6f12d9f05 31d5963f	no	2

Warnings:

Information:

Total Files Size (in bytes):	835899

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	
Examiner Name	
Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4335809	A	1982-06-22	J. L. Wain	
	2	5667440	A	1997-09-16	Sasaki et al.	
	3	6135887	A	2000-10-24	L. L. Pease	
	4	6219836	B1	2001-04-17	B. Wells et al.	
	5	6251014	B1	2001-06-26	J. Stockdale et al.	
	6	6273821	B1	2001-08-14	Moriguchi	
	7	6077163		2000-06-20	Walker et al.	
	8	6749510		2004-06-15	Giobbi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	
Examiner Name	
Attorney Docket Number	CYBS5805CIP

	9	6280328		2001-08-28	Holch et al.	
	10	6089982		2000-07-18	Holch et al.	
	11	5800269		1998-09-01	Holch et al.	
	12	5674128		1997-10-07	Holch et al.	
	13	5179517		1993-01-12	Sarbin et al.	
	14	6916247	B2	2005-07-12	Gatto et al.	
	15	5759102	A	1998-06-02	Pease et al.	
	16	5762552	A	1998-06-09	Vuong et al.	
	17	5970143	A	1999-10-19	Schneier et al.	
	18	6048269	A	2000-04-11	Burns et al.	
	19	6908391	B2	2005-06-21	Gatto et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	
Examiner Name	
Attorney Docket Number	CYBS5805CIP

	20	6463530	B1	2002-10-08	Sposato	
	21	6945870	B2	2005-09-20	Gatto et al.	
	22	6142876	A	2000-11-07	Cumbers	
	23	6710895	B1	2004-03-23	Gatto et al.	
	24	6732920	B2	2004-05-11	Gatto et al.	
	25	6921331	B2	2005-07-26	Gatto et al.	
	26	6409602		2002-06-25	Wiltshire et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020137217	A1	2002-09-26	R. E. Rowe	
	2	20020147040	A1	2002-10-10	Walker et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	
Examiner Name	
Attorney Docket Number	CYBS5805CIP

	3	20020174444	A1	2002-11-21	Gatto et al.	
	4	20030037335	A1	2003-02-20	Gatto et al.	
	5	20020090934	A1	2002-07-11	Eliott R.D. Mitchelmore	
	6	20030087683	A1	2003-05-08	Gatto et al.	
	7	20030100369	A1	2003-05-29	Gatto et al.	
	8	20030100370	A1	2003-05-29	Gatto et al.	
	9	20030100371	A1	2003-05-29	Gatto et al.	
	10	20030100372	A1	2003-05-29	Gatto et al.	
	11	20030171140	A1	2003-09-11	Gatto et al.	
	12	20050032577	A1	2005-02-10	Christopher W. Blackburn et al.	
	13	20050054448	A1	2005-03-10	Gary Frerking et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-20
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		CYBS5805CIP

	14	20050059494	A1	2005-03-17	Keith Donald Kammler	
	15	20050113172	A1	2005-05-26	Xiaoqiang D. Gong	
	16	20050233811	A1	2005-10-20	Gatto et al.	
	17	20050282637	A1	2005-12-22	Gatto et al.	
	18	20060183537	A1	2006-08-17	Scott Dickerson	
	19	20060270478	A1	2006-11-30	William J. Barhydt et al.	
	20	20070180371	A1	2007-08-02	Keith Donald Kammler	
	21	20070184896	A1	2007-08-09	Scott Dickerson	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1004970	EP	A2	2000-05-31	International Game Technology		□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-20
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		CYBS5805CIP

	2	1004970	EP	A3	2000-05-31	International Game Technology		□
	3	1074955	EP	A2	2001-02-07	Maygay Machines Limited		□
	4	1074955	EP	A3	2001-02-07	Maygay Machines Limited		□
	5	1231577	EP	A2	2001-11-09	WMS Gaming Inc.		□
	6	1231577	EP	A3	2001-11-09	WMS Gaming Inc.		□
	7	19941504	DE	A1	2001-03-01	Internet Special Services		□
	8	1120757	EP	A2	2001-08-01	International Game Technoology		□
	9	1120757	EP	A3	2001-08-01	International Game Technoology		□
	10	1087323	EP	A1	2001-03-28	Nokia Corporation		□
	11	0182176	WO	A	2001-11-01	Gaming System Technologies		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147	
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	CYBS5805CIP	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

CYBS5803EP
EPSR 11/28/06
Ref. 4/7

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 004 970 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.05.2000 Bulletin 2000/22

(21) Application number: 99119351.7

(22) Date of filing: 29.09.1999

(51) Int. Cl.^{7}: G06F 17/60, G07F 17/32,
A63F 13/00

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 14.10.1998 US 172786

(71) Applicant:
International Game Technology
Reno, Nevada 89511-8986 (US)

(72) Inventors:
- Wells, Bill
Reno, Nevada 89502 (US)
- Wilder, Richard
Sparks, Nevada 89436 (US)

(74) Representative:
Manitz, Finsterwald & Partner
Postfach 22 16 11
80506 München (DE)

(54) Method for downloading data to gaming devices

(57) Memories coupled to a gaming terminal, are reprogrammed by a method and apparatus which includes identification, negotiation, downloading and verification information from an external information source to a gaming terminal. Hardware devices are used to identify gaming terminals or components.

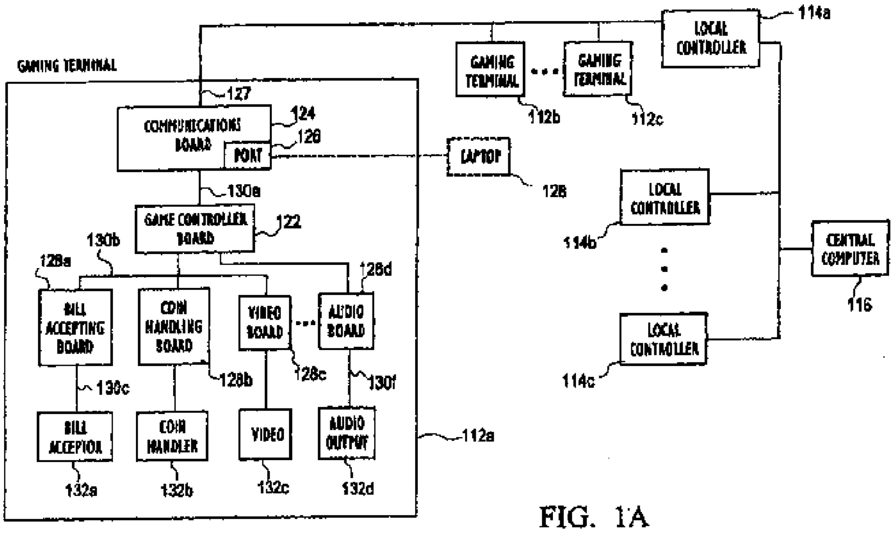


FIG. 1A

EP 1 004 970 A2

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

[0001] Cross-reference is made to U.S. Serial No. 09/088,205 (Attorney File No. 3735-905-CON) filed June 1, 1998, which is a continuation of Serial No. 08/600,311 (for "PERIPHERAL DEVICE DOWNLOAD METHOD AND APPARATUS" filed February 12, 1996), both incorporated herein by reference.

[0002] The present invention relates to a method and apparatus for downloading information to a gaming device and in particular, to a process for using a computer, directly or remotely, to transfer information to a gaming device in a secure fashion.

BACKGROUND INFORMATION

[0003] Many current gaming machines are configured with electronic components, commonly mounted on one or more printed circuit boards (PCBs). Many such electronic components use programming or other information stored in memories. In at least one typical configuration, a gaming terminal or gaming machine will include a controller board, a communications board or module, and one or more so-called peripheral boards such as a display controller board, a currency acceptor board, a coin handler board, and the like. Typically at least one board, such as the game controller board, includes a processor (e.g., a microprocessor) or other computer unit which often operates based on programming or other information (software) stored in a memory such as one or more electronically erasable programmable read-only memories (EEPROMS). Such software may be programmed or stored in the memory locations during the manufacturing or assembly of the gaming device. Additionally, software may be provided to replace or supplement the software in a gaming device which is in operation (in the field), e.g. to add new features, implement new games and the like, and/or to correct programming errors. In either case, the new software is transferred or "downloaded" from a source (which may be, e.g., a computer such as a workstation personal computer, laptop computer, and the like) to the "target" memory in a particular gaming terminal or machine.

[0004] Downloading from one computer to another is a process that is known, in general. In one previous system, information from a host system such as a state lottery host has been downloaded to a clerk validation terminal (CVT). A clerk validation terminal is used for verifying a ticket obtained from a lottery terminal e.g. to verify a validation number, amount and the like before a lottery ticket is paid, e.g. as an anti-counterfeiting procedure. However, downloading software to components of gaming devices and/or to a plurality of gaming devices or components thereof presents particular problems not readily addressed by conventional downloading techniques.

[0005] One aspect applicable to gaming devices is the stringent regulatory oversight and control exercised by regulatory authorities in many jurisdictions. In many, and perhaps all, regulated gaming jurisdictions, downloading of software to a gaming terminal will not be permitted without some assurance that the new software will comply with local regulations.

[0006] For example, a gaming regulatory authority in one jurisdiction may require assurance that downloading to, e.g., update bill acceptor software will result in a machine having bill acceptor software appropriate (and approved) for that jurisdiction (and will not, e.g., run the risk of inadvertently and/or intentionally downloading bill acceptor software that was approved in a different jurisdiction).

[0007] It is also commonly found that gaming devices occur in a wide variety of configurations, such as employing numerous different types of processors, memories, game configurations , versions and types, peripheral hardware and software and the like. Additionally, owing to differences in manufacturing dates, maintenance history and the like, gaming devices are often encountered with a wide variety of different hardware and software components which may not be apparent (or may be discernable only with difficulty) from a visual inspection of the gaming device, its components, or its operation. For this reason, when it is desired to download software to a particular gaming terminal, it is typically necessary to select a particular software version for downloading, bearing in mind the types of software and hardware found on the particular gaming terminal, lest the newly-downloaded software is incompatible with the gaming terminal or results in operation which is not approved by a particular jurisdiction. Additionally, it is possible that the software which is to be downloaded is, in fact, already present on a particular gaming terminal, so that the download process represents a waste of time and effort.

[0008] Although many types of memories can be modified to store other or additional programs (such as an erasable programmable read-only memory or EPROM), in many previous devices this was often a labor-intensive and time-consumptive procedure, sometimes involving removing the EPROM or other memory device and reprogramming it in a separate device and/or replacing it with a differently-programmed memory device. Many pin-type memory devices are configured to tolerate only a limited number of removal and insertion operations. Other memory devices are configured for solder connection or are otherwise not readily replaceable, necessitating replacement of an entire board to effect updating.

[0009] Such manual operations have, in the past, typically required a significant investment of time, especially when a relatively large number of gaming terminals are being programmed or reprogrammed. To make matters worse, the time investment is typically made by relatively highly-trained personnel. Such investment of time by relatively highly-trained personnel represents a significant expense involved in storing or updating gaming terminal programming or other information which, owing at least partly to the regulatory environment found for gaming devices, was previously believed to be a largely unavoidable cost. Furthermore, it has been found that even relatively highly-trained personnel have an undesirably high error rate when attempting to perform a download which may lead to inoperability or improper operation of a gaming device, or violation of gaming jurisdiction laws or rules and may require an additional investment of time to correct such errors.

[0010] This situation is particularly burdensome in the context of gaming devices in which it is sometimes necessary or desirable to change the programming in a large number of peripheral devices in a relatively short amount of time. One example of such a situation is when it is desired to reprogram a bill acceptor, e.g. to thwart a previously-unknown counterfeiting scheme. Previous systems which required labor-intensive and time-intensive reprogramming methods increased the risk of incurring losses during the time it took to perform this reprogramming for all the various gaming machines (e.g., in a plurality of different casinos) or their various components. An important feature of the invention is that it allows for download of data to multiple gaming devices simultaneously.

[0011] Another feature of many gaming devices which affects the manner in which revisions of software can or should be performed is the fact that gaming devices are often configured to dispense money so there is a potential for modifications or downloads to be performed in an unauthorized fashion in such a manner as to create unauthorized or improper payouts. This is a potential which is typically not present in many other types of downloads from one computer to another. Accordingly, it is important, not only to gaming regulatory authorities but also to casinos or other game operators, to achieve a level of confidence that not only will inadvertent (e.g. cross-jurisdictional) downloads be avoided but there are procedures in place to avoid or prevent intentional or unauthorized downloads.

[0012] Furthermore, previous reprogramming took place in a relatively conspicuous manner requiring personnel to access the interior of each individual peripheral and/or terminal, often for an extended period of time, thus potentially alerting the counterfeiters that they had been detected and decreasing the likelihood of using the new software to identify (possibly leading to apprehension of) the counterfeiters. In addition, the time during which a machine was being fitted with the new programs was time that the machine was out of service and not generating revenues.

[0013] In some situations, it may be advantageous to update the programming of two or more different gaming terminals and/or two or more different peripheral devices coupled to a single gaming device. Previous methods would, in this situation, typically have required separately accessing each of the gaming terminals and/or peripheral devices in order to modify or update programming.

[0014] As noted, it is often desirable to reprogram gaming terminals, e.g. to accommodate new games, regulatory changes, correct bugs or other programming errors, install new features and the like. Preferably, this should be accomplished with a minimum of down time of gaming devices (which often are intended normally to be accessible 24 hours a day) and a minimum of inconvenience to players.

[0015] Accordingly, it would be advantageous to provide a method and apparatus for downloading programming information in a manner which is less labor-intensive and less costly than previously provided, preferably without requiring individual direct access to each peripheral device which is being reprogrammed, and preferably while providing sufficient security and reliability safeguards that fully and partially automatic downloads will be permitted by gaming regulatory authorities.

SUMMARY OF THE INVENTION

[0016] The present invention provides for securely loading information, received from an external device (such as a laptop or a networked central computer) to one or more gaming devices. Preferably, the secure downloading system provides identification, negotiation, data transfer and verification features. Identification involves obtaining information for characterizing the hardware and/or software on a gaming terminal or other target. The identification information can be used to provide assurance that the programming or other data to be downloaded and/or the download procedures are appropriate for the target device. Negotiation involves providing information from the source to the target, relating to the download, such as where to load, compression information (if any) and the like. Preferably the source requests approval from the target device before data transfer begins. Preferably, data transfer is performed block-wise with checking of each block. Verification can be performed by the source requesting a digital signature calculated from the transferred data, preferably based on a public key decryption algorithm.

[0017] In one embodiment, the update or modified peripheral device program is received in the gaming terminal (or other computing device) from an external device (such as a hand-held or portable device or a central computer coupled via a communications link) and is downloaded from the gaming terminal controller board to one or mor coupled peripheral devices.

[0018] Preferably, the programming information is downloaded in such a way as to reduce or minimize the amount of down time or inconvenience to players. In one embodiment, when the new peripheral program is downloaded from a central computer to each gaming terminal, the method avoids disabling all gaming terminals at the same time, such as by waiting until the gaming terminal is idle for a predetermined period before downloading the new program to peripheral devices or by cycling through various gaming terminals or groups of gaming terminals so that a relatively small number of the gaming terminals are disabled (for reprogramming) at any one time. Additionally, the invention allows for download to multiple gaming devices or peripheral devices simultaneously.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019]

Fig. 1A is a block diagram depicting components of a multi-terminal gaming system, including components of a gaming terminal, of a type which may be used in connection with the present invention.

Fig. 1B is a block diagram of a plurality of gaming terminals, each coupled to a plurality of peripheral devices, and a central computer coupled to the gaming terminals which can be used according to an embodiment of the present invention;

Fig. 2 is a flow chart of a procedure for downloading information according to an embodiment of the present invention;

Fig. 3 is a block diagram of gaming terminals linked to a central system, usable according to an embodiment of the present invention;

Fig. 4 is a block diagram of a gaming terminal assembly and development system usable in accordance with an embodiment of the present invention; and

Fig. 5 is a flow chart depicting a download procedure in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0020] Although the present invention can be used in connection with many types of gaming terminals either as stand-alone devices or coupled in any number of different multi-terminal configurations, one example of a gaming terminal 112a coupled, along with other gaming terminals 112b,c, via one or more local controllers 114a,b,c to a central computer 116 is depicted in Fig. 1A. In the embodiment of Fig. 1A, gaming terminal 112a (and, typically, all gaming terminals in the group) includes a game controller board 122 which will typically include, among other items, a microprocessor and a memory such as an EEPROM storing programming and/or other information for controlling an operation of the controller board 122. Typically the hardware and software of the game controller board 122 will contain the information defining the type of game and making determinations of the win/loss local outcome (as opposed to, e.g., a progressive win/loss outcome) for the gaming terminal 112a. Because of the central role of the game controller board 122 in determining any monetary payout, it is particularly important to assure the presence of the correct software for the game controller board to avoid improper or incorrect payouts and to assure compliance with local regulatory authorities. Although it is possible to combine numerous functions onto a given board, typically numerous boards will be provided in a gaming terminal for forming a plurality of functions. In the depicted embodiment, the game controller board communicates with a communications board 124 which provides information to and, receives the information from a local controller 114 and/or central computer 116, for purposes such as monitoring use and performance, assuring compliance, performing accounting and similar functions, and facilitating implementation of progressive or other multi-terminal based games or prizes. In one embodiment, the communications board 124 includes one or more ports by which a laptop 128 or other computer may be coupled to the gaming terminal 112a for, among other purposes, downloading as described more fully below. In the embodiment of Fig. 1A, a plurality of peripheral boards 128 a-d communicate with the game controller board 122 and control various peripheral devices for performing various functions such as bill acceptor functions 132a, coin handling functions 132b, video functions 132c and audio output functions 132d. In many configurations, some or all of the peripheral and other boards 128 a-d, 124 will contain EEPROMs or other devices for storing software for running on microprocessors or other computing devices on such boards.

[0021] As depicted in Fig. 1B, a computing device such as one or more gaming terminals 1102a, 1102b may be coupled to various peripheral devices 1104a,b,c,d,e,f. Many types of peripheral deices can be provided, including the currency acceptor as depicted including, for example, printers, display screens or devices, keypads and the like. More than three peripheral devices may be provided, or fewer may be provided, the gaming terminal or other computing device may be housed in the same housing 1106a, 1106b as the peripheral devices 1104a-f, and more than two gaming devices may be used in connection with the download procedure. In one embodiment, download of information to the gaming terminals 1102a, 1102b is provided from a central computer 1108. However, it is possible to use the present invention in connection with stand-alone gaming terminals and peripherals which are not connected to a central computer 1108.

[0022] In the depicted embodiment, each gaming terminal includes a processor 1110a, 1110b, a memory 1112a, 1112b, and a communications module 1114a, 1114b. In the depicted embodiment, the processor 1110 is coupled to both the memory 1112 and the communications module 1114 and the memory and communications modules 1114, 1112 are coupled together to permit communication therebetween. In one embodiment, the processor 1110a is an Intel processor model 80960, although the invention can be used in connection with computing devices having other types of processors and in connection with gaming terminals which are controlled by devices other than microprocessors such as ASICS.

[0023] Following the establishment of the communication link 206, (Fig. 2) information is transferred from the information source to one or more gaming terminals. In one embodiment, if desired, the information is encrypted before being transmitted to the gaming terminal, particularly if the information is transmitted over a local area or wide area network to avoid the possibility of unscrupulous individuals gaining access to the information. Many types of data transfer can be used including serial and parallel transfer. In one embodiment, the information which is downloaded may include information within more than or different from information to be used for reprogramming the memory of one of the coupled peripherals. For example, the downloaded information may contain new programming information for two or more different peripherals coupled to a gaming terminal and/or may include information for programming the gaming terminal itself, in addition to, or rather than, one or more of the peripherals.

[0024] In the strict regulatory environment for many gaming devices, it is typically necessary to provide assurance that approved and proper software is provided in the peripheral and other boards, in addition to that provided on the game controller board.

[0025] Fig. 3 depicts an embodiment in which a network interface system 312 is used to connect a gaming terminal 112a, which may in turn be connected, such as in a daisy-chain fashion, to other gaming terminals 112b, 112c in a group, via a cluster controller 314 to a local server or controller 114. In the depicted embodiment, the gaming terminal 112a includes a central or controller (CPU) board 122 and one or more peripheral controller boards 128e, 128f. Although the present invention can be used in connection with a wide variety of systems and applications, in the depicted embodiment, while the gaming terminals 112 a-c would typically be located in a gaming area such as a gaming region of a casino, the local servers 114 and associated devices would typically be located in a casino local office 318. The local server 114 (and, in some embodiments, additional local servers for the same or other casinos) may be coupled, e.g. via modems 322a, 322b over a LAN line or wireless link 324 to a central computer 116 typically located in a central office 325 different from the local office 318 of the casino. As depicted, preferably each gaming terminal 112 also includes a port or other connector for coupling a computer such as a laptop computer 128 e.g. via a fiber-optic, cable or other connector 326. Thus, as illustrated in Figs. 1A, 1B and 3, transferring programming data or other information according to the present invention may be used in connection with transferring information from a remote location such as a central computer 116 or, in some cases, local server 114 to a gaming terminal 112. This procedure provides the desirable ability to download programs or other information to one, some, all or various combinations of the gaming machines 112a-c connected to the network, preferably substantially simultaneously, if desired. Such an ability is particularly useful when the target devices 112 may be relatively numerous, such as in the case of a casino or multi-casino network and/or when target devices are spread across a relatively wide region such as a plurality of lottery terminals. The download rates in such a system would typically be governed by the communication rates of the network or telecommunication system 324, 312. Also as depicted in Figs. 1A and 3, it is possible, in addition to or in place of downloading from a central computer or local controller, to download from a computer, such as a laptop 128, coupled directly to a gaming terminal. In one embodiment, the laptop computer 128 is coupled by a fiber-optic connection 326 directly to the game controller board 122. If the programming data or other information is intended for storing on a peripheral controller (end use device a-f) the data, in this embodiment, is channeled through the game controller board (in a pass-through mode) to the peripheral controller board, if desired. This procedure can be used, e.g., on a casino floor (for repairing or updating gaming terminal software) at a lottery location, or in the manufacturing process, such as in a final assembly stage. Preferably, such a download method does not require peripheral controllers 128a-f or other boards or components to be removed from the machine and can be used on machines that have no suitable network interface 312.

[0026] In addition to downloading programming or other information to gaming terminals or similar devices at a casino location, the present invention can also be used in connection with downloading information during a gaming terminal or similar device manufacturing process. Fig. 4 depicts a system usable in subassembly or final assembly downloading, e.g., in a gaming terminal manufacturing environment. Fig. 4 includes a plurality of computers such as workstation computers, network server computers, and/or PC-type computers coupled by network lines and a firewall 452 in a manner well-known to those of skill in computer network technologies.

[0027] At various stages in employing the system of Fig. 4, programming data or other information is stored in a number of different storage systems such as data bases (typically providing storage on hard drives or other well-known storage media). In the depicted embodiment, information, during program design process, is held in an engineering database 454. And software and firmware engineers use and modify such information via computers 456, 458 having at least indirect access to engineering database 454. Preferably, programs or other data which are still in the development phase are restricted to the engineering database 454 and are not stored in other databases. At some point, engineering will release the program or other information to product assurance 462 which, after review, will submit the programming or data to a gaming jurisdiction for approval. After the program or data is approved by the gaming jurisdiction, the program is copied to a production download server 466 and, preferably, stored in a released database 468. Information about the approved program is provided to a customer order system 472 and other systems such as engineering 474a and product assurance 474b. Although released programs may be provided in various forms such as on CD ROM 476a via a CD duplicator 476b, Fig. 4 also illustrates a system for downloading programming data or other information as part of a gaming terminal assembly or fabrication system. The programming or data may be loaded onto boards or other subassemblies 478, e.g. via a translator/power assembly 482 and download terminal 484 or may be loaded into one or more gaming terminals 486a,b, e.g. via connection to a communication board for downloading, in turn, to target peripheral devices or other subassemblies within the gaming terminals 486a, 486b, e.g. via a download terminal 488.

[0028] Downloading on the fabrication or assembly line, as depicted in Fig. 4 in the strict regulatory environment for many gaming devices, it is typically necessary to provide assurance that only approved and proper software and data is used in the gaming terminals, including peripheral and other boards (in addition to that provided on, e.g., the game controller board). Depending on the nature of the download, it will be advantageous, in performing assembly line downloading, to recognize or distinguish different boards, e.g. to obtain information regarding characteristics of the Board and/or its identity or history.

[0029] In the environment of the system of Fig. 4, a host device such as the download terminal 484 connects directly to the subassembly or through a test box 482 that provides the physical connection and power. A download terminal 488 can also be used to download information to boards which have already been assembled into gaming terminals 486a,b (which, provide physical connection and power and thus can be used for downloading without a test box 482). The host device 484, 488 can be network-connected as depicted or can be a standalone device. In a standalone configuration, the program information can be stored on a CD ROM 476a or other storage medium. The depicted download system can be used on the production floor as depicted or, at a service bench, e.g. for repair purposes. Preferably the download media 492a, 492b are configured to facilitate downloading of information (as opposed to, e.g., the components 312, 324 of a casino or multi-casino system which may be configured for other purposes such as data gathering, progressive game systems and the like) and can thus be configured or optimized to achieve relatively high rates of data transfer.

[0030] In order to facilitate security in downloading information, preferably so as to achieve approval for such downloading by gaming regulatory bodies, a downloading process as depicted in Fig. 5 may be used. According to the process of Fig. 5, an initial or early stage of the process involves identification. Although it may be possible to configure gaming terminals to provide identification using only software procedures (such as by providing encrypted identification data, hand shaking procedures and the like), according to one embodiment, it is preferred to provide a gaming terminal with one or more hardware-based identification components such as one or more one-time programmable and/or add-only memory devices for storing information which identifies or characterizes the gaming terminal or components thereof. In one embodiment, a gaming identification apparatus and system can be used in accordance with that described in U.S. Patent Application Serial No. ________________ (Attorney File No. 3735-924) for "GAMING DEVICE IDENTIFICATION METHOD AND APPARATUS" filed on even date herewith and incorporated herein by reference. Providing one or more gaming terminals with such identification capability means that such gaming terminals have been placed in a "download ready" configuration according to an embodiment of the invention.

[0031] As depicted in Fig. 5, in the identification phase, the source device sends a message to the target device requesting identification information 512. When downloading is intended to download information to two or more devices, the identification (and/or the download) can be performed serially, by polling each device, or a single request addressing all target devices may be sent. If the identification response is not received 514, the system enters a failure mode and no connection is established 516. The identification response which is acceptable can include many types of information, examples of which include serial or other hardware identification numbers, manufacturing ID information or codes, manufacturer name, hardware or software revision designations, date of manufacture, installation, sale, shipping and the like, date of software revision, software file size, memory addresses and the like. Preferably, a starting address for the program to be downloaded is returned. Preferably, data integrity information such as a CRC (cyclic redundancy check) signature is returned. The identification information returned in response of the request 512 is used to verify that the information to be downloaded and/or the download procedures (such as data transfer rates) are appropriate for the hardware and software present in the target devices. For example, the returned identification information can be used to verify that the gaming jurisdiction to which the gaming terminal is subject, has approved the software which is to be downloaded, that the software which is to be downloaded is compatible with software or hardware already present in the gaming terminal and the like. If, on the basis of the identification information, it is determined that the gaming terminal already possesses the download information, the download step can be skipped.

[0032] Following the identification phase, a negotiation phase includes the sending of a negotiation message 518. The negotiation message includes information which is used to enable or facilitate the download procedure. For example, it may be necessary to inform the target device of the location or locations in memory where the downloaded information is to be stored, the size of the download file, the data transfer rate, whether any special transfer procedures such as compression, decompression, encryption, decryption and the like, are required. Preferably the negotiation message includes (or is interpreted to include) a request for a response such as an approval response, from the target device or devices. For example, waiting for approval from the target device is useful to, e.g., avoid initiating a download when there is someone currently playing the game, or when the gaming terminal is in an error mode. In one embodiment, if there are current credits on a gaming terminal, the gaming terminal is assumed to be in an actively played state. As depicted in Fig. 5, if the approval or "ready" response 522 is not received, a failure state is declared and error-handling procedures are required, such as outputting a notification to an operator and/or reinitiating the download procedure. If the ready response is received, the download phase can begin.

[0033] In the embodiment of Fig. 2, the data is transmitted in a block fashion, i.e., by transmitting a predetermined number of bits of the information (such as 1024 bits) from the source to the gaming terminal 208, and then checking for errors in the block 210. As will be well-known to those of skill in the art, other block lengths can also be used. Preferably, the data is transmitted by a serial transmission protocol. In one embodiment, verification or other checking is performed to assist in detecting data transmission or other errors. A number of well-known verification or error detection schemes can be used, such as a CRC. One type of CRC check is described in U.S. Patent Application Serial No: 08/348,268, filed November 30, 1994, for "METHOD AND APPARATUS FOR VERIFYING THE CONTENTS OF A STORAGE DEVICE" (incorporated herein by reference). These or other verification or error checking schemes can be adapted for use in the present invention in a manner that will be apparent to those of skill in the art, after understanding the present disclosure.

[0034] If there are errors detected in the block of information (using, e.g. a cyclic redundancy check error detection routine, or other error detection routines well-known to those of skill in the art), the procedure loops back 212 to retransmit the block. Preferably, after some blocks have been successfully downloaded, errors in subsequent blocks do not necessarily require reinitiating the download from the beginning but, only requires downloading, anew, those blocks which have not thus far been successfully transmitted. In one embodiment, only a limited number (e.g., 3) of the re-tries are permitted before a "total error" is declared and, e.g., the device is put out of service. At the end of each block transmission, it is determined 528 whether all blocks have been transmitted 214. If not, the procedure loops back 216 to transmit the next block. Preferably, following the CRC or other error detection for each block, an overall CRC or other error check (e.g. digital signature) is performed after all blocks have been downloaded to the gaming terminal. Thus, at the end of the first portion of the procedure 202, the entire desired information will have been transmitted, block-wise, with error detection, from the information source 108 to at least one gaming terminal 102.

[0035] After all blocks have been successfully downloaded, a verification stage is initiated by sending a message to the target device (or devices) which requests certain verification information 532. In one embodiment, the verification information is based on (such as being calculated from) information stored in the target device, and preferably including at least some of the downloaded information. For example, a CRC or other digital signature based on some or all of the downloaded information can be used. Preferably, the portion of the information which is used as the basis for calculating verification information or signature is selected in a fashion that is not readily known or predictable in advance or by unauthorized persons. For example, rather than always calculating the verification signature based on information starting from a predetermined and/or unchanging starting address, it is preferred that the verification signature be calculated from a starting address which is different for different download operations and/or different terminals. In one embodiment, the starting address is randomly selected and communicated (e.g. as part of the verification request message 532). For further promoting confidence in the verification system, it is possible to use a digital signature calculation procedure which is based on a private key value which is preferably randomly selected by the source computer and used to encrypt part of the download information. In response, the gaming terminal uses a known procedure (such as a decryption calculation procedure) to calculate the verification signature. If the calculated verification signature matches the expected verification signature, verification is considered to have been accomplished.

[0036] Upon receiving a valid verification 534, the download session can be completed. If a valid verification is not obtained, a failure is declared 538 and an error-handling procedure can be initiated e.g. to provide notification to operators and/or reinitialize the download procedure.

[0037] As will be apparent to those of skill in the art after understanding the present disclosure, the particular procedures illustrated in Fig. 5 may be modified or varied in a number of ways. For example, although it is believed a high and desirable level of security is achieved when all four phases (identification, negotiation, downloading and verification) are used, it is possible to provide for downloading procedures in which one or more of the phases is eliminated or abbreviated. For example, it would be possible to provide for a somewhat secure download procedure without including a verification step. Additionally, the download method according to the present invention is not necessarily strictly limited to the order of steps illustrated in Fig. 5. For example, it may be possible to perform some or all negotiation steps prior to some or all identification steps. Some or all of the steps or phases described in connection with Fig. 5 can be used in connection with purposes other than downloading, such as using identification and/or verification transactions to query and check loaded programs e.g. by regulatory agencies.

[0038] In light of the above description a number of advantages of the present invention can be seen. The present invention makes it feasible to reduce or eliminate the need for manual operations (such as physically visiting, and opening gaming terminals, analyzing, testing and/or replacing boards or components) in connection with program updating, replacement, modification and the like, while maintaining a high level of security and reliability. The present invention provides the ability to query a gaming terminal to obtain hardware and software information for regulatory, maintenance, repair, inventory, and similar purposes. The present invention makes it feasible to download information to one or many machines at the same time. The downloaded information may be information particularly directed to peripheral devices (such as a updating a bill acceptor program) and/or may involve changing features of a game such as upgrading or adding a bonus game or similar feature to a gaming terminal. The present invention is useful in facilitating the standardization of programming or other data across a variety of gaming terminals. The present invention provides the ability to permit local customers such as individual casinos or similar locations, to download their own customized video and/or audio files (e.g., using the security features described to provide regulators with assurance that downloading of such files will not change or result in unacceptable modifications to other features of game operation). The present invention facilitates the ability of casinos, game operators, game manufacturers and the like to obtain and maintain accurate inventories on programs and board modules in gaming machines. The present invention facilitates locating or identifying particular printed circuit boards (or particular classes or types of PCBs or other components on a casino floor). The present invention facilitates the secure and reliable automatic electronic loading of programs into machines in a manufacturing (assembly line) environment e.g. based on customer orders, with reduction or elimination of manual steps in such process. The present invention facilitates querying and verifying the presence and nature of hardware or software components thereof e.g. at the end of an assembly or fabrication process such as before shipping to customers, upon receipt, and the like. The present invention facilitates a verification of installed programs e.g. by gaming and/or lottery regulatory agencies.

[0039] Providing downloading from a central computer to individual gaming terminals has a number of advantages. The download can be easily performed on a number of gaming terminals at the same time, so that the amount of time required to perform the download for all the various gaming terminals is reduced. Further, it is not necessary to have personnel physically walk from terminal to terminal, and perform a download at each terminal, so that labor costs are also reduced.

[0040] The present invention makes it possible to provide for new or additional programming for peripheral devices in a manner which is secure, less labor intensive, less time-consumptive, and less obtrusive than previous methods. The present invention makes it possible to download the programming to a plurality of gaming terminals (or other computing devices) substantially simultaneously.

[0041] A number of variations and modifications of the invention can also be used. In addition to downloading computer program information, the invention can be used to download data such as data which defines the manner in which peripherals accept currency (or, detect counterfeiting). In addition to a central computer and a portable computer hand-held device, the information may be downloaded to the gaming terminal from other devices, such as a cluster controller. When reprogramming of two or more peripherals attached to a given gaming terminal is desired, in one embodiment, the new programming information for each peripheral to be reprogrammed is downloaded to the gaming terminal and the gaming terminal begins downloading the information to the attached peripherals preferably only after all information has been downloaded to the terminal. In this way, only a single session of downloading to the gaming terminal is needed in order to provide eventual updating of two or more coupled peripherals.

[0042] In situations in which security is a concern, such as systems in which money handling occurs (e.g., gaming terminals, lottery terminals, and the like) the information may be encrypted when it is transferred to the computing device and is decrypted either in the gaming device or in one or more peripheral devices.

[0043] Preferably the transactions are controlled and monitored automatically e.g. using an information file generated from information from firmware, mechanical, configuration, jurisdiction approvals and production bill of materials. Preferably such an information file is always encrypted, although program or other download data can be compressed and/or encrypted e.g. depending upon jurisdiction requirements. In one embodiment, the information file contains a number of fields including the filename, source directory or path, destination directory, version number or other version designator, CRC value, platform code (e.g. indicating the type of gaming terminal), target code (e.g. indicating the type of peripheral (e.g. bill validator)), agency approval(s), and game name or other game indicator.

[0044] Although the procedures and steps illustrated and described in connection with Fig. 5 are believed to provide a high level of security, it is believed that security of the entire system is particularly enhanced by the combination of the identification, especially hardware and/or memory-based identification (residing on the gaming terminal or gaming terminal components) and the procedures and steps illustrated in Fig. 5, particularly when combined with an information file as described.

[0045] In the embodiment of Fig. 1B it is possible to download the information to two or more gaming terminals 102a, 102b, substantially simultaneously. However, in some configurations, it will be necessary to suspend use of the gaming terminal during the downloading process. In this case, it may not be desirable to suspend operation of all gaming terminals at the same time. Therefore, in one embodiment information is downloaded from the central computer 108 to a first subset of the connected gaming terminals (during which time, use of that subset of gaming terminals is suspended), and following downloading to that subset of gaming terminals the first set of gaming terminals will be available for normal use, and downloading to the second subset of gaming terminals will be initiated, suspending use of the second subset of gaming terminals during downloading thereof. The process is repeated for various subsets of the gaming terminals until the information has been downloaded to all desired gaming terminals. In some situations, it may be desired to download information only to some of the connected gaming terminals. For example, if the information to be downloaded is intended to thwart passing of $10 counterfeit bills, there would be no need to download the new information to gaming terminals which are connected to currency acceptor peripherals that accept only $5 bills.

[0046] In the embodiment depicted in Fig. 1B, each gaming terminal 1102a, 1102b is coupled to a central computer 1108. The coupling may be by communication link 1124, such as a common local area network connection (e.g., Ethernet, Token Ring, LocalTalk, etc.), a wide area network and the like, using any of a variety of physical media such as cables, optical fibers, radio, infrared or other wireless links and the like. The type of communication module 1114a, 1122, which will be used depends on the type of communication link which is being used and may include, e.g., commercially-available network boards and supporting software, modems, universal asynchronous receiver/transmitter (UART) devices and the like.

[0047] As noted above, in some configurations it may be necessary to suspend operation of the gaming terminal during downloading from the information source to the gaming terminals, and/or from the gaming terminal to the peripheral. In one embodiment, the gaming terminal will provide an indication of the suspended status, so that a user will have the option to move to a different gaming terminal or to await reactivation. In one embodiment, the display 103 will provide an estimate of the amount of time before reactivation of the terminal. This estimate can be based, if desired, on an empirically-derived relationship between the average download time and the number of blocks of information to be downloaded, (or other indication of the size of the information to be downloaded).

[0048] In situations in which operation or use of the gaming terminal must be suspended while the information is being downloaded to peripherals, it may be desirable to configure the gaming terminal to wait until there is an apparent idle period on the gaming terminal before commencing downloading to a peripheral. Thus, in the procedure of Fig. 2, the gaming terminal will determine whether it has been idle for at least a predetermined minimum period (such as about one minute, 220). for example, when the gaming terminal is an electronic slot machine, the gaming terminal can use at timer circuit to determine if there has been any wager placed or any handle-pull or electronic equivalent thereof) for the predetermined period. If the gaming terminal has not been idle for at least the predetermined period, the gaming terminal will optionally wait another predetermined period 221 (such as about one minute) before testing to determine if the gaming terminal is idle. Once the gaming terminal is idle, the gaming terminal can commence procedures to transmit information to appropriate peripherals 224, preferably in a blockwise fashion, with error checking.

[0049] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g. for achieving ease and reducing cost of implementation.

[0050] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. Although the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g. as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended the appended claims be construed to include alternative embodiments to the extent permitted.

Claims

1. A method for downloading data from a source to a gaming device, wherein said gaming device is subject to governmental regulations, the method comprising:

   transmitting first information to said source, identifying at least a first hardware component of said gaming device;

   verifying that said data is appropriate for said at least first hardware;

   transmitting second information from said source to said gaming device describing at least a first characteristic of said download;

   transmitting third information from said gaming device to said source indicating that said gaming device is configured to receive said download;

   transmitting said data from said source to said gaming device;

   calculating a signature based at least partially on said data and transmitting said signature to said source; and

   comparing said signature with a signature available to said source.

2. A method as claimed in Claim 1 wherein said first information includes information identifying software stored on said gaming device.

3. A method as claimed in Claim 1 further comprising outputting a message when said first information indicates said data is already stored on said gaming device.

4. A method as claimed in Claim 1 wherein said gaming device includes a plurality of circuit boards, and wherein said source is coupled to a first of said circuit boards and wherein said first information identifies hardware on at least a second of said circuit boards.

5. A method as claimed in Claim 1 wherein said gaming device includes a plurality of circuit boards which contain a non-programmable memory storing hardware identification information.

6. A method, as claimed in Claim 1, wherein said data includes data for programming at least a first programmable memory chip.

7. A method, as claimed in Claim 1, wherein said step of transmitting said data from said source to said gaming device uses a serial data transmission protocol.

8. A method, as claimed in Claim 1, wherein said step of calculating a signature comprises calculating a signature based on data stored in a memory, beginning with a random address in said memory.

9. A method, as claimed in Claim 1, wherein said step of calculating a signature comprises calculating a signature using a seed value, wherein said seed value is available to both said source and said gaming terminal.

10. Apparatus for downloading data from a source to a gaming device, wherein said gaming device is subject to governmental regulations, the apparatus comprising;

    means for transmitting first information to said source, identifying at least a first hardware component of said gaming device;

    means for verifying that said data is appropriate for said at least first hardware;

    means for transmitting second information from said source to said gaming device describing at least a first characteristic of said download;

    means for transmitting third information from said gaming device to said source indicating that said gaming device is configured to receive said download;

    means for transmitting said data from said source to said gaming device;

    means for calculating a signature based at least partially on said data and transmitting said signature to said source; and

    means for comparing said signature with a signature available to said source.

11. Apparatus as claimed in Claim 10 wherein said first information includes information identifying software stored on said gaming device.

12. Apparatus as claimed in Claim 10 further comprising means for outputting a message when said first information indicates said data is already stored on

said gaming device.

13. Apparatus as claimed in Claim 10 wherein said gaming device includes a plurality of circuit boards, and wherein said source is coupled to a first of said circuit boards and wherein said first information identifies hardware on at least a second of said circuit boards.

14. Apparatus as claimed in Claim 10 wherein said gaming device includes a plurality of circuit boards which contain a non-programmable memory storing hardware identification information.

15. Apparatus, as claimed in Claim 10, wherein said data includes data for programming at least a first programmable memory chip.

16. Apparatus, as claimed in Claim 10, wherein said means for transmitting said data from said source to said gaming device uses a serial data transmission protocol.

17. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a signature based on data stored in a memory, beginning with a random address in said memory.

18. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a signature using a seed value, wherein said seed value is available to both said source and said gaming terminal.

19. Apparatus, as claimed in Claim 10, wherein said means for calculating a signature comprises means for calculating a digital signature based on data stored in memory using a public key encryption decryption algorithm.

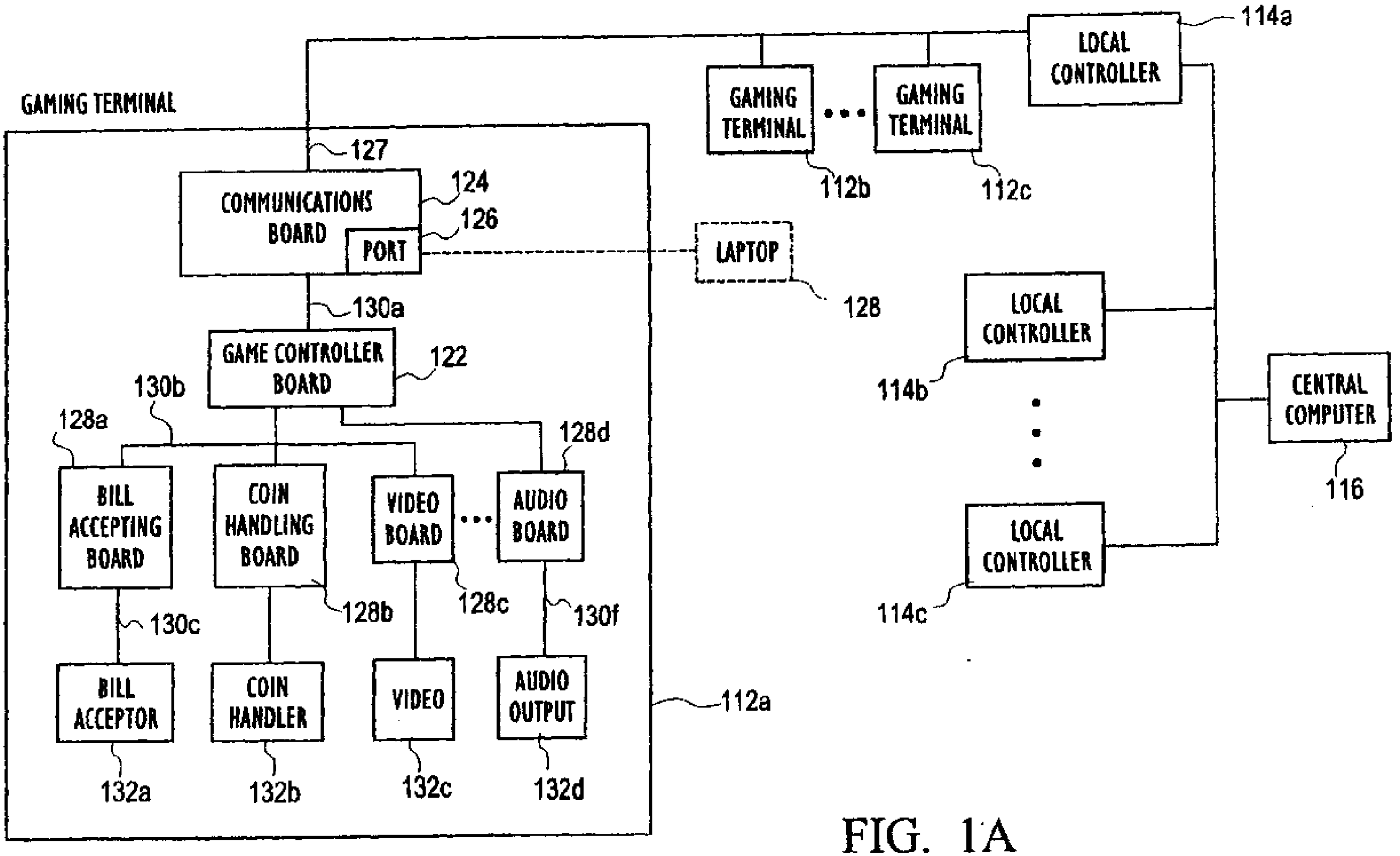

GAMING TERMINAL
127
COMMUNICATIONS BOARD
124
126
PORT
130a
GAME CONTROLLER BOARD
122
130b
128a
BILL ACCEPTING BOARD
COIN HANDLING BOARD
VIDEO BOARD
AUDIO BOARD
128d
128b
128c
130c
130f
BILL ACCEPTOR
COIN HANDLER
VIDEO
AUDIO OUTPUT
132a
132b
132c
132d
112a
LAPTOP
128
GAMING TERMINAL
GAMING TERMINAL
112b
112c
LOCAL CONTROLLER
114a
LOCAL CONTROLLER
114b
LOCAL CONTROLLER
114c
CENTRAL COMPUTER
116

FIG. 1A

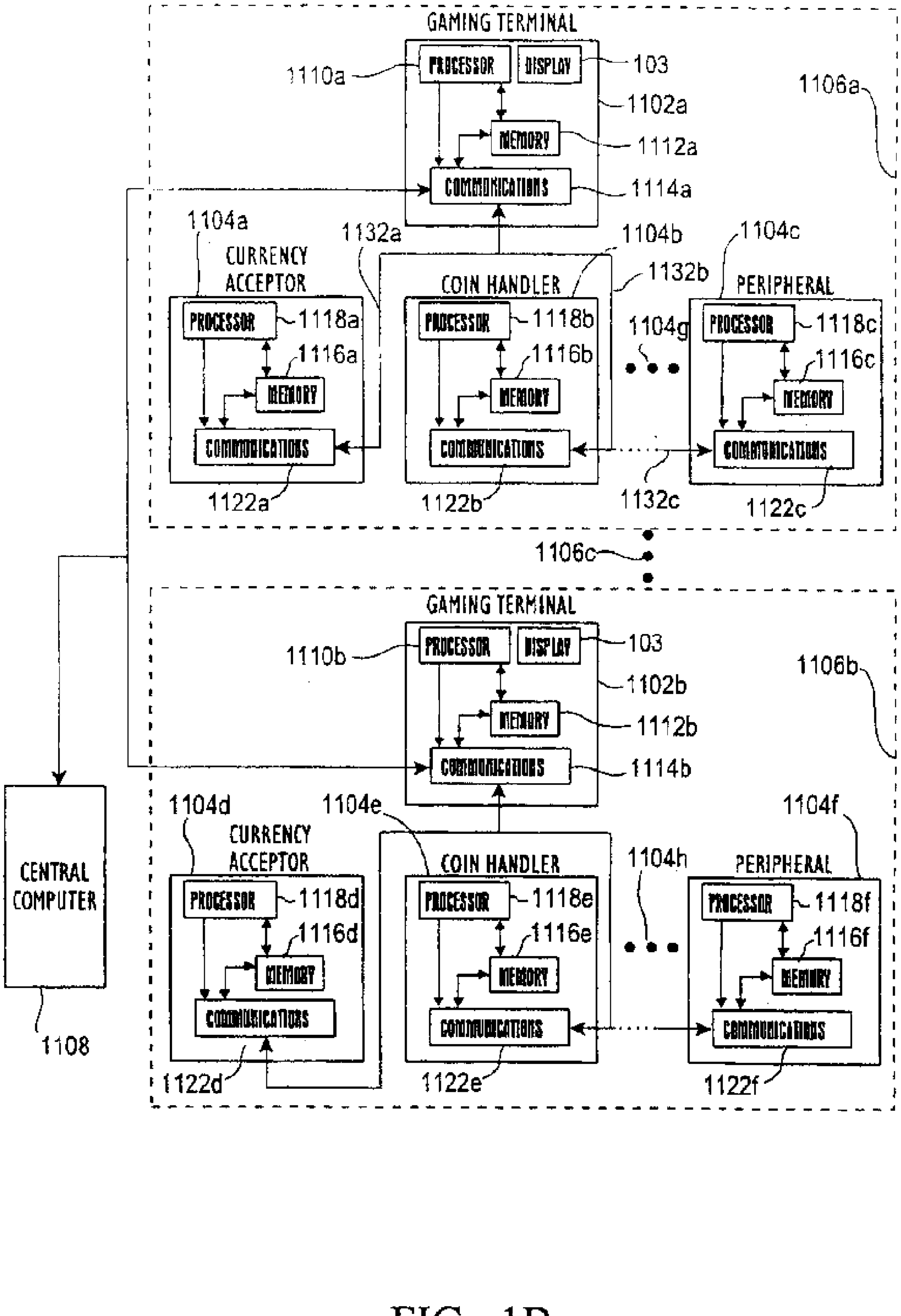

GAMING TERMINAL
PROCESSOR
DISPLAY
103
1110a
1106a
1102a
MEMORY
1112a
COMMUNICATIONS
1114a
1104a
CURRENCY ACCEPTOR
1132a
1104b
1104c
COIN HANDLER
1132b
PERIPHERAL
PROCESSOR
1118a
1116a
MEMORY
COMMUNICATIONS
1122a
PROCESSOR
1118b
1116b
MEMORY
COMMUNICATIONS
1122b
1104g
1132c
PROCESSOR
1118c
1116c
MEMORY
COMMUNICATIONS
1122c
1106c
GAMING TERMINAL
PROCESSOR
DISPLAY
103
1110b
1106b
1102b
MEMORY
1112b
COMMUNICATIONS
1114b
1104d
1104e
1104f
CURRENCY ACCEPTOR
COIN HANDLER
1104h
PERIPHERAL
CENTRAL COMPUTER
1108
PROCESSOR
1118d
1116d
MEMORY
COMMUNICATIONS
1122d
PROCESSOR
1118e
1116e
MEMORY
COMMUNICATIONS
1122e
PROCESSOR
1118f
1116f
MEMORY
COMMUNICATIONS
1122f

FIG. 1B

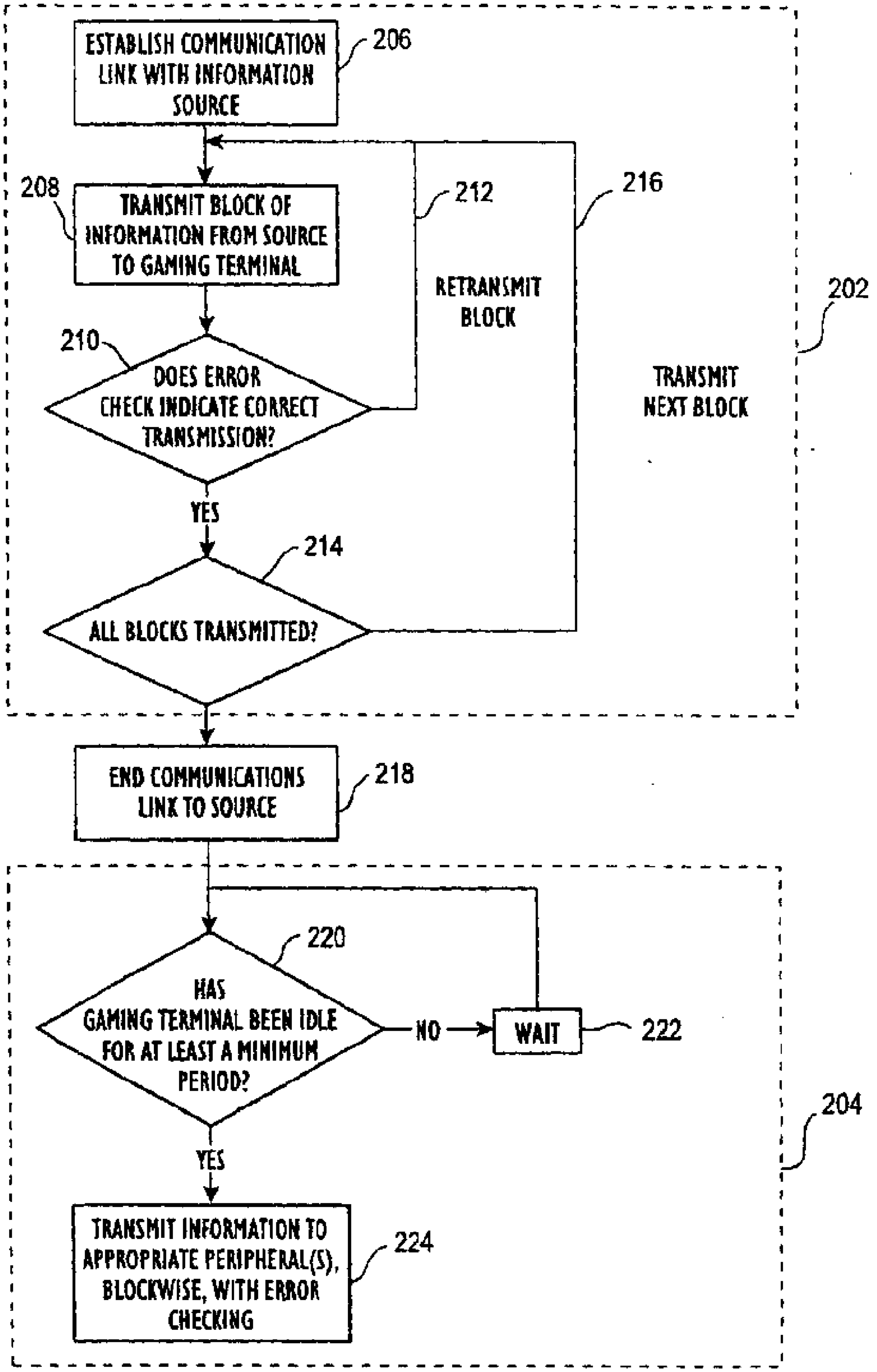

ESTABLISH COMMUNICATION LINK WITH INFORMATION SOURCE
206
208
TRANSMIT BLOCK OF INFORMATION FROM SOURCE TO GAMING TERMINAL
212
216
RETRANSMIT BLOCK
202
TRANSMIT NEXT BLOCK
210
DOES ERROR CHECK INDICATE CORRECT TRANSMISSION?
YES
214
ALL BLOCKS TRANSMITTED?
END COMMUNICATIONS LINK TO SOURCE
218
220
HAS GAMING TERMINAL BEEN IDLE FOR AT LEAST A MINIMUM PERIOD?
NO
WAIT
222
204
YES
TRANSMIT INFORMATION TO APPROPRIATE PERIPHERAL(S), BLOCKWISE, WITH ERROR CHECKING
224

FIG. 2

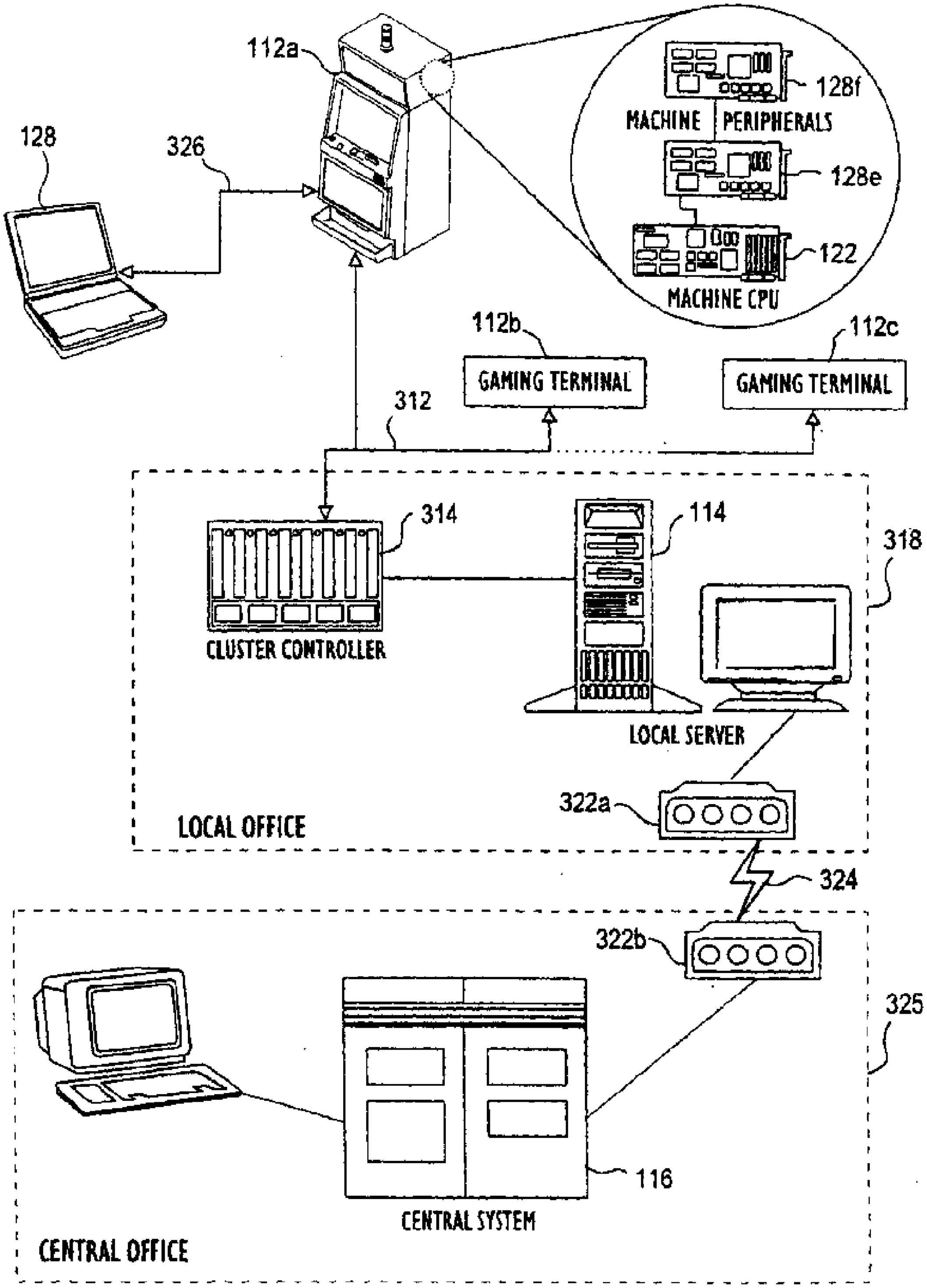

112a
128f
MACHINE
PERIPHERALS
128
326
128e
122
MACHINE CPU
112b
112c
GAMING TERMINAL
GAMING TERMINAL
312
314
114
318
CLUSTER CONTROLLER
LOCAL SERVER
322a
LOCAL OFFICE
324
322b
325
116
CENTRAL SYSTEM
CENTRAL OFFICE

FIG. 3

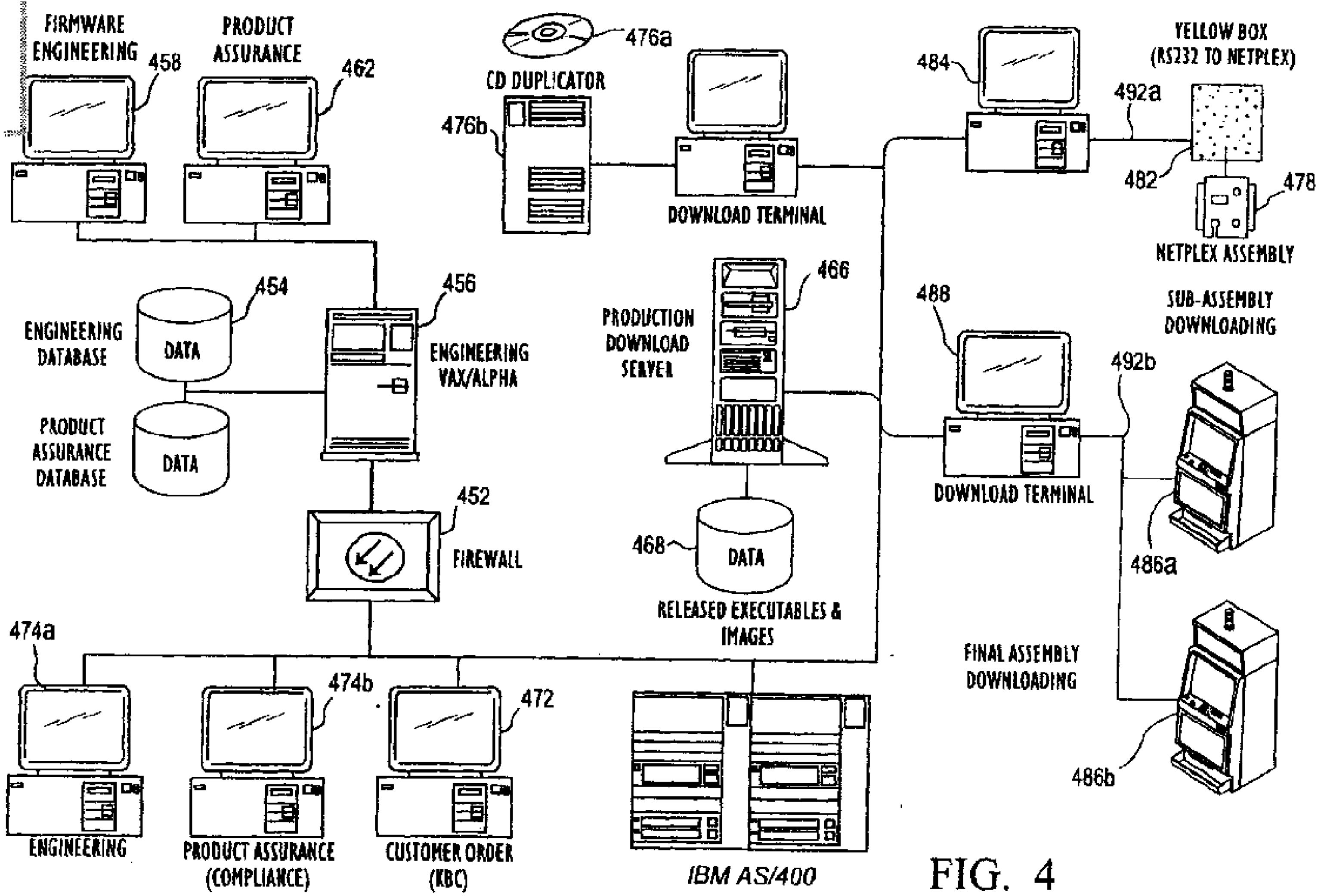

FIRMWARE ENGINEERING
458
PRODUCT ASSURANCE
462
476a
CD DUPLICATOR
476b
DOWNLOAD TERMINAL
484
492a
YELLOW BOX (RS232 TO NETPLEX)
482
478
NETPLEX ASSEMBLY
454
ENGINEERING DATABASE
DATA
PRODUCT ASSURANCE DATABASE
DATA
456
ENGINEERING VAX/ALPHA
PRODUCTION DOWNLOAD SERVER
466
488
SUB-ASSEMBLY DOWNLOADING
492b
452
FIREWALL
468
DATA
RELEASED EXECUTABLES & IMAGES
DOWNLOAD TERMINAL
486a
474a
474b
472
FINAL ASSEMBLY DOWNLOADING
486b
ENGINEERING
PRODUCT ASSURANCE (COMPLIANCE)
CUSTOMER ORDER (KBC)
IBM AS/400

FIG. 4

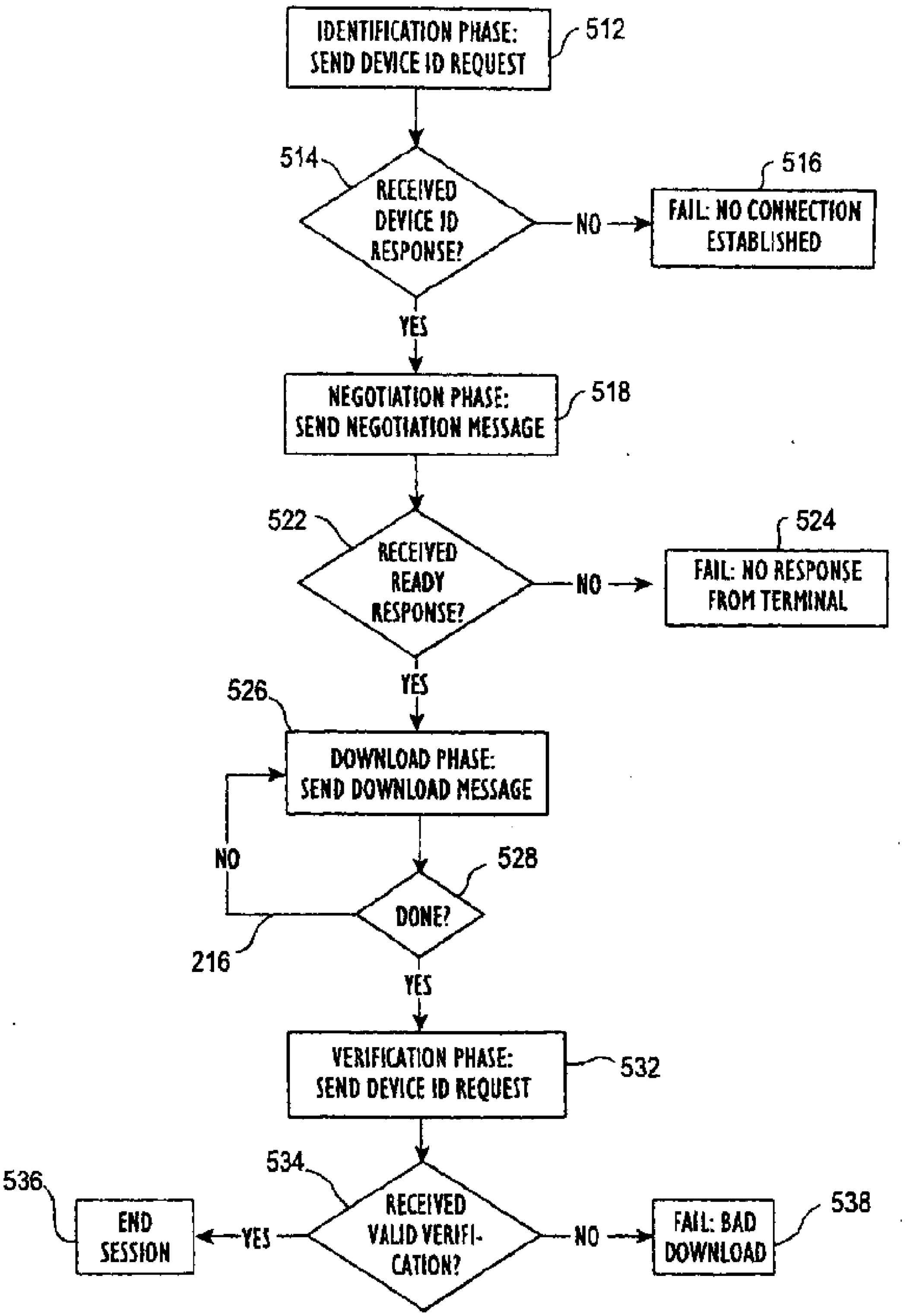

IDENTIFICATION PHASE: SEND DEVICE ID REQUEST
512
514
RECEIVED DEVICE ID RESPONSE?
NO
FAIL: NO CONNECTION ESTABLISHED
516
YES
NEGOTIATION PHASE: SEND NEGOTIATION MESSAGE
518
522
RECEIVED READY RESPONSE?
NO
FAIL: NO RESPONSE FROM TERMINAL
524
YES
526
DOWNLOAD PHASE: SEND DOWNLOAD MESSAGE
NO
DONE?
528
216
YES
VERIFICATION PHASE: SEND DEVICE ID REQUEST
532
534
RECEIVED VALID VERIFI-CATION?
536
END SESSION
YES
NO
FAIL: BAD DOWNLOAD
538

FIG. 5

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 004 970 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
06.06.2001 Bulletin 2001/23

(43) Date of publication A2:
31.05.2000 Bulletin 2000/22

(21) Application number: **99119351.7**

(22) Date of filing: **29.09.1999**

(51) Int Cl.7: **G06F 17/60**, G07F 17/32,
A63F 13/00, A63F 9/24

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **14.10.1998 US 172786**

(71) Applicant: **International Game Technology**
Reno, Nevada 89511-8986 (US)

(72) Inventors:
- **Wells, Bill**
  Reno, Nevada 89502 (US)
- **Wilder, Richard**
  Sparks, Nevada 89436 (US)

(74) Representative: **Manitz, Finsterwald & Partner**
Postfach 22 16 11
80506 München (DE)

(54) **Method for downloading data to gaming devices**

(57) Memories coupled to a gaming terminal, are reprogrammed by a method and apparatus which includes identification, negotiation, downloading and verification information from an external information source to a gaming terminal. Hardware devices are used to identify gaming terminals or components.

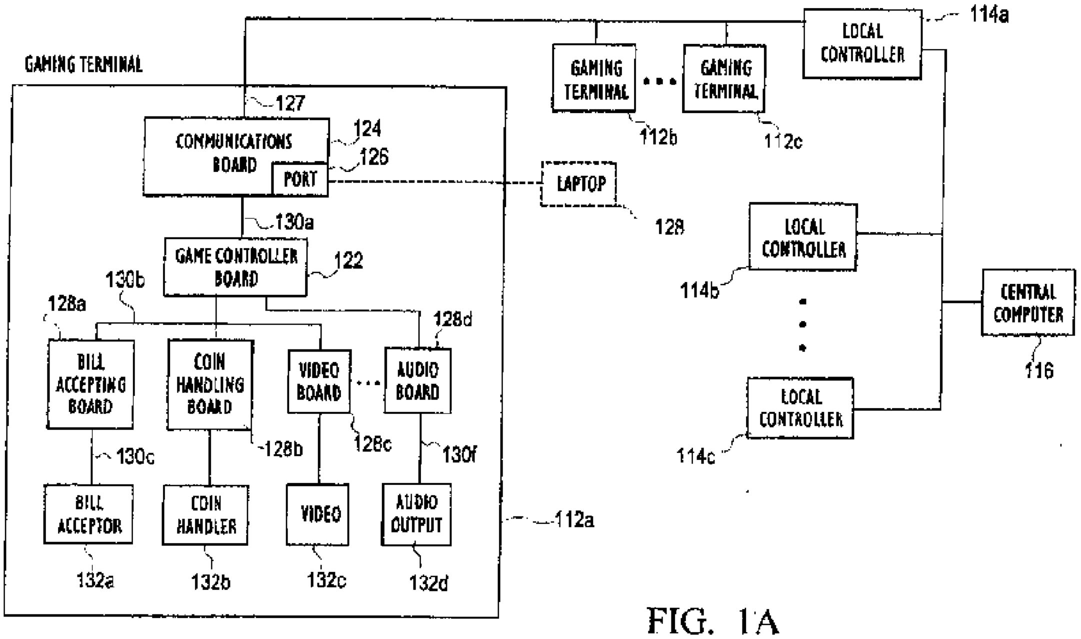


FIG. 1A

EP 1 004 970 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 11 9351

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 805 814 A (TSUDA Y ET AL) 8 September 1998 (1998-09-08) * claim 1 * ---	1,10	G06F17/60 G07F17/32 A63F13/00 A63F9/24
A	US 5 668 591 A (SHINTANI PETER) 16 September 1997 (1997-09-16) * claim 1 * ---	1,10	
A	EP 0 735 764 A (SONY TELECOM EUROP NV) 2 October 1996 (1996-10-02) * abstract * -----	1,10	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G06F
G07F
A63F
A63B
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
VIENNA	16 January 2001	Schlechter

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 11 9351

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-01-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5805814 A	08-09-1998	JP 2769789 B	25-06-1998
		JP 8112450 A	07-05-1996
US 5668591 A	16-09-1997	JP 7271697 A	20-10-1995
		GB 2288044 A,B	04-10-1995
EP 0735764 A	02-10-1996	AT 195047 T	15-08-2000
		AU 5398896 A	16-10-1996
		DE 69518144 D	31-08-2000
		DE 69518144 T	22-03-2001
		WO 9631064 A	03-10-1996

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 074 955 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.02.2001 Bulletin 2001/06

(51) Int Cl⁷: G07F 17/32

(21) Application number: 00306668.5

(22) Date of filing: 04.08.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 04.08.1999 GB 9918427

(71) Applicant: MAYGAY MACHINES LIMITED
Wolverhampton, West Midlands WV10 9NL (GB)

(72) Inventor: Powell, David John
Wem, Shropshire SY4 5NX (GB)

(74) Representative: Hackney, Nigel John et al
Mewburn Ellis,
York House,
23 Kingsway
London WC2B 6HP (GB)

(54) Data transfer devices and methods

(57) In one aspect, the present invention provides a network of game machines (506, 508, 510, 514) including a central controller (500). The central controller is useable to receive data from the game machines and also to transmit data to the game machines, for example to upload new or corrected software to the game machines. Some of the game machines may be connected to the network via radio link (512). Higher baud rates, such as 10,000 baud, are acheivable with the network of the present invention.

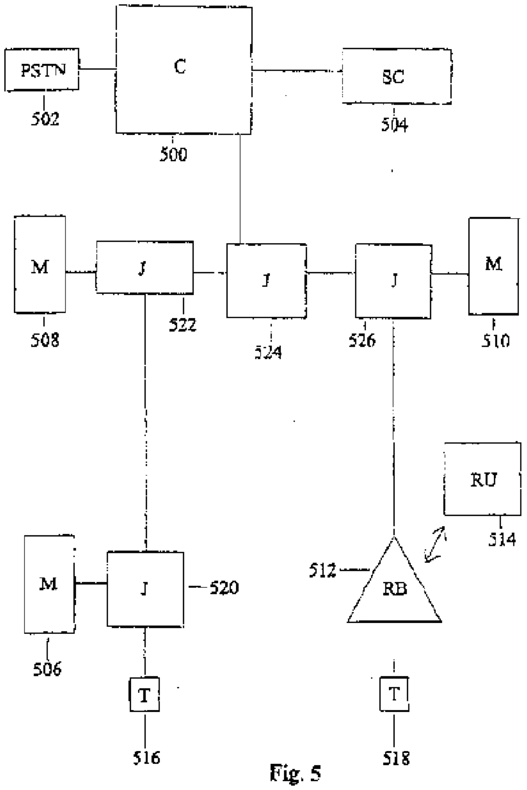


Fig. 5

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to transferring data to or from a cash or token operated machine, or between a plurality of cash or token operated machines. Each cash or token operated machine may, for example, be a vending machine or a game machine, for example a game machine used for gambling. The invention further relates to a network of cash or token operated machines, and a method of transferring data within the network.

[0002] A single site, e.g. a public place such as a public house, amusement arcade or railway station, may be provided with many cash or token operated machines, such as vending machines or game machines. In this context the term "cash or token operated machine" is traditionally used to mean any machine which delivers goods or a service upon receiving a payment (e.g. by a coin, a banknote, or a token such as a pre-purchased token or a credit or debit card), but nowadays can also include machines for which 'payment' is made remotely e.g. at a bar in a pub, and the machine is then given appropriate 'credits' and also machines which may be operated wholly or periodically without payment. The term is used in this specification in this broader sense.

[0003] Nowadays many, though not all, cash or token operated machines include a data processing unit. For example, a modern game machine conventionally includes a CPU communicating with many information output devices (lights, sounders etc.) and input devices (e.g. push buttons) based on game software which it reads from a memory device. Each coin or token operated machine at a given site may be designed, installed, or maintained by a different supplier, yet it is desirable for them to be able to communicate with a central location, to allow control, security or accounting operations to be performed centrally.

[0004] For example, it is known to connect a plurality of machines to a coordinator ("server") at a central location, so that each machine can transmit signals to the central location. The signals may include alarm signals (e.g. to indicate that a machine is being interfered with), financial information about the money taken by the machine, or information about the usage of the machine, e.g. statistical information concerning the number of plays made. The latter type of information is useful to identify when a machine is not being frequently used, to determine that it should be updated or replaced.

[0005] This data would be useful also off-site, for example to a designer of game machines, and for this reason it is known for the server to transmit data out of the network by telephone. In practise, however, the expense of doing this means that only a selection of the data available to the server is transmitted.

[0006] Conventionally the data received by the server is accumulated for later analysis. For example, in a case that it is to be transmitted out of the server by telephone, it is accumulated during the day and transmitted at night to reduce costs. Thus, if there is a power failure at the central location, the accumulated data may be lost or corrupted.

[0007] A known interface which transmits data out of a game machine (to the server) is called a "datapak". It is connected to the main processor of the game machine and receives data from the main processor at a standard rate of up to 1200 baud. No higher transmission rate is possible, due to the low power of a typical game machine processor. This interface can transmit data either by a permanent electrical connection (e.g. a wire to the server), or to at intervals a recording medium connected to the game machine by an operator.

[0008] In fact, since the concept of transferring data via an interface into a game machine has not so far been realised, local parameters are actually input by inserting an extra physical unit into the game machine, such as an extra ROM memory device or a mechanical "key".

[0009] At this point we should distinguish between game machines which merely entertain the user by sound and visual stimuli (for example video racing games), and those which provide the user with a potential financial return (i.e. gambling machines). The latter type are here referred to as "gaming machines".

[0010] An example of a game machine which is not conventionally a gaming machine is a pool table (a term used here to include a snooker or billiards table or similar). Conventionally pool tables contain little or no electronic circuitry, even the coin receiving mechanism being mechanical, so pool machines are not integrated into a site-wide accountancy system.

[0011] A popular form of gaming machine (often called a "fruit machine") employs spinning reels which are at least partly visible to a user, and generates complex electronic control signals to operate sounders and lights.

[0012] In the complex software of game machines (especially gaming machines) it is inevitable that bugs of various kinds will occur, leading to unwanted behaviour of the game machine. Some such bugs will come to light as the designer tests the software on a PC which emulates the low power processor of a game machine. The designer may eradicate these bugs by interrogating the emulator in the PC to determine exactly what has gone wrong, i.e. exactly what state the emulated the processor was in when the unwanted behaviour of the game machine occurred.

[0013] However, other bugs only become evident after extensive actual use of the game machine. For example, in the case of gaming machines, some bugs only generate unwanted effects in the event that the gaming machine reaches a rare configuration.

[0014] Furthermore, if the unwanted behaviour occurs after the game machine has been commercially released, or even during pre-release testing of the game at a commercial site, the game may acquire a commercial reputation for unreliability. In this case, even if the bug is corrected, the reputation of the game is hard to restore. For example, in the case of gaming machines, it is an unfortunate fact that many perfectly adequate gaming machines, which have been developed at great expense, are withdrawn from the market place and discarded simply because of an adverse commercial reputation caused by bug which has already been corrected.

[0015] Game software is frequently written so that it automatically produces run-time indicators of the usage and operation of the game machine, such as statistical information about how often a particular button is pushed or the values of (e.g. critical) registers at certain moments. These indicators are used when the game software is written, but once the software is installed in a real game machine it is hopeless to try to extract it using the interface since the volume of data is much greater than the capacity of the interface. Even if it were possible to transfer the indicator data out of the game machine into the network as mentioned above, it would not be practical to transmit it out of the network (e.g. to the writer of game machine software). For example, a given machine may generate 4Kbytes of indicator data every 10 minutes, and the network may contain 127 machines, so that each day more than 20Mbytes of data would be generated.

[0016] Apart from correcting bugs, there are other reasons why a game manufacturer modifies existing game software. One of these is when he releases an improved version of a game. In this case existing game machines are usually not supplied with the new game software; instead the new software is only provided in new game machines. One reason for this is the sheer technical difficulty of installing replacement memory chips in off-site (i.e. away from the manufacturer's base) game machines. Also, there are security issues involved in supplying memory chips containing proprietary software separately from game machines. Another reason for modifying software is to bring it into line with (e.g. new) legal requirements.

[0017] Security is of great importance in the installation of any cash or token operated machine, since there is a great potential (dishonest) profit available to an operative who succeeds in installing a machine incorrectly. Furthermore, an inadvertent installation error (operatives are not always highly skilled) may also lead to a loss by the operator of the machines. There is therefore a general need to control installation of machines to make it more secure and reliable, and to improve the accountability of operatives.

[0018] The present invention seeks to provide a new and useful game machine, and especially (though not exclusively) a game machine which is a gaming machine.

[0019] The invention further seeks to provide new and useful methods and devices for transferring data to and/or from a game machine or a cash or token operated machine.

[0020] The concept of transmitting game software to a game machine constitutes an independent aspect of the invention, which is a game machine including:

payment receiving means;
a writeable memory;
a processor for processing game software stored in the memory; and
an interface for receiving game software from outside the game machine, and writing it to the memory.

[0021] An operator may be able to program (usually re-program) the game machine, for example updating some or all of the game software to modify the game (e.g. to correct bugs, or to improve the pleasure of the game). For example, the game operator may be able to provide data to keep the game topical (e.g. with references to contemporary world events, personalities or other news), or with updated quiz questions.

[0022] If the manufacturer devises an improvement to the game software in the game machine (e.g. corrects a bug in the game software) he or she may be able to implement that improvement (e.g. correct the bug) by transmitting to the game machine through the interface replacement game software which includes the improvement (e.g. a debugged portion of the game software).

[0023] Within the scope of this aspect of the invention, a game machine which is a part of a network may be able to input the game software which it is to process from a central location (e.g. server)in the network, e.g. according to an instruction generated at the central location. This gives the operator of the network great flexibility, in determining which of a plurality of game machines is used to play which of a plurality of games stored at the cental location. The game manufacturer may be able to update the game software at the central location, for subsequent transmission to game machines.

[0024] Indeed, it is possible for new game software to be transmitted (e.g. from the central location of a network) whenever the game is used. That is, a plurality of games may be stored in a central location in communication with the central location, and an operator or the user may select one game which is then transferred to the machine for the user to play.

[0025] In a further aspect, the present invention provides a method of reprogramming a game machine according to this aspect of the invention by transmitting game software to the game machine.

[0026] In an aspect the invention proposes a game machine, having a data interface for transferring data into and/or out of the game machine or cash or token operated machine.

[0027] Preferably the interface permits a data transfer rate which is e.g. at least 10,000 baud, at least 100,000 baud, or at least, 1,000,000 baud. Preferably the baud rate is not over 10,000,000

[0028] Preferably, the interface transmits information both into and out of the machine.

[0029] In the case that the interface transmits information out of the machine, the interface preferably transmits indicators characterizing the operation of the game software. The indicators may include any one or more of (i) data characterizing when the machine is used, (ii) data (e.g. statistical data) on the timings at which the user inserts money or operates information input devices (e.g. buttons), (iii) the state of the display and/or sound generated by the machine at times when the user inserts money or operates information input devices, (iv) financial information concerning the cash or tokens received by the machine, and (v) data concerning the internal running of the game software (e.g. values stored in particular registers).

[0030] Preferably, enough information is transmitted out of the interface to reconstruct the play of the game. For example, at least enough information may be transmitted to reconstruct the display generated to a user of the machine and his reactions to that display. More preferably, the transmitted data allows identification of bugs in the software or other portions of the software which should be improved.

[0031] The information may be transmitted in real time (as the game is played) or stored in the memory and transmitted in bursts, e.g. with a predetermined timing (e.g. periodically) or in response to a triggering signal received from outside of the machine, e.g. through the interface.

[0032] The possibility of transmitting large amounts of data into a game machine or cash or token operated machine makes it possible to conceive of a possibility not envisaged in the literature, of transmitting not just parameters into the game machine but actually applications (that is game software consisting of instructions).

[0033] As a separate independent aspect of the invention, the interface may include data storage means e.g. memory. The data storage means may also have a battery backup power supply or other suitable power means in order to retain data in the data storage means in the event of a mains power failure. In this way data relating to, for example, the operation of the interface e.g. the protocols to be used, can be stored and updated as necessary.

[0034] Further independent aspects of the invention relate to using radio communication to transfer data into and/or out of a cash or token operated machine (especially a game machine), or between networks of cash or token operated machines. In some embodiments radio communication gives the advantage of secrecy, while in some embodiments it gives the advantage that one or more game machines can be easily integrated into a network (e.g. on a single site). In some embodiments, the radio communication device is a mobile telephone which can exchange data with a conventional mobile telephone network.

[0035] Specifically, in a third aspect, the invention provides (e.g. a cash or token operated) game machine including:

payment receiving means
means for analysing usage of the game machine to generate usage data; and
a radio communication device for transmitting signals carrying said usage data out of the machine.

[0036] In a first embodiment, the data may be transmitted to a radio receiver on the same site, so that the game machine can be integrated with the data collection at that site. That is, one or more machines according to the third aspect of the invention may compose part of a system which includes a collating device (server) which receives radio signals from the machines and collates them.

[0037] For example, the game machine may be a pool table, such as a pool table which is not controlled by a processor. However, even though the game machine is not controlled by a processor, the means for analysing the usage of the game machine may include device(s) to monitor the usage of the game machine (e.g. a measuring device, such as an optoelectronic device, to measure when coins are inserted into a mechanical coin receiving device (so that the total take of the machine can be transmitted out of the machine), or to indicate the fall of the final ball of the game). The game machine may include a processor to analyse the usage data before it is transmitted out of the game machine.

[0038] This aspect of the invention can be particularly useful for game machines (e.g. a pool table) which are not powered by mains electricity or, even if they are capable of being powered by mains electricity, are situation in a location to which it is inconvenient to supply mains power. For such machines, in the absence of mains power it may be difficult to operate data transfer apparatus in accordance with other aspects of the invention. Often it will be more convenient to transfer data using a radio communication device in accordance with this aspect of the invention.

[0039] In a second embodiment, the data may be transmitted off-site, for example to a manufacturer of game machines.

[0040] Preferably, as in the first aspect of the invention, the game machine of the third embodiment includes a processor running game software.

[0041] In either embodiment, the communication device may just emit a certain signal once whenever the game software is run. Thus, an operator (on site or off site) can count how often the game is played by counting the emitted signals. Alternatively, the game machine might include means for storing information on how often the game is played and the communication device may transmit this stored information, for example periodically or in response to an interrogation signal (e.g. received by the radio device).

[0042] Alternatively or additionally, the data may be data (indicators) concerning the state of the game. For example, the data may be sufficient that an operator can use the signals to follow the play of the game from a remote location. A further possibility is that the data may describe any problems which have arisen during play (e.g. due to software bugs), and the configuration (internal state) of the game machine at that time, so that the receiver of the data can attempt to deduce the reason for the problem. In any of these cases, the receiver of the data may monitor features of the play, even if the game machine is located out of the premises of the manufacturer, for example during commercial testing of the game machine, or even once the game machine has been commercially released.

[0043] In fact, a fourth independent aspect of the present invention is a method of monitoring a game machine according to the third aspect of the invention, by receiving and analysing signals transmitted from it.

[0044] The communication device of the machine of the third aspect may also be capable of receiving radio signals. These signals may be signals to control the game machine. For example, the signal may be a signal activating the game machine (e.g. transmitted to the game machine to turn it on), or a signal which enables the game machine to indicate that the user has paid to use it. In this case the payment receiving means may just be a register recording that the enablement signal has been transmitted.

[0045] In a further example, the game apparatus may be arranged to run one of a number of games according to a signal received by the game machine via an interface.

[0046] Alternatively, and preferably, the signals include game software, for example as described above. This may, for example, be done even without the knowledge of the keeper of the game machine. Thus, de-bugging is possible without even making public the existence of the bug.

[0047] The third aspect of the invention has been explained above in relation to transferring data by radio to or from a single game machine. However, alternatively there may be a plurality of game machines, arranged into one or more networks of electrically connected machines. Each network may optionally also include other components, such as other cash or token operated machines or data collators and storage devices. The one or more networks may transfer data off-site or between themselves by radio. In the latter case this means that even physically separated networks at a single site (e.g. on different storeys of the same building) can be coordinated.

[0048] Specifically, in a fifth aspect the invention may provide a network of game machines (e.g. cash or token operated machines), each including:

payment receiving means; and
means for analysing usage of the machine to generate usage data;

said machines being arranged in one or more groups of electrically connected groups, each group being provided with a radio communication device for receiving and/or transmitting signals carrying said usage data (e.g. off-site or to another of the groups).

[0049] Sixth, seventh and eighth aspects of the invention relate to transferring data into or out of a game machine or a network of game machines by providing them with an interface for communicating with a physical recording medium. In the case of the sixth and seventh aspects of the invention, the data is input to the game machine or network of game machines to configure the machine(s). Preferably, the data is accompanied by data identifying the operator (the holder of the recording medium).

[0050] Specifically, in a sixth aspect, the invention proposes that a (e.g. cash or token operated machine) game machine having payment receiving means includes a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the machine.

[0051] Preferably, the recording medium is a smart card, and the reader interface is a smart card reader device for reading data from the smart card.

[0052] By means of the invention, an operative can install a new game machine by supplying it and then allowing it to read configuration data from the recording medium to configure it. Since the data is read from a recording medium, the installation is relatively simple compared to inserting extra mechanical components into the machine.

[0053] Furthermore, the recording medium (smart card) preferably includes identification data identifying the holder of the recording medium. The game machine may store this identification data, so that in the future it is possible to determine which operative set up the machine. Alternatively or additionally, if the game machine is part of a network of game machines, it may communicate the identification data out of the game machine into the network, so that (e.g. at a central location) the identity of the operative may be checked and optionally recorded. Since the operative must supply the identification data in order to complete the set-up of the game machine, the system is open to less abuse than the conventional system described above. Furthermore, the identification data can be used to check that the correct recording medium (smart card) is being used, thus reducing the chance of an error being made in set-up.

[0054] In a further aspect, the invention proposes a network of game machines, each machine having payment receiving means and being electrically connected to at least one coordinating device (e.g. at a central location of the site), the coordinating device including a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the network.

[0055] The recording medium read by the coordinating device may carry the local information about the site, for example the price per unit of the game. The coordinating unit may transfer this data to the machine(s), for example when the machine is first installed or when the machine is first turned on. Thus, the recording medium read by the coordinating device may function as a key for the control of the entire network.

[0056] Preferably the recording medium read by the coordinating device contains identification data, so that it can be checked that it is the correct recording medium for that network. This makes it more difficult to incorrectly configure the network by using the recording medium of another site.

[0057] Preferably, the sixth and seventh aspects of the invention are combined, so that both a coordinating device (server) of a network has an interface for reading from the first recording medium, and at least one cash or token operated game machine includes an interface for reading data from a (e.g. respective) second recording medium. The installation of a new game device can then involve a coordinated process in which the operative inserts a second recording medium into the game machine(s), which transmits information to the coordinating device, to identify the type of game machine which has been inserted. The coordinating device reads local information from the first recording medium, and transmits it back to the game machine to configure it to operate according to the local standards.

[0058] The eighth and ninth aspects of the invention each relate to methods of handling reliably and economically within a network a high volume of generated data, such as the volume of data which can be generated by one or more game machines according to the first aspect of the invention.

[0059] In an eighth aspect, the present invention proposes a network of:

> one or more game machines, each machine generating data characterising the operation of the machine;
> at least one collating device receiving said data from the machines and including a data storage device, the collating device further including a writer interface for transferring the data to a recording medium.

[0060] The present invention makes it possible to transfer large amounts of data economically out of a network by incrementally, e.g. periodically, transferring it to a recording medium. Thus it makes possible for example economical transmission out of the network of the volume of indicator data which one or more game machines according to the first aspect of the invention can transmit into the network, and which may then optionally be sent to a producer of game software.

[0061] In other words, in the eighth aspect of the invention the machines are preferably game machines according to the first aspect of the invention. That is, in contrast to a conventional game machine which transmits such a small amount of data into a network that telecommunications may be adequate to transmit the data out of the network, even if the game machines in the eight aspect of the invention are capable of transmitting a high level of data into the network (e.g. a game machine according to the first aspect of the invention) a network according to the eighth aspect of the invention is capable of transmitting it out.

[0062] In a ninth aspect, the present invention proposes a network of:

> one or more game machines, each machine including a writable memory device and each machine generating data characterising the operation of the machine;
> at least one collating device in two-way communication with the machines and including a writable memory device, the collating device receiving said data from the machines, writing data to its memory device, and re-transmitting data to the machines to store it in the respective memory devices of at least one (preferably more than one) of the machines, whereby if there is a power failure to one of the machines or to the collating device the data is not lost.

[0063] Preferably, the collating device also processes the data, and it is the processed data which it stores in its own memory device and stores in the respective memory devices of at least one of the machines.

[0064] Alternatively, instead of or in addition to the network including the collating device (and the data storage device associated with the collating device), one or more of the machines may each include data storage means (e.g. memory) for storing the type of data which would otherwise be transmitted on the network. In effect the data storage means can act as a buffer to store data relating to certain events or a certain time period, for example for later or periodic transmission over the network.

[0065] The feature of the data storage means is also particularly advantageous where some or all of the machines each include an external data port via which data can be accessed other than over the network.

[0066] In practical embodiments, this may be used for manual collection of the data e.g. at periodic intervals. For example, someone could connect to the data port a data collection device e.g. a hand-held unit and go to each machine in turn collecting the appropriate data. The data thus stored by the hand-held unit can then be processed remotely. In some embodiments, the data collection unit may also write data to the data storage means, for example, the date and time at which the data is collected. The internal clock of the data collection means may of course not be consistent with the clock of the network and so it could cause problems if these two clock times were confused. Accordingly, the data storage means preferably records the clock time of the hand-held storage device and compares it to the current clock time according to a network.

[0067] A further aspect of the present invention relates to the architecture and/or topology of the network used to link the machines. More particularly, the network includes a plurality of machines and each machines is linked to at least one other machine. Preferably only one of the machines (or one point on the portion of the network connecting the machines to each other) is in turn also connected to a controller e.g. a server. The server may be connected e.g. via a PSTN, ADSL or ISDN link to an external network. As described previously, the server may then be used to read and/or write data to each or all of the machines. This topology enables improved data communication as compared to the prior art topology.

[0068] As mentioned previously, one or more of the machines in the network may in fact be substituted by radio communication means for radio communication with equipment not directly included in the network. Preferably the machines of the network are connected in a line i.e. each of the machines is connected to only two other machines with the exception of the two machines one at each end of the network which are of course connected to only one machine. Preferably the or each end of the network is terminated in a suitable impedance. Preferably each machine receives all of the data being transmitted on the network. In a separate embodiment the machines may be connected in a loop i.e. each machine is connected to only two other machines.

[0069] As a separate aspect, one or more of the machines in a network may each include backup power supply means e.g. one or more batteries. The purpose of such a backup power supply is of course to enable some or all of the machine to continue to be able to function in the event of a mains power supply failure. Preferably the network controller includes power management means for managing the power consumption of a machine connected to the network in the event that the machine is disconnected from mains power. Preferably in the event of such a disconnection, the machine affected sends a suitable notification signal to the controller. The controller may then instruct the machine to terminate certain functions whilst maintaining other functions in order to conserve power consumption. Typically, the functions which will be maintained will be those relating to monitoring the security of the machine e.g. a tamper alarm etc.

[0070] The term "payment receiving means" is used throughout this document to include a coin receiving device (e.g. having a coin authenticating function), a banknote receiving device, a token receiving device which receives a pre-purchased token representing money or a credit or debit card (which is here regarded as a kind of token). In fact, it includes any device by which the user can pay to use the machine, or by which a signal is transmitted to the machine (e.g. through a network) to indicate that the user has paid to use the machine.

[0071] Preferably the game machine of the invention is a gaming machine, and includes payment dispensing means, such as coin dispensers, token dispensers, or means for transmitting a signal to an external device which acts on the signals to make a payment to the user. The game machine preferably includes information output devices (lights, sounders, spinning reels, etc), and information input devices (buttons, arms, pedals, etc).

[0072] It will be appreciated that while the above aspects have been explained in relation to game machines, preferably each or all are also applicable more generally to coin or token operated machines.

[0073] Any of the above aspects of the invention may be used in conjunction with any or all of the other aspects.

[0074] Embodiments of the invention will now be described, for the sake of example only, by reference to the accompanying figures, in which:

Fig. 1 shows schematically a first game machine according to the invention;

Fig. 2 shows schematically a network of cash or token operated machines;

Fig. 3 shows a second game machine according to the invention.

Fig. 4 shows a prior art network;

Fig. 5 shows a second embodiment of a network of the machines according to the present invention.

[0075] A first embodiment of a game machine 1 according to the invention is shown schematically in Fig. 1. It includes a coordinator unit (gate) 3 which coordinates transfer of data between a memory device 5 and a processor 7 (which may in fact consist of several physically separate processing units). The memory 5 includes at least a component of writeable memory.

[0076] The processor may for example be a Hitachi 32bit microprocessor from the family known as Super "H". The gate 3 may be a custom gate array. This gate is also able to provide a high speed multi element interchange interface for external I/O devices. The interface runs at 571KHz and can fully service all external resources in 128uS. The main system processor 7 has no connection with this process, all transfers are performed by the ASIC and data is read or written directly to/from the main battery backed static RAMs.

[0077] The game machine also includes a payment receiving device 9 (e.g. a coin receiver), and output devices such as sounders and lights (not shown). These may all be controlled by the processor 7, for example via the coordinator unit 3.

[0078] The game machine further includes a smart card reader 15, which can read data from a smart card inserted into it. The smart card data includes set-up data, for example setting a first configuration of the game machine, and/or portions of game software. The smart card data further includes identification data identifying the holder of the smart card.

[0079] The game machine further includes an interface 17 for interfacing the game machine with leads 19 which connect the game machine to a coordinating/collating device ("server") 21 (described below in relation to Fig. 2).

[0080] The coordinator device can read data (e.g. game software) from the network through electrical leads 19 and transfer it into the memory 5 without interaction by the processor 7 (e g. on a time scale which is independent of the clock speed of the processor 7).

[0081] On receiving data from a smart card using the reader 15, the game machine can exchange data via the interfaco 17 with the rest of tho network, for oxamplo to send information to tho coordinating dovico 21 to identify the game machine. In particular, the identification data on the smart card may be stored within the memory device 5 and/or in the data storage device which is part of the coordinating device 21.

[0082] The game machine further includes a radio receiver and transmitter, including an aerial 11 and signal processing device 13.

[0083] The coordinator 3 may transmit data (e.g. statistical data) out of the game machine using radio signals transmitted by the aerial 11. It may receive data via radio signals received by the aerial 11. These radio signals may include control instructions (e.g. when the game machine is turned on or off) and/or game software. The coordinator 3 can transmit the game software into the writeable portion of the memory 5.

[0084] The aerial 11 and processor 13 may, in fact, be technologically compatible with a mobile telephone network. Thus, an operator of the game machine may be able to transmit or receive radio signals using a conventional mobile telephone network, for example by dialling a telephone number associated with the game machine. Similarly, the radio apparatus 11,13 may be able to dial up the game machine operator by transmitting a dialling request to a conventional mobile telephone network.

[0085] Turning to Fig. 2, a network of coin operated machines is shown, including a plurality of game machinos 1 illustratod in Fig. 2. Tho notwork further includes an aerial 23 and corresponding signal processor 25 for receiving data transmitted from an on-site game machine which is not in electrical contact with the network (as described below in relation to Fig. 3), and a cash or token operated machine 27 which is not a game machine. In the figure, the various machines are shown connected to the coordinating device 21 by a single cable 19 arranged along a closed path, but there may in fact be many cables arranged in other formations (see for example Fig. 5).

[0086] The coordinating device 21 includes a processor 22 a data storage device 29, a smart card reader 31, a connection to a telephone line 33 and an aerial 35.

[0087] The coordinating unit 21 receives various data from the game machines 1 via the cables 19. For example, it may receive set-up data transmitted by the game machines from the smart card operator. At the same time, the coordinating device 21 may receive data identifying the game machine 1, for example data characterizing its requirements. Also, at this time the coordinating device 21 receives via the cables 19 from the game machine(s) identification data from a smart card read by the game machine. The coordinating unit 21 may store this identification data in a storage device 29, or alternatively transmit it (e.g. by telephone line 33), to the supplier of game machines for example.

[0088] A smart card stored on-site can be read by the reader 31 to insert a local information into the network. The coordinating device 21 may transmit this local information via tho cablos 19 to machinos 1, 27, 40.

[0089] Information may bo sont out of tho notwork, o. g. to an adjacent network of equivalent form, using optional ra[illegible]erial 35.

[0090] [illegible]en it is decided to update the software in the gam[illegible]chines, this can be done by a telephone signal tra[illegible]mitted by the supplier of games software along telephone cable 33 to the coordinating device 21, which re-transmits it along cable 19 to the game machine 1, where the game software is transferred through interface 17 and coordinator unit 3 to the memory 5.

[0091] In use, the game machines 1 generate large volumes of data (e.g. at least tens of Kbytes), and this is transmitted (e.g. after a temporary storage in the memory device 5) via the interface 17 to the network through cable 19, so that it is received by the coordinating device 21, optionally collated (e.g. formatted and analysed), and stored in the storage device 29. Accumulated data may be transferred using a data writing device 37 to a recording medium such as a diskette or zip disk, so that the recording medium can be transferred to the writer of games software to enable improvements to be made. Although as shown above, the smart card reader 31 and the writer 37 are separate units, it is alternatively possible to form them as a single unit which both reads from and writes to a recording medium.

[0092] The coordinating device (e.g. periodically) backs up the data stored in the storage device 2a by copying it to at least ono of tho gamo machinos 1 to bo written into the memory 5. Thus, evon if the memory devices 29,5 are volatile the redundancy of storage means that the network as a whole is less vulnerable to loss of power (or other influences) at one or more points in the network. Optionally, the storage device 29 can be omitted and the system can rely entirely on the memory devices 5 of the game machines 1.

[0093] The game machine shown in Fig. 3 is a machine such as a pool table in which the game is not controlled (or only to a limited extent) by a processor. A measuring device 110 (e.g. an optical switch for counting coin input) is provided for obtaining measurements about the insertion of money into a payment receiving device (not' shown) or for measuring characteristics of the play. The measuring device 110 transfers data to a processor 117 which processes it, and transmits it to a signal processor 113 for generating a radio signal to be transmitted from the game machine using aerial 111.

The signal transmitted from aerial 111 is received by the aerial 23 of the network (shown on Fig. 2), decoded by the unit 25 and transmitted to the coordinating unit 21. Thus, the coordinating unit 21 is able to derive information (e.g. financial information) from the game machine 40 without a wire connection existing between the game machine 40 and the coordinating unit 21.

[0094] Fig. 4 shows a prior art network used to connect four gaming machines 400. Each of the gaming machines 400 is connected directly to a server 402 which in turn may be connected to a telephone line for transmission of data out of the network. Such a network typically had a maximum transmission rate of 1200 board.

[0095] By way of contrast, Fig. 5 shows a second embodiment of a network according to an aspect of the present invention. A central controller or server 500 is connected or connectable to an external network 502 (for example a PSTN or ISDN link). The server 500 also includes a smart card device 504 for reading or writing data to a suitable smart card.

[0096] Three game machines 506, 508 and 510 are connected to the network and thereby indirectly connected to the controller 500. As will be seen, machine 508 is effectively connected to both machines 506 and 510. Machine 506 is effectively at one end of the network and is therefore connected only to machine 508. Machine 510 is connected to machine 508 and a RF base station 512 which can be considered to take the place of a further fourth machine. Base station 512 is effectively at the other end of the network and is therefore only connected to machine 510.

[0097] Associated with RF base station 512 is an RF unit 514 which may be located in a further machine, possibly one which does not have ready access to mains power for example a pool table. Effectively therefore the pool table or other remote machine is incorporated into the network via an RF link between the base station 512 and the unit 514.

[0098] As will be seen from Fig. 5, the network can be considered to be in a "horseshoe" arrangement and the respective ends of the network are terminated by impedance terminations 516, 518. The impedance of terminations 516, 518 may be selected or adjusted so as to minimise reflections in the network.

[0099] In fact, as will be seen in Fig. 5, the machines 506, 508, 510 and RF base station 512 are not connected directly to each other by single cable runs but instead are interconnected via a series of junction boxes 520, 522, 524 and 526. Machines 506, 508 and 510 are associated with junction boxes 520, 522 and 526 respectively, whilst commander 500 is connected to the remainder of the network via junction box 524.

[0100] The embodiments above have been given for the sake of example only, and various modifications are possible within the scope of the invention.

Claims

1. A game machine including:

   payment receiving means;
   a writeable memory;
   a processor for processing game software stored in the memory; and
   an interface for receiving game software from outside the game machine, and writing it to the memory.

2. A network including a plurality of game machines according to claim 1 and a server for transferring the game software to the game machines.

3. A network according to claim 2 wherein the server is provided with a plurality of games selected ones of which are transferrable to selected machines for the users to play.

4. A cash or token operated game machine, having a data interface for transferring data into and/or out of the machine at a data rate of at least 10,000 baud.

5. A machine according to claim 4 wherein the interface is usable to transmit indicators characterizing the operation of the game software including any one or more of (i) data characterising when the machine is used, (ii) data on the timings at which the user inserts money or operates information input devices, (iii) the state of the display and/or sound generated by the machine at times when the user inserts money or operates information input devices, (iv) financial information concerning the cash or tokens received by the machine, and (v) data concerning the internal running of the game software.

6. A machine according to claim 4 wherein the interface is usable to transmit enough information to reconstruct a play of the game.

7. A machine according to claim 5 or claim 6 wherein the information is transmittable in real time (as the game is played) or is stored in a memory and transmitted periodically or in response to a triggering signal received from outside of the machine.

8. A machine according to any one of claims 4 to 7 wherein the interface includes data storage means and a backup power supply means in order to retain data in the data storage means in the event of a mains power failure.

9. A cash or token operated or game machine including:

   payment receiving means;

means for analysing usage of the machine to generate usage data; and
a radio communication device for transmitting signals carrying said usage data out of the machine.

10. A machine according to claim 9 which is not powered by mains electricity.

11. A machine according to claim 9 or 10 including means for storing information relating to operation of the machine and wherein the communication device is usable to transmit this stored information periodically or in response to an interrogation signal.

12. A machine according to claims 9 to 11 wherein the communication device is also capable of receiving radio signals.

13. A network including a machine according to any of claims 8 to 11 and a radio receiver and/or transmitter for receipt and/or transmission of radio signals to/from the machine.

14. A cash or token operated machine or game machine including a reader interface for reading data from a physical recording medium, the data including configuration data for determining operation of the machine.

15. A machine according to claim 14 wherein the recording medium is a smart card, and the reader interface is a smart card reader device for reading data from the smart card.

16. A machine according to claim 14 or 15 wherein the recording medium includes identification data identifying the holder of the recording medium.

17. A network including a plurality of cash or token operated machines being electrically connected to at least one coordinating device, the co-ordinating device including a reader interface for reading data from a physical recording medium, the data including configuration data.

18. A network including one or more cash or token operated machines, each machine including:

means for generating data characterising the operation of the machine;
at least one collating device receiving said data from the machines and including a data storage device, the collating device further including a writer interface for transferring the data to a recording medium.

19. A network according to claim 18 wherein each machine includes a writeable memory device and the collating device is in two-way communication with the machines and includes a writeable memory device, the collating device including means for receiving said data from the machines and writing data to its memory device, and means for re-transmitting data to the machines to store it in the respective memory devices of at least one of the machines, whereby if there is a power failure to one of the machines or to the collating device the data is not lost.

20. A network according to claim 18 or 19 wherein some or all of the machines each include an external data port via which data can be accessed other than over the network.

21. A network including a plurality of game machines, wherein each machine is linked to at least one other machine and only one of the machines is in turn connected to a controller.

22. A network according to claim 21 wherein each of the machines is connected to only two other machines with the exception of two machines one at each end of the network which are connected to only one machine.

23. A network according to claim 22 wherein the or each end of the network is terminated in a suitable impedance.

24. A network according to claims 21 to 23 wherein each machine receives all of the data being transmitted on the network.

25. A network according to claims 21 to 24 wherein one or more of the machines includes backup power supply means.

26. A network according to claim 25 wherein a network controller includes power management means for managing the power consumption of a machine connected to the network in the event that the machine is disconnected from mains power.

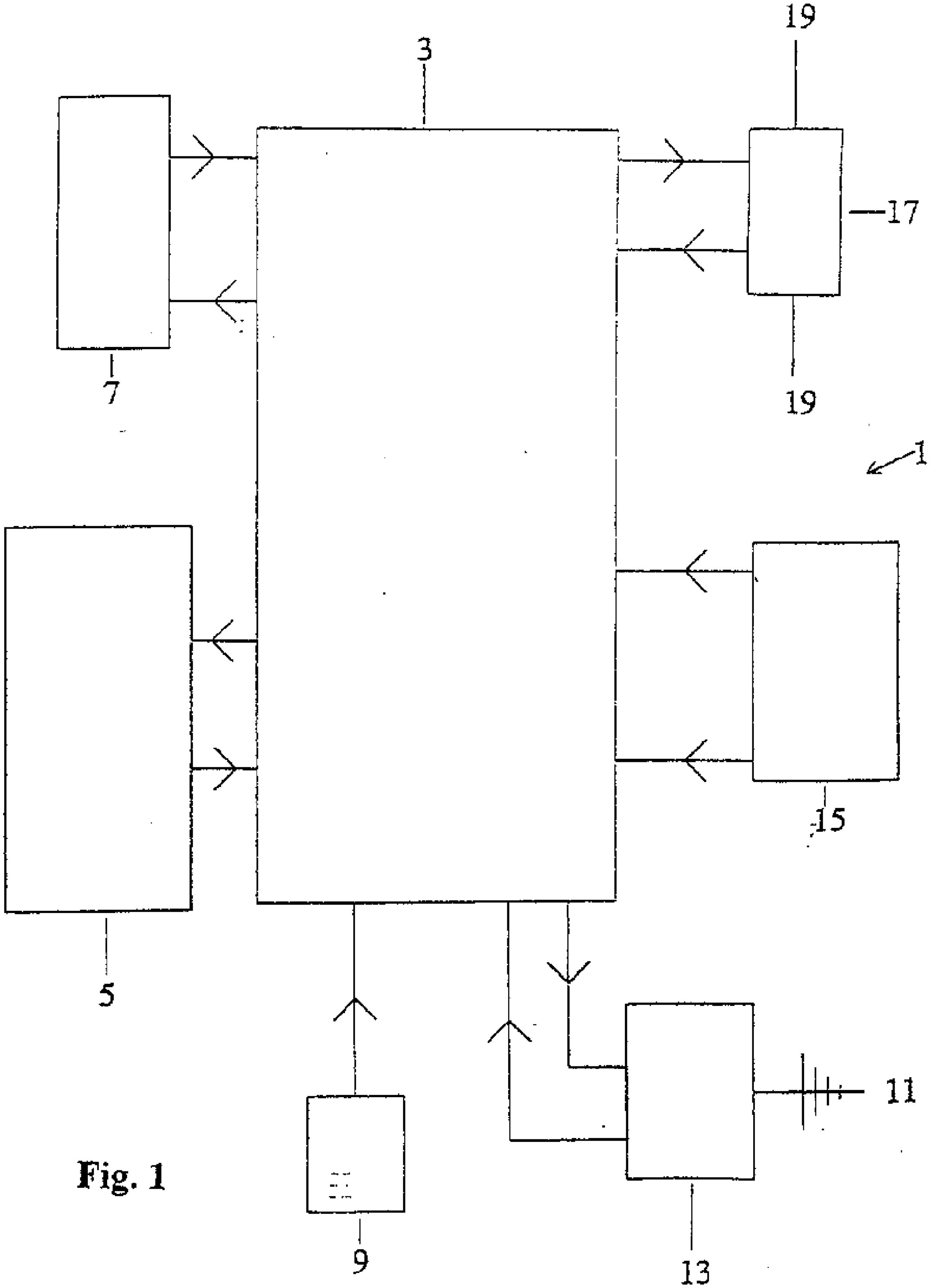


Fig. 1

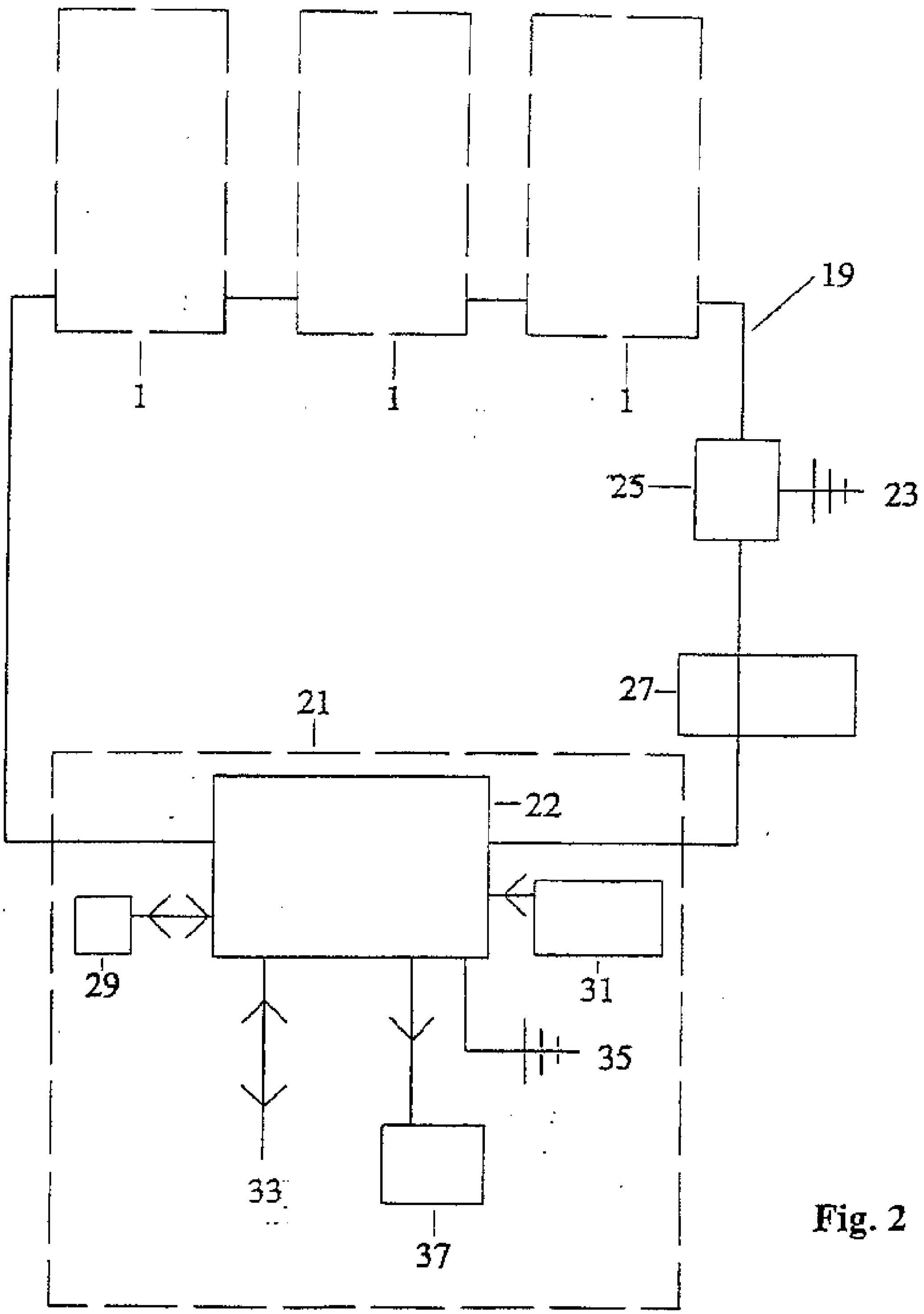


Fig. 2

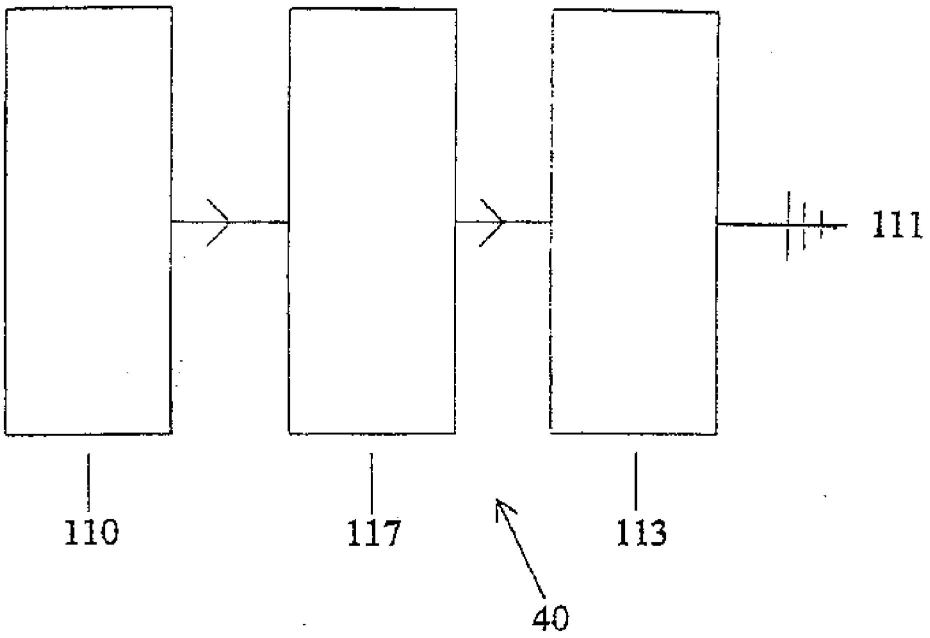


Fig. 3

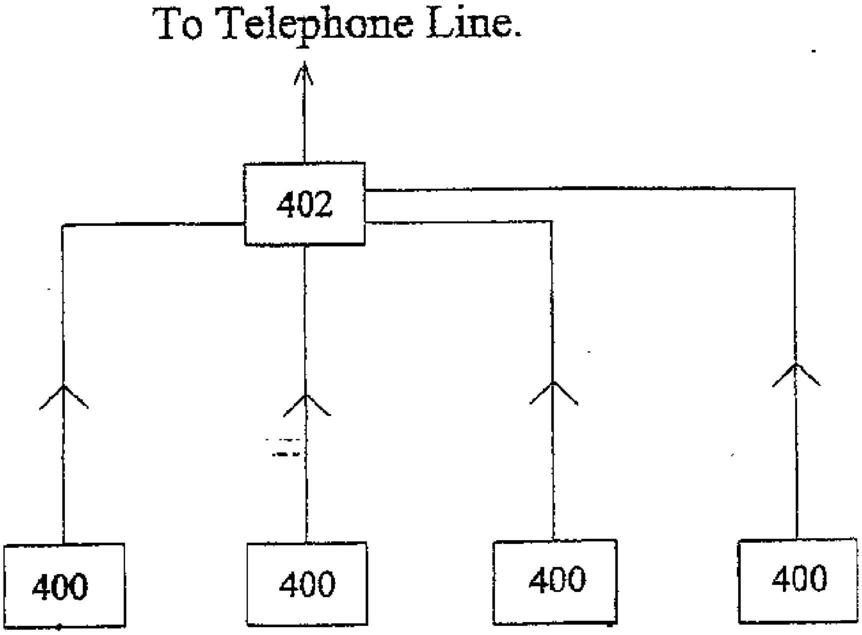


Fig. 4

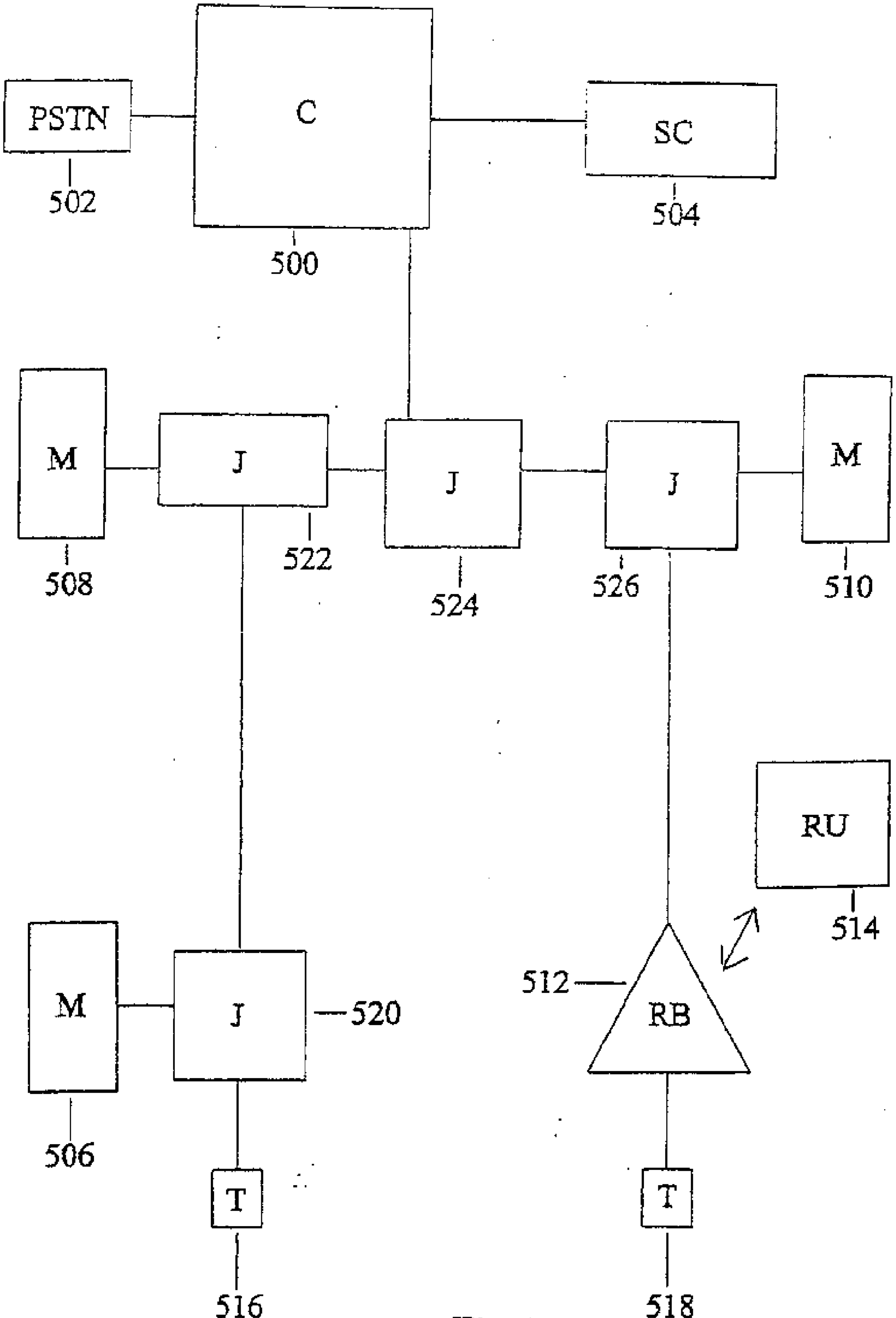

PSTN
502
C
500
SC
504
M
508
J
522
J
524
J
526
M
510
RU
514
512
RB
M
506
J
520
T
516
T
518

Fig. 5

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 074 955 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
22.10.2003 Bulletin 2003/43

(43) Date of publication A2:
07.02.2001 Bulletin 2001/06

(21) Application number: 00306668.5

(22) Date of filing: 04.08.2000

(51) Int Cl 7: G07F 17/32

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 04.08.1999 GB 9918427

(71) Applicant: MAYGAY MACHINES LIMITED
Wolverhampton, West Midlands WV10 9NL (GB)

(72) Inventor: Powell, David John
Wem, Shropshire SY4 5NX (GB)

(74) Representative: Hackney, Nigel John et al
Mewburn Ellis,
York House,
23 Kingsway
London WC2B 6HP (GB)

(54) Data transfer devices and methods

(57) In one aspect, the present invention provides a network of game machines (506, 508, 510, 514) including a central controller (500). The central controller is useable to receive data from the game machines and also to transmit data to the game machines, for example to upload new or corrected software to the game machines. Some of the game machines may be connected to the network via radio link (512). Higher baud rates, such as 10,000 baud, are acheivable with the network of the present invention.

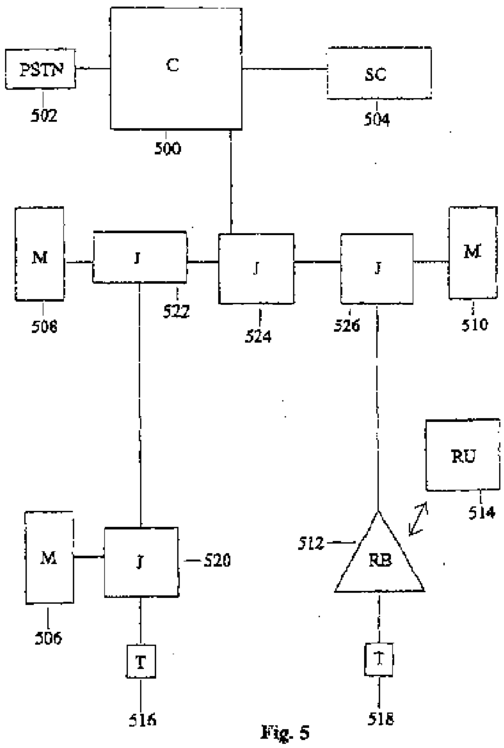


Fig. 5

EP 1 074 955 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 6668

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 759 102 A (PEASE LOGAN L ET AL) 2 June 1998 (1998-06-02) * column 1, line 11 - line 40 * * column 2, line 13 - line 20 * * column 3, line 21 - line 44 * * column 4, line 12 - line 18 * * column 5, line 8 - line 16 * * column 6, line 7 - line 21 * ---	1-13, 18-20	G07F17/32
X	DE 197 30 002 A (NSM AG) 14 January 1999 (1999-01-14)	1-8, 18-20	
A	* column 3, line 27 - column 4, line 27 * * claims 1,2 * ---	9-13	
X	US 4 335 809 A (WAIN JOHN L) 22 June 1982 (1982-06-22)	1-3, 9-13, 18-20	
A	* abstract * * column 2, line 57 - column 3, line 2 * * column 3, line 30 - line 35 * * column 3, line 62 - column 4, line 16 * * column 4, line 54 - column 5, line 2 * * column 6, line 44 - column 7, line 23 * ---	4-8	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07F
X	WO 99 00162 A (VEGAS AMUSEMENT INC) 7 January 1999 (1999-01-07) * page 27, line 1 - page 29, line 19 * * figure 7 * ---	21-26	
X	WO 97 15361 A (CAPPETTA LOUIS) 1 May 1997 (1997-05-01) * page 7, line 12 - page 8, line 6 * * figure 1 * ---	21-26	
X	US 5 855 515 A (PEASE LOGAN L ET AL) 5 January 1999 (1999-01-05) * column 3, line 17 - line 43 * * figure 1 * --- -/--	21-26	

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
THE HAGUE	27 August 2003	Van Dop, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 6668

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 655 961 A (GINSBURG ALEC ET AL) 12 August 1997 (1997-08-12) * abstract * ---		
A	DE 41 40 450 A (-) 9 June 1993 (1993-06-09) * the whole document * ---		
A	GB 2 236 423 A (BARCREST LTD) 3 April 1991 (1991-04-03) * the whole document * ---		
A	EP 0 829 834 A (INT GAME TECH) 18 March 1998 (1998-03-18) -----		
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
THE HAGUE	27 August 2003	Van Dop, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 00 30 6668

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

□ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

□ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

□ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

□ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☒ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

1-13,18-26

□ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 00 30 6668

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1-13, 18-20

1.1. Claims: 1-3
Claims 1 to 3 deal with the problem of transmitting game software to a gaming machine (p.7, l.17-19) by providing an interface for receiving game software from outside the machine and writing it to a memory.

1.2. Claims: 4-8
Claims 4 to 8 deal with the problem of transferring a sufficient amount of data into and/or out of the game machine for allowing identification of flaws in the software (p.9, l.11-14 and p.10, l.14-16) by providing an interface for transferring data at a rate of at least 10,000 baud.

1.3. Claims: 9-13
Claims 9 to 13 are directed at easily integrating one or more game machines into a network (p.11, l.20-21) by providing the game machine(s) with a radio communication device from transmitting data out of the machine(s).

1.4. Claims: 18-20
Claims 18 to 20 deal with the problem of handling a high volume of generated data reliably and economically within a network (p.19, l.14-15) by providing a collating device with a writer interface for transferring data to a recording medium.

2. Claims: 14-17

Claims 14 to 17 aim at a simple installation of a new game machine / a network of game machines (p.17, l.4-9) by reading configuration data from a physical recording medium.

3. Claims: 21-26

Claims 21 to 26 deal with an improved data communication (p.23, l.1-4) by providing a network topology where each game machine is linked to at least one other game machine and only one of the machines is in turn connected to a controller.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 6668

This annex lists the patent family membersrelating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-08-2003

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 5655961	A		US	6162122	A	19-12-2000
DE 4140450	A	09-06-1993	DE	4140450	A1	09-06-1993
GB 2236423	A	03-04-1991	NONE			
EP 0829834	A	18-03-1998	US	5779545	A	14-07-1998
			AU	713106	B2	25-11-1999
			AU	3745297	A	12-03-1998
			BR	9704683	A	02-02-1999
			CA	2214956	A1	10-03-1998
			EP	0829834	A2	18-03-1998
			ZA	9708125	A	03-03-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 231 577 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.08.2002 Bulletin 2002/33

(51) Int Cl.7: G07F 17/32

(21) Application number: 01402888.0

(22) Date of filing: 09.11.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 07.02.2001 US 778351

(71) Applicant: WMS Gaming Inc
Waukegan, Illinois 60085 (US)

(72) Inventor: Giobbi, John J.
Northbrook, Illinois 60062 (US)

(74) Representative: Loisel, Bertrand
Cabinet Plasseraud,
84, rue d'Amsterdam
75440 Paris Cédex 09 (FR)

(54) Centralized gaming system with modifiable remote display terminals

(57) A centralized gaming system comprises a central server system and a plurality of display terminals remote from and linked to the central server system. The central server system includes a master game server, a game execution server, and a database server. The master game server stores a plurality of games of chance. Each game includes respective game play software and respective audiovisual software. In response to one of the games being selected for play at one of the display terminals, the game play software for the selected game is loaded from the master game server into the game execution server and is executed by the game execution server to randomly select an outcome. The audiovisual software for the selected game is selectively executed at the display terminal to visually represent the outcome on a display of the display terminal. The database server collects game activity data based on the outcome and maintains such data for report generation and player tracking purposes. The master game server may evaluate the collected game activity data and, in turn, modify one or more of the display terminals for maximizing earnings and target marketing.

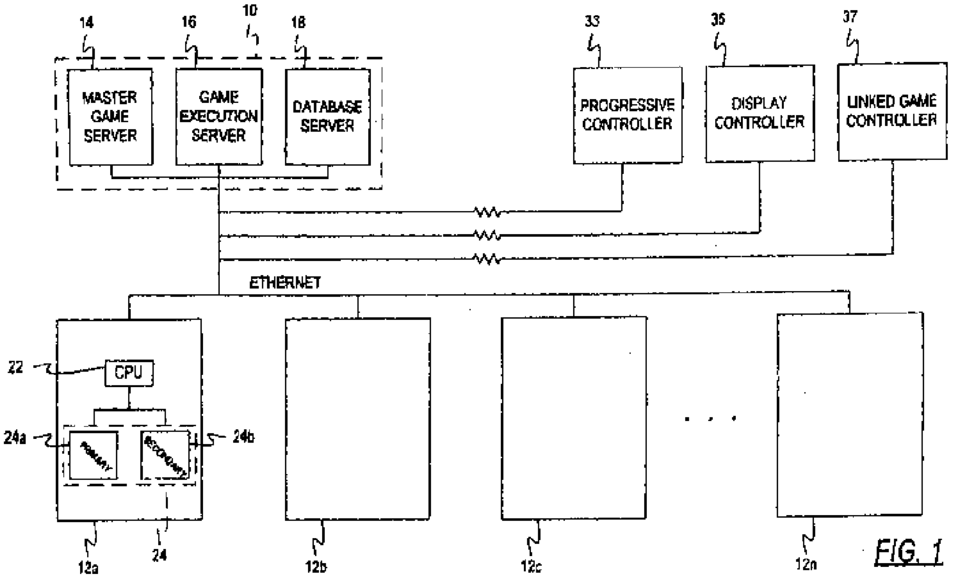


FIG. 1

EP 1 231 577 A2

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

[0001] The present invention relates generally to gaming systems and, more particularly, to a centralized gaming system with modifiable remote display terminals.

BACKGROUND OF THE INVENTION

[0002] Heretofore, gaming systems have generally been decentralized despite the presence of a central server. In such systems, the central server is linked to a plurality of gaming machines. In response to a wager, the gaming machines execute game software to randomly select an outcome and awarding an appropriate payout based on the outcome. The game software resides in memory located within the gaming machines. Accounting meters and a random number generator may reside in either the machines or the central server. The above-described arrangement suffers from numerous drawbacks.

[0003] First, if a gaming machine malfunctions and/or suffers an unplanned power loss, game activity data at the time of power loss can be difficult to precisely track. Untracked data may void a payout for a valid outcome that occurred just prior to the loss of power. Also, because the game software resides in the gaming machine, the gaming machine must be re-booted and must initialize the game software when brought back online.

[0004] Second, because live and historical outcome data are stored in the gaming machine, it can be difficult to generate reports concerning the activity of each gaming machine. Such data must be individually downloaded from each gaming machine. To generate a comprehensive report of all gaming machines, the downloaded data must then be combined.

[0005] Third, techniques for modifying or replacing the game software in the gaming machines are generally inconvenient, time-consuming, and expensive. In one technique, the entire machine is disconnected from the central server and replaced with a new machine. This involves the shipment of machines to and from a gaming establishment and requires the services of an appreciable number of skilled and semi-skilled service personnel. The service personnel must identify the machines to be replaced, locate the machines on the gaming establishment floor, and then replace the existing machines with the new machines. In another technique, the memory chip(s) containing the software is replaced with new software. Once again, the service personnel must identify the machines to receive the new memory chip(s), locate the machines on the gaming establishment floor, and then replace the existing memory chip (s) with the new memory chip(s). Also, any game-specific elements (e.g., artwork, button labels, etc.) must be replaced so that the machine is tailored to the new software. In yet another technique, the new software can be downloaded to the gaming machine from either the central server or a personal computer temporarily linked to the gaming machine. This downloading technique facilitates modifications to the game software in that it does not require removal of the gaming machine and does not require service personnel to visit the gaming machine site or the gaming machine itself. Nonetheless, the procedure for downloading the new game software to the gaming machine across a communications link can be time-consuming and subject to security concerns. The machine is generally out of service and therefore not generating any revenues during the time at which the new software is being downloaded. Also, regulated gaming jurisdictions may be reluctant to permit new software to be downloaded to the gaming machine without some assurance that the downloaded software complies with local regulations. Therefore, the downloaded software may need to be verified and authenticated.

[0006] Fourth, decentralized gaming systems typically limit the games available for play on each gaming machine. Because different casino players are attracted to different types of games of chance, a player may find it difficult to locate a gaming machine configured to play his/her preferred game. Heretofore, the player generally has had to walk around and search the casino floor for the preferred gaming machine. If the player is part of a group and different members of the group wish to play different games, the members of the group have had to split up to play their preferred games.

[0007] Although more centralized gaming systems have heretofore been proposed, such proposed systems have merely included a central game bank containing multiple gaming machines playable with handheld units plugged into "plug and play pods" remote from the central game bank. If one of the gaming machines in the central game bank is being used by one of the remote handheld units, the system does not allow that gaming machine to be selected by another of the remote handheld units for play at the same time. Thus, the central game bank is not a true multi-user game server, but rather provides a limited one-on-one system where each gaming machine in the central game bank can only be used by one of the remote handheld units at a time

[0008] A need therefore exists for a centralized gaming system that overcomes one or more of the aforementioned shortcomings associated with existing gaming systems

SUMMARY OF THE INVENTION

[0009] In accordance with the present invention, a centralized gaming system comprises a central server system and a plurality of display terminals remote from and linked to the central server system. The central server system includes a master game server, a game execution server, and a database server. The master game server stores a plurality of games of chance. Each game includes respective game play software and respective audiovisual software. In response to one of the games being selected for play at one of the display terminals, the game play software for the selected game is loaded from the master game server into the game execution server and is executed by the game execution server to randomly select an outcome. The audiovisual software for the selected game is selectively executed at the display terminal to visually represent the outcome on a display of the display terminal. The database server collects game activity data based on the outcome and maintains such data for report generation and player tracking purposes. The master game server may evaluate the collected game activity data and, in turn, modify one or more of the display terminals for maximizing earnings and target marketing.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings.

FIG. 1 is a block diagram of a centralized gaming system embodying the present invention.

FIG. 2 is a block diagram of a game available for play on the centralized gaming system.

FIG. 3 is an isometric view of a smart card terminal employed in the centralized gaming system.

FIG. 4 is an isometric view of a remote display terminal employed in the centralized gaming system.

FIG. 5 is a side view of the remote display terminal.

FIG. 6 is a flow diagram of a method of configuring remote display terminals in the centralized gaming system to maximize earnings.

[0011] While the invention is susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and will be described in detail herein. It should be understood, however, that the invention is not intended to be limited to the particular forms disclosed. Rather, the invention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0012] Turning now to the drawings and referring initially to FIG. 1, there is depicted a centralized gaming system comprising a central server system 10 and a plurality of remote display terminals $12_{a,b,c,...n}$. The remote display terminals are identified hereafter by the reference numeral 12, whether referring to one terminal or multiple terminals. The central server system 10 includes a master game server 14, a multi-user game execution server or play engine 16, and database server 18. The servers 14, 16, and 18 may be physically housed in separate boxes externally linked to each other by transmission lines or wireless technology, or may be physically housed in a common box and internally linked by wires and/or computer bus architecture, or may run on the same hardware.

[0013] The plurality of remote display terminals 12 are linked to each other and the central server system 10 by a high-speed local or wide area network using a data transfer protocol such as 100Base-T Ethernet or Gigabit Ethernet, which support data transfer rates of 100 megabits per second and 1 gigabit per second, respectively. Alternatively, the remote display terminals 12 and the central server system 10 may each be outfitted with transceivers that support two-way wireless communication. Each remote display terminal 12 is assigned a respective permanent identification number (PIN) for identifying the terminal 12 to the central server system 10 and allowing the central server system 10 to address the terminal 12.

[0014] The master game server 14 stores master copies of all games of chance available for play on the remote display terminals 12 The games of chance may, for example, include slots, poker, blackjack, keno, and bingo. The games are preferably stored in nonvolatile, read-only memory such as a hard drive, CD, DVD, etc.

[0015] As best shown in FIG. 2, each game of chance 20 may be defined as including two components: executable audiovisual software 20a and executable game play software 20b The audiovisual software 20a includes all audiovisual routines of the game 20 and all game-related I/O functions except for peripheral I/O functions that are not game specific. The audiovisual routines selectively play audio and visual resources to manage the content of visual images displayed by a remote display terminal 12 on which the routines are executed and the content of sounds emitted from speakers of the terminal 12. The game play software 20b, which includes underlying game play routines involving math tables, a random number generator, metering, auditing, etc., manages the game play execution for the game 20. The outcome randomly selected by the game 20 is stored in the database server 18. Referring back to FIG. 1, in response to a player's request at one of the remote display terminals 12 to play a game, the master game server 14 downloads the audiovisual software 20a for that game to the requesting terminal 12 and loads the game play software 20b for that game into the game execution server 16.

[0016] The game execution server 16 contains the game play software of all games currently selected for play (i.e., games in session) at the remote display terminals 12. As stated above, the game play software is loaded from the master game server 14 into the game execution server 16. If the same game is selected for play at more than one of the remote display terminals 12 at the same time, the game play software utilizes true multi-user procedures so that only one copy of the game play software for that game need be loaded into the game execution server 16.

[0017] The database server 18 stores any data to be maintained and used to generate reports. Such data may, for example, include live and historical game activity data and accumulated accounting meters. The game activity data includes the outcomes randomly selected by the games played on each terminal 12. The accounting meters store credits in, credits out, credits played, credits won, etc. for each of the remote display terminals 12. The data residing in the database server 18 may be marked with the PIN of the terminal 12 that generated the data. The database server 18 may, in turn, include an open interface for player tracking or generating audit reports. The audit reports may be organized by record type, terminal PINs, game name, game type (slots, poker, keno, bingo, etc.), or some other criteria.

[0018] The multi-game remote display terminal 12 allows a player at the terminal 12 to play any of the games of chance stored in the master game server 14. For example, if the master game server 14 contains eighty-seven slot games, ten poker games, one blackjack game, one keno game, and one bingo game, any of these one hundred games may be played at each remote display terminal 12 even if the same game is already being played at another one of the remote display terminals 12. Because the central system 10 is a true "server" of game software utilizing multi-user procedures, the same game or different games can be simultaneously played on different ones of the remote gaming terminals 12. Each time a game is selected for play on one of the remote display terminals 12, the game play software for the selected game is loaded from the master game server 14 into the game execution server 16 and run on the game execution server 16. If the same game is selected for play on multiple terminals 12 at the same time, the game play software for the selected game is merely loaded into the game execution server 16 the first time the game is selected. The game play software utilizes multi-user procedures to accommodate players at different terminals 12 who wish to play the same game at the same time. In an alternative embodiment in which the game play software does not utilize multi-user procedures, the game play software for the selected game is loaded into and run on the game execution server 16 each time the game is selected such that multiple copies of the game play software for the same game are simultaneously running on the game execution server 16.

[0019] The remote display terminal 12 includes a central processing unit (CPU) 22 and memory structure 24. The CPU 22 includes the terminal's operating system, which is responsible for managing general peripheral I/O functions such as bill validators, coin mechanisms, printers, hoppers, etc. The memory structure 24 preferably includes a . primary storage unit 24a and a secondary storage buffer 24b. The primary storage unit 24a may be battery-backed random access memory. The secondary storage buffer 24b may be a hard drive or disc storage used only for buffering/caching. The secondary storage buffer 24b contains the audiovisual software 20a (see FIG. 2) for the last N number of games selected for play at the associated terminal 12, where N depends upon storage capacity. For example, the storage buffer 24b may contain the audiovisual software for the last ten games selected for play at the associated terminal 12. Alternatively, the storage buffer 24b may contain sufficient storage capacity to contain the audiovisual software of all the games stored in the master game server 14.

[0020] After a player at a remote display terminal 12 has redeemed any credits remaining on terminal 12 and the terminal 12 has remained idle for a predetermined period of time ranging from a few seconds to a few minutes, the remote display terminal 12 may be configured to notify prospective players as to the games available for play on the remote display terminal 12. Toward that end, the remote display terminal 12 displays a game selection menu with a plurality of game selection indicia If the remote display terminal 12 has not remained idle for the predetermined period of time, instead of the game selection menu the terminal 12 may display the primary screen of the last game played on the terminal 12.

[0021] To play one of the games available for play on the remote display terminal 12, a new player selects one of the game selection indicia on the game selection menu. If the video display of the remote display terminal 12 is outfitted with a touch screen, the player makes this selection by touching the video display at the location of the game selection indicia for the game the player wishes to play. Alternatively or in addition, the remote display terminal 12 may include physical lighted push-buttons or other means for selecting the game selection indicia. The push-buttons are arranged relative to the game selection indicia in such a way that visually associates the push-buttons with respective ones of the game selection indicia.

[0022] In response to selecting one of the game selection indicia, the remote display terminal 12 sends a message to the master game server 14 identifying the sending terminal's PIN and the selected game (including the version of any audiovisual software residing in the secondary storage buffer 24b). If the audiovisual software for the selected game is buffered in the secondary storage buffer 24b and the master game server 14 verifies that the buffered version matches the version stored in the master game server 14, the master game server 14 loads the game play software for the selected game into the game execution server 16 and directs the remote display terminal 12 to load the buffered audiovisual software from the secondary storage buffer 24b into the primary storage unit 24a.

[0023] If the correct version of the audiovisual software is not buffered in the secondary storage buffer 24b, the master game server 14 may immediately update any buffered version with the correct version by downloading the correct version of the audiovisual software to the secondary storage buffer 24b of the appropriate remote display terminal 12. Alternatively, the master game server 14 may direct the remote display terminal 12 to inform the player that the selected game is temporarily unavailable and implement the update process according to a predefined schedule. The schedule may call for updates on all or groups of the remote display terminals 12 at predetermined times, such as during off-peak hours.

[0024] With the game play software loaded into the game execution server 16 and the buffered audiovisual software loaded into the primary storage unit 24a, the game execution server 16 proceeds to execute the game play software for the selected game Initially, the game execution server 16 directs the operating system of the remote display terminal 12 to execute an audiovisual routine that will display the main screen of the selected game. If, for example, the selected game includes a multi-line, five-reel video slot game, the main screen may include five symbol-bearing reels, game session meters, and various on-screen "soft" buttons for placing wagers, cashing out, obtaining help, and initiating play. The game session meters vary from game to game but with respect to slots, for example, may include credits, line bet, total bet, and paid.

[0025] Next, the player places a wager at the remote display terminal 12. To be able to place a wager, the player must add credits to the "credits" meter for the remote display terminal 12 on which the player wishes to play. Toward that end, the centralized gaming system preferably promotes wagering without cash, i.e., cashless gaming, to minimize the need for service personnel to visit the remote display terminals 12. To realize wagering without cash, smart card terminals 26 of the type illustrated in FIG. 3 are interspersed throughout the gaming establishment. Alternatively, cashless gaming may be accomplished by other means such as tickets/coupons, magnetic cards, or the like.

[0026] Referring briefly to FIG. 3, the smart card terminal 26 includes a smart card reader/dispenser 28, a cash acceptor 30, and a cash dispenser 32. To obtain a smart card prior to playing at one of the remote display terminals 12, the player deposits cash (bills) into the cash acceptor 30. After the desired amount of cash has been deposited, the player presses a vend card button 34 to cause the terminal 26 to dispense a smart card from the smart card dispenser 28. The smart card is embedded with a microcontroller having a memory storing funds corresponding to the amount of cash deposited into the smart card terminal 26. The use of smart cards for cashless gaming is advantageous over other cashless media, such as credit cards, because smart cards generally heighten a player's awareness of funds spent.

[0027] In an alternative embodiment, the smart card not only serves as a funds handling card but also serves as a player tracking card. To be able to track the player, the smart card terminal may include a player interface, such as a keyboard and/or a touch screen, that allows the player to enter player tracking information. The player tracking information may be limited to personal identification information or may include additional details such as play data as disclosed in U.S Patent No. 5,179,517 to Sarbin et al. and player preference data as disclosed in U.S. Patent No. 6,110,041 to Walker et al. Instead of vending new smart cards at the smart card terminal 26, the gaming system may require the player to obtain a new smart card directly from a registration authority in the gaming establishment, which acquires the player tracking information prior to tendering the smart card. The player tracking information is preferably stored in a personal record residing in the database server 18 in FIG. 1 or a separate player tracking database coupled to the open interface of the database server 18. The smart card stores a personal identifier for addressing and accessing this personal record. If the smart card terminal 26 only accepts smart cards but does not vend new cards, then the player inserts his or her smart card (obtained from the registration authority) into the smart card reader 28 prior to depositing cash into the cash acceptor 30.

[0028] Referring back to FIG. 1, to place a wager at the remote display terminal 12, the player inserts his or her smart card into a card reader (see FIG. 4) of the remote display terminal 12. The remote display terminal 12, in turn, sends a message to the game execution server 16 identifying the sending terminal's PIN, the personal identifier on the smart card, and the amount of funds on the smart card. The personal identifier is used to address and access the player's personal record in the player tracking database and thereby implement player tracking functions in a manner heretofore known in the art. The game execution server 16 updates its game session meters based on the amount of funds on the smart card, and then directs the operating system of the remote display terminal 12 to correspondingly update the terminal's on-screen game session meters. The actual funds may still reside on the smart card, which is locked in the terminal's card reader, but the amount of funds is visually represented on the main screen so the player is aware of the amount of funds on the card and available for game play. Alternatively, the funds may actually be electronically transferred from the smart card to the game execution server 16.

[0029] Next, the player enters a wager amount via the touch screen or push-buttons on the remote display terminal 12. If the selected game includes a multi-line, five-reel video slot game, the player's wager includes the number of pay lines to play and the wager amount per pay line The remote display terminal 12 displays the number of pay lines played on the terminal's on-screen "lines" meter, the wager amount per pay line on the "bet per line" meter, and the total wager amount on the "total bet" meter.

[0030] To spin the reels simulated on the video display, the player presses a "play" or "spin reels" button on the remote display terminal 12. The remote display terminal 12, in turn, sends a message to the game execution server 16 identifying the terminal's PIN, the number of pay lines played, the wager amount per pay line, and the instruction to play. The game execution server 16 updates its game session meters and then directs the operating system of the remote display terminal 12 to correspondingly update the terminal's onscreen game session meters. Using a random number generator (RNG) in the game play software, the game execution server 16 randomly selects an outcome for the selected game. The outcome may, for example, be represented by a particular set of reel stop positions and a payout for a symbol combination along each active pay line. The outcome is randomly selected from a plurality of possible outcomes. The payouts depend upon the probability of occurrence of the respective outcomes such that the lower the probability of occurrence of an outcome, the higher the payout awarded for that outcome. The payout may, of course, range from zero to a value much greater than zero. A pay table identifies the non-zero payouts and the outcomes corresponding to those payouts and may be accessed by pressing a "pay table" button on the remote display terminal 12.

[0031] After randomly selecting an outcome, the game execution server 16 updates its game session meters based on the payout for that outcome. To report the outcome to the player, the game execution server 16 sends a message to the remote display terminal 12 identifying the outcome. Based on the outcome, the remote display terminal 12 executes audiovisual routines that will display a simulation of spinning reels, stop the reels at the stop positions corresponding to the selected outcome, and update the values in the terminal's onscreen game session meters to correspond to the server's game session meters.

[0032] The above-described process for executing a game selected for play on the remote display terminal 12 is repeated until the player wishes to stop playing the game and "cash out" any credits remaining on the "credits" meter. To cash out, the player presses a "collect" button on the remote display terminal 12. The remote display terminal 12, in turn, sends a message to the game execution server 16 identifying the sending terminal's PIN and the cash out instruction. The game execution server 16 responds by updating its game session meters, modifying the amount of funds on the card to correspond to the "credits" meter, and instructing the terminal's card reader to unlock and dispense the smart card. The database server 18 updates its accumulated accounting meters based on the completed game session and may, from time to time, also update its accounting meters during a game session. If funds remain on the smart card, the player can insert the smart card into a smart card terminal 26 of the type depicted in FIG. 3 and collect the funds in the form of cash dispensed from the cash dispenser 32.

[0033] In one embodiment, the remote display terminals 12 only permit cashless gaming and therefore contain no bill validators, no coin mechanisms, and no hoppers. If the player uses up all the funds on the smart card, the smart card is automatically dispensed from the card reader so that the player can take the card to a smart card terminal 26 (see FIG. 3) and load additional funds onto the card. In an alternative embodiment, the remote display terminals 12 include bill and/or coin acceptors for the sole purpose of loading funds onto the card should the player use up the existing funds. With this arrangement, the player need not leave the remote display terminal 12 to reload. In yet another alternative embodiment, the bill and/or coin acceptors can additionally be employed to directly load funds onto the "credits" game session meter for the remote display terminal 12.

[0034] In addition to being linked to the remote display terminals 12, the central server system 10 is optionally linked by the local or wide area computer network to a progressive controller 33, a display controller 35, and/or a linked game controller 37. The progressive controller 33 establishes a common progressive jackpot based on wagers placed at the remote display terminals 12 and awards the jackpot to a player at one of the terminals 12 based on predetermined criteria such as a highly unlikely outcome triggered by that terminal 12. The display controller 35 may control various overhead video displays for displaying the amount of a progressive jackpot, displaying a shared bonus game or bonus amount triggered by one of the remote display terminals 12, reproducing the images appearing on one of the terminals 12 such as a terminal 12 in a bonus mode, attracting attention to the terminals 12 or a particular bank of the terminals 12, or just generally increasing the level of excitement in the gaming establishment. The display controller 35 may also selectively illuminate various overhead non-video signs such as neon signs.

[0035] The linked game controller 37 may be integrated into the game execution server 16 or may be a separate hardware component linked to the game execution server 16. The linked game controller 37 preferably allows individual terminals 12 or groups of terminals 12 to play a common game feature in which the terminals compete against each other or play together toward a common goal. If the terminals compete against each other, each terminal may be assigned a respective visual element such as a character, symbol, or the like. For example, if the visual elements are horses, race cars, or runners, the participating terminals may complete against each other in a race where movement of the visual elements along the race track is entirely random or based on subsequent wagers or outcomes on the participating terminals. If the terminals play together toward a common goal, achievement of that goal may generate a bonus shared by the participating terminals. The bonus may be distributed to the participating terminals in equal or unequal shares, depending upon the extent to which each terminal contributed toward the achievement of the common goal. The common game feature may be depicted on a large central display and/or participating terminal displays under the control of the linked game controller 37.

[0036] Participation in the common game feature by a terminal 12 may be triggered by either the linked game controller 37 or the terminal 12. The linked game controller 37, for example, may trigger participation at random or predetermined times of day. The terminal 12 may trigger participation of that terminal in the common game feature in response to a special start-feature outcome generated by the game played via the terminal 12, or a player's election to participate in the common game feature. Also, one terminal's participation may cause one or more other terminals to also participate in the common game feature.

[0037] FIGS 4 and 5 illustrate one embodiment of the remote display terminal 12. In this embodiment, the remote display terminal 12 includes upper and lower displays 36 and 38. The upper display 36 is preferably a flat panel video display mounted to a vertical support 40 and selected from a group consisting of a liquid crystal display (LCD), plasma display, field emission display, digital micromirror display (DMD), dot matrix display, vacuum florescent display (VFD), etc. While the remote display terminal 12 is in an attract mode, the upper video display 36 may be used to depict billboard indicia for attracting attention to the terminal 12. While a player is playing a game at the terminal 12, the upper video display 36 may continue to display the billboard indicia, or may alternatively display special effects or secondary game play features.

[0038] The lower display 38 may be any of the aforementioned video displays, a CRT, or a plurality of mechanical slot reels viewable through a display window. If the lower display 38 is a video display, it is preferably outfitted with a touch screen. While a player is playing a game at the terminal 12, the lower display 38 displays primary game play features (e.g., slot reels, poker cards, keno board, bingo board, etc.) according to messages from the game execution server 16 identifying routines of the terminal's audiovisual software that should be executed (see FIG. 1).

[0039] The remote display terminal 12 includes a generally horizontal support 42 for housing the lower display 38, a smart card reader 44, and the electronics of the CPU 22 and memory structure 24 discussed in connection with FIG. 1. The horizontal support 42 is preferably hinged to the vertical support 40 such that it can be rotated upwardly as shown by an arrow in FIG. 5 to permit access the electronics within the horizontal support 42 via an access panel on a lower side of the support 42.

[0040] The remote display terminal 12 also includes a swivel seat 46 mounted to a horizontal seat support 48. The seat support 48 contains a footrest 50 beneath the horizontal support 42 and extends forwardly from the vertical support 40.

[0041] The present invention has several advantages. First, because the central server system 10 in FIG. 1 executes the game play software, malfunctions or unplanned power losses on the remote display terminals 12 generally do not affect game outcomes. The central server system 10 itself is redundantly protected from such problems. Further, game development is simplified.

[0042] Second, because historical data is centrally stored in the database server 18 in FIG. 1, the central server system 10 facilitates generation of reports concerning the activity of the remote display terminals 12. Using off-the-shelf database tools manufactured by such companies as Oracle Corporation, such reports can be easily generated and organized as desired.

[0043] Third, the present invention facilitates modification to the games available for play via the remote display terminals 12. Because games are centrally stored on the master game server 14, a game is easily changed by simply updating the software residing in the master game server 14. Modifications or updates do not require the entire software to be installed in each of the remote display terminals 12 in what would be a time-consuming process subject to elevated security concerns.

[0044] Fourth, due to the ease of modifying the games available for play via the remote display terminals 12, the remote display terminals 12 may be configured to maximize earnings using the method depicted in FIG. 6. More specifically, the remote display terminals 12 may be arranged in a plurality of banks (groups) coupled to the central server system (steps 100 and 102). The terminals 12 in the same bank may have a common characteristic, such as the type of game (slots, poker, bingo, keno, etc.), game theme, minimum wager for playing a game, volatility of a game, payback percentage, etc. Based on the historical data collected in the database server 18 (step 104), it may be determined that certain banks perform better, e.g., are played more frequently or earn more money, than other banks. This determination may be explained by market research and/or by evaluating the performance statistics of certain games when placed in different banks (step 106). Using a graphical user interface at the master game server, the master game server 14 may then be configured to modify the selection, content, and/or math of games available to each terminal 12 according to predetermined criteria, such as performance (e.g., frequency of play or money earnings), time, location of terminal, or various player or casino preferences (step 108). If, for example, it is determined that low volatility slot games with a low minimum wager (e.g., 5 cents) are most popular when available in Bank X near the front door of the gaming establishment between the hours of 6 pm and 11 pm, then the master game server 14 may be configured to modify the games available for play via the terminals 12 in Bank X to be low volatility slot games with a low minimum wager between 6 pm and 11 pm. The master game server 14 is preferably linked to a display for graphically presenting the programmed configuration to an operator and allowing the operator to easily modify the configuration. Modifications can preferably be done not only on a bank-by-bank basis, but also a terminal-by-terminal basis. Thus, the earnings generated by the remote display terminals 12 can be maximized.

[0045] Fifth, the remote display terminals 12 may similarly be configured for target marketing. For example, terminals 12 near the front door may offer a new game to bring the game to the attention of prospective players and get players acquainted with the game.

[0046] Sixth, to facilitate a player's ability to play a variety of games on a remote display terminal 12 without having to search the casino floor for his or her preferred game, the terminal 12 may be configured to offer a large number of games. By buffering the audiovisual software but not the game play software for each game, the remote display terminal 12 may be constructed to have sufficient memory capacity to accommodate the large number of games. To the extent that the games on the remote display terminal 12 have a wide range of characteristics, the games may be arranged in a heirarchy of primary and secondary game selection menus to emphasize those games that will maximize earnings as discussed above.

[0047] Seventh, the remote display terminals 12 are reliable and require minimal maintenance because they have few parts that are easily repaired if a problem should occur.

[0048] While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention.

[0049] For example, the game of chance selected for play on a remote display terminal 12 may include multiple stages involving more interaction between the game and the player than just the initial wager. Video draw poker, for example, requires the player to select which cards to hold and which cards to discard after the initial deal. Likewise, many slot games include bonus features triggered by certain outcomes in the main slot game and requiring the player to select from multiple game playing elements. Such interactive games require multiple messages between the game execution server 16 and the remote display terminal 12 where the game execution server 16 may need to update its game session meters in mid-game, randomly select an outcome, and remotely request the operating system of the terminal 12 to change its display based on the outcome more than once during the game.

[0050] In addition, instead of buffering the audiovisual software in the secondary storage buffer 24b for each of the games available for play on a remote display terminal 12 and then loading the audiovisual software for a selected game from the secondary storage buffer 24b into the primary storage unit 24a, the audiovisual software for the selected game may be loaded into the primary storage unit 24a from the master game server 14 in response to a player's selection of that game. The secondary storage buffer 24b is therefore eliminated, but at the expense of a more time-consuming download from the master game server 14.

[0051] Further, instead of executing the game play software in the game execution server 16, the game play software may be downloaded from the master game server 14 to a requesting remote display terminal 12 and locally executed by the terminal 12. In other words, the game execution server 16 in FIG. 1 can be eliminated, and the game play software can reside in and be executed locally by the terminal 12. Whether the game play software is executed remotely by the game execution server 16 in FIG. 1 or locally by the terminal 12, the terminal 12 already includes a central processing unit with memory such that few additional components would be required for the terminal 12, and not the central game execution server 16, to locally execute game play software.

[0052] Each of these embodiments and obvious variations thereof is contemplated as falling within the spirit and scope of the claimed invention, which is set forth in the following claims.

Claims

1. A centralized gaming system, comprising:

    a central server system storing a plurality of games of chance and including a play engine; and
    a plurality of remote display terminals linked to the central server system, each remote display terminal including a display;

    wherein in response to one of the games being selected for play at one of the remote display terminals, game play software for the selected game is loaded into and executed by the play engine to randomly select an outcome, and the outcome is visually represented on the display of the one of the remote display terminals.

2. The gaming system of claim 1, wherein each game includes audiovisual software, and wherein in response to one of the games being selected for play at one of the remote display terminals, the audiovisual software for the selected game is downloaded from the central server system to the one of the remote display terminals and is selectively executed at the one of the remote display terminals to visually represent the outcome on the display of the one of the remote display terminals.

3. The gaming system of claim 1, wherein each game includes audiovisual software selectively executed at the one of the remote display terminals to visually

represent the outcome on the display of the one of the remote display terminals.

4. The gaming system of claim 1, wherein the game play software includes a random number generator for randomly selecting the outcome.

5. The gaming system of claim 1, wherein each remote display terminal includes upper and lower video displays, the upper video display depicting billboard indicia, the lower display visually representing the outcome.

6. The gaming system of claim 5, wherein the upper display is a flat panel display selected from a group consisting of a liquid crystal display (LCD), plasma display, field emission display, digital micromirror display (DMD), dot matrix display, and vacuum florescent display (VFD).

7. A centralized gaming system, comprising:

   a central server system storing a plurality of games of chance and including a play engine; and
   a display terminal remote from and linked to the central server system;

   wherein in response to one of the games being selected for play at the display terminal, game play software for the selected game is loaded into and executed by the play engine to randomly select an outcome, and the outcome is visually represented on a display of the display terminal.

8. The gaming system of claim 7, wherein in response to one of the games being selected for play at the display terminal, audiovisual software for the selected game is downloaded from the central server system to the display terminal and is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal.

9. The gaming system of claim 7, wherein audiovisual software for the selected game is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal.

10. The gaming system of claim 7, wherein in response to one of the games being selected for play at the display terminal, the display terminal informs the central server system of a version of any audiovisual software for the selected game already residing in the display terminal; and wherein if the version is up to date, the audiovisual software is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal; and wherein if the version is not up to date, updated audiovisual software for the selected game is downloaded from the central server system to the display terminal and is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal.

11. The gaming system of claim 7, wherein in response to one of the games being selected for play at the display terminal, the central server system compares versions of audiovisual software for the selected game residing in the central server system and the display terminal; wherein if the versions match, the audiovisual software is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal, and wherein if the versions do not match, the audiovisual software in the central server system is downloaded to the display terminal and is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal.

12. A centralized gaming system, comprising:

   a central server system including a master game server and a game execution server, the master game server storing a plurality of games of chance; and
   a display terminal remote from and linked to the central server system;

   wherein in response to one of the games being selected for play at the display terminal, game play software for the selected game is loaded from the master game server into the game execution server and is executed by the game execution server to randomly select an outcome, and the outcome is visually represented on a display of the display terminal.

13. The gaming system of claim 12, further including a database server for storing game activity data based on the outcome.

14. A centralized gaming system, comprising:

   a central server system including a master game server and a game execution server, the master game server storing a plurality of games of chance, each of the games including respective game play software and respective audiovisual software; and
   a display terminal remote from and linked to the central server system,

   wherein in response to one of the games being selected for play at the display terminal, the game play software for the selected game is loaded from the master game server into the game execution server and is executed by the game execution server to randomly select an outcome, and the audiovisual software for the selected game is selectively executed at the display terminal to visually represent the outcome on a display of the display terminal.

15. The gaming system of claim 14, wherein in response to one of the games being selected for play at the display terminal, the master game server compares versions of the audiovisual software for the selected game residing in the master game server and the display terminal; wherein if the versions match, the audiovisual software is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal; and wherein if the versions do not match, the audiovisual software in the master game server is downloaded to the display terminal and is selectively executed at the display terminal to visually represent the outcome on the display of the display terminal.

16. The gaming system of claim 14, further including a database server for storing game activity data based on the outcome.

17. A method of executing a game of chance, comprising:

providing a central server system storing a plurality of games of chance and including a play engine;
providing a plurality of display terminals remote from and linked to the central server system;
receiving a player's selection of one of the games to be played at one of the display terminals;
loading game play software for the selected game into the play engine;
executing the game play software in the play engine to randomly select an outcome; and
visually representing the outcome on a display of the one of the display terminals.

18. The method of claim 17, wherein the step of executing the game play software includes generating a random number for randomly selecting the outcome.

19. The method of claim 17, further including selectively executing audiovisual software for the selected game at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals.

20. The method of claim 19, further including downloading the audiovisual software from the central server system to the one of the display terminals prior to the step of selectively executing the audiovisual software.

21. The method of claim 17, further including comparing versions of audiovisual software for the selected game residing in the central server system and the one of the display terminals; if the versions match, selectively executing the audiovisual software at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals; and if the versions do not match, downloading the audiovisual software in the central server system to the one of the display terminals and selectively executing the audiovisual software at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals.

22. A method of executing a game of chance, comprising:

providing a central server system including a master game server and a game execution server, the master game server storing a plurality of games of chance;
providing a plurality of display terminals remote from and linked to the central server system;
receiving a player's selection of one of the games to be played at one of the display terminals;
loading game play software for the selected game from the master game server into the game execution server;.
executing the game play software in the game execution server to randomly select an outcome; and
visually representing the outcome on a display of the one of the display terminals.

23. The method of claim 22, further including selectively executing audiovisual software for the selected game at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals.

24. The method of claim 23, further including downloading the audiovisual software from the central server system to the one of the display terminals prior to the step of selectively executing the audiovisual software

25. The method of claim 22, further including comparing versions of audiovisual software for the selected game residing in the central server system and the one of the display terminals; if the versions match, selectively executing the audiovisual software at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals; and if the versions do not match, downloading the audiovisual software in the central server system to the one of the display terminals and selectively executing the audiovisual software at the one of the display terminals to visually represent the outcome on the display of the one of the display terminals.

26. The method of claim 22, wherein the central server system includes a database server, and further including storing game activity based on the outcome in the database server.

27. A game-on-demand gaming system, comprising:

a central server system storing a plurality of games of chance; and
a plurality of gaming terminals remote from and linked to the central server system;

wherein in response to one of the games being selected for play at one of the gaming terminals, the central server system downloads at least some software for the selected game to the one of the gaming terminals so that the game can be played via the one of the gaming terminals, the selected game being concurrently playable via another of the gaming terminals.

28. The gaming system of claim 27, wherein the downloaded software includes game play software.

29. The gaming system of claim 27, wherein the downloaded software includes audiovisual software but not game play software

30. The gaming system of claim 27, wherein each gaming terminal includes a video display for displaying a plurality of game selection indicia associated with the respective games.

31. The gaming system of claim 30, wherein the plurality of game selection indicia are displayed on the video display in response to the gaming terminal being idle for a predetermined period of time.

32. A method of operating gaming terminals, each gaming terminal being remote from and linked to a central server system storing a plurality of games of chance, the method comprising:

receiving a player's selection of one of the games to be played at one of the gaming terminals; and
downloading at least some software for the selected game from the central server system to the one of the gaming terminals so that the game can be played via the one of the gaming terminals, the selected game being concurrently playable via another of the gaming terminals.

33. The method of claim 32, further including receiving a wager at the one of the gaming terminals to play the selected game.

34. The method of claim 32, wherein the downloaded software includes game play software.

35. The method of claim 32, wherein the downloaded software includes audiovisual software but not game play software.

36. The method of claim 32, further including executing the selected game to randomly select an outcome, and visually representing the outcome on a display of the one of the gaming terminals.

37. The method of claim 32, further including displaying a plurality of game selection indicia associated with the respective games on a display of each gaming terminal.

38. The method of claim 37, wherein the displaying step occurs in response to the respective gaming terminal being idle for a predetermined period of time.

39. A method of configuring remote gaming terminals that permit games of chance to be played in response to a wager, comprising:

coupling the remote gaming terminals to a central server system;
generating game activity data at the remote gaming terminals;
transmitting the game activity data to the central server system;
evaluating the game activity data; and
using the central server system to modify the remote gaming terminals based on the game activity data.

40. The method of claim 39, wherein the game activity data is selected from a group consisting of frequency of play of the remote gaming terminals and earnings generated by the remote gaming terminals.

41. The method of claim 39, wherein the step of evaluating the game activity data is performed by the central server system.

42. The method of claim 39, wherein the step of evaluating the game activity data is performed by a device or person external to the central server system.

43. The method of claim 39, wherein the step of using the central server system to modify the remote gaming terminals includes modifying the games of chance that can be played via the remote gaming terminals.

44. The method of claim 39, wherein the step of using the central server system to modify the remote gaming terminals includes modifying one or more of the following:

a selection of the games of chance available for play via the remote gaming terminals, menus identifying the games of chance available for play via the remote gaming terminals, the content of the games of chance, and math tables associated with the games of chance.

45. The method of claim 39, wherein the remote gaming terminals are arranged in groups, and wherein the step of using the central server system to modify the remote gaming terminals includes modifying the remote gaming terminals in the same group in a similar manner.

46. The method of claim 39, wherein the step of using the central server system to modify the remote gaming terminals includes making a modification effective for a limited period of time.

47. A gaming system comprising:

a plurality of remote gaming terminals for generating game activity data in response to wagers on games of chance played via the remote gaming terminals;
a central server system for receiving the game activity data and modifying the remote gaming terminals based on the game activity data, the central server system being coupled to the remote gaming terminals; and
means for evaluating the game activity data received by the central server system.

48. The system of claim 47, wherein the game activity data is selected from a group consisting of frequency of play of the remote gaming terminals and earnings generated by the remote gaming terminals.

49. The system of claim 47, wherein the central server system includes the means for evaluating the game activity data.

50. The system of claim 47, wherein the central server system modifies the games of chance that can be played via the remote gaming terminals.

51. The system of claim 47, wherein the central server system modifies one or more of the following: a selection of the games of chance available for play via the remote gaming terminals, menus identifying the games of chance available for play via the remote gaming terminals, the content of the games of chance, and math tables associated with the games of chance.

52. The system of claim 47, wherein the remote gaming terminals are arranged in groups, and wherein the central server system modifies the remote gaming terminals in the same group in a similar manner.

53. The system of claim 47, wherein the central server system makes a modification to the remote gaming terminals effective for a limited period of time.

54. A method of configuring remote gaming terminals that permit games of chance to be played in response to a wager, comprising:

coupling the remote gaming terminals to a central server system; and
using the central server system to modify the remote gaming terminals.

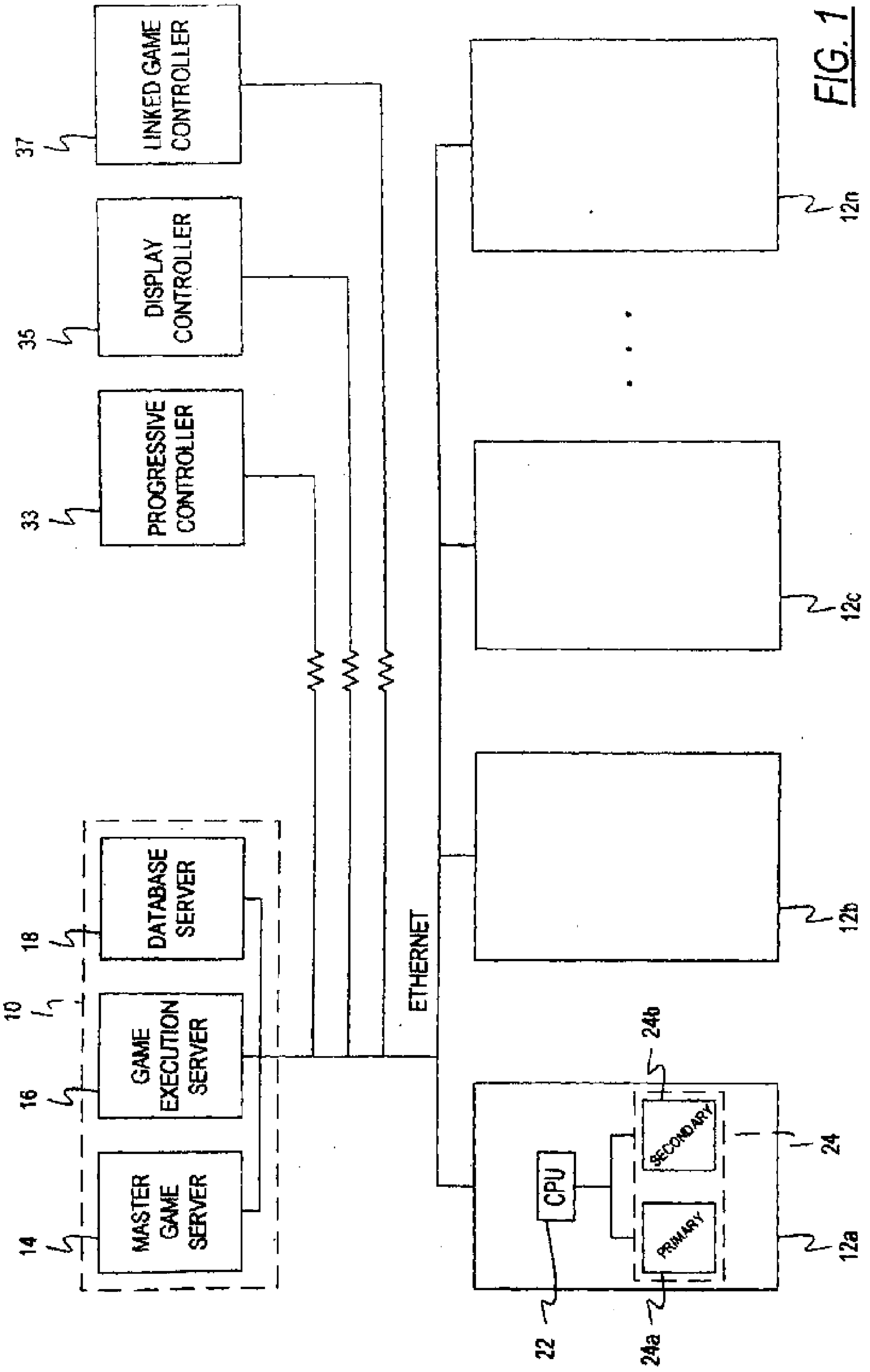

14
MASTER GAME SERVER
16
GAME EXECUTION SERVER
18
DATABASE SERVER
10
33
PROGRESSIVE CONTROLLER
35
DISPLAY CONTROLLER
37
LINKED GAME CONTROLLER
ETHERNET
CPU
PRIMARY
SECONDARY
22
24a
24b
24
12a
12b
12c
12n

FIG. 1

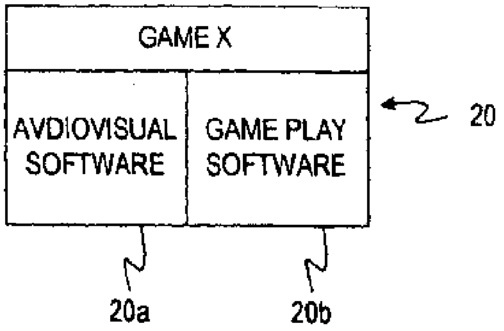


FIG. 2

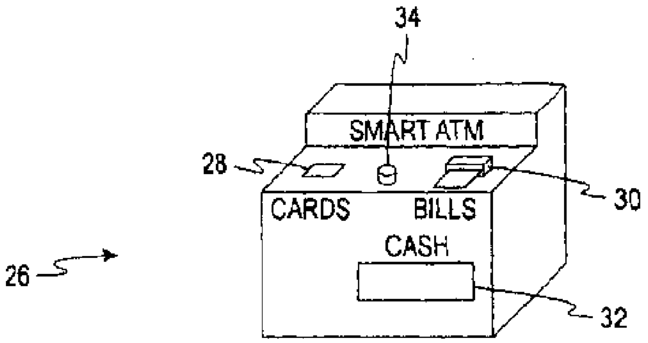


FIG. 3

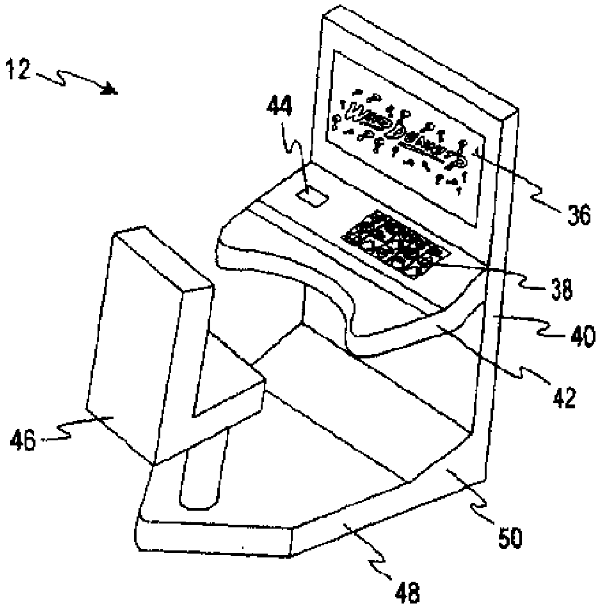


FIG. 4

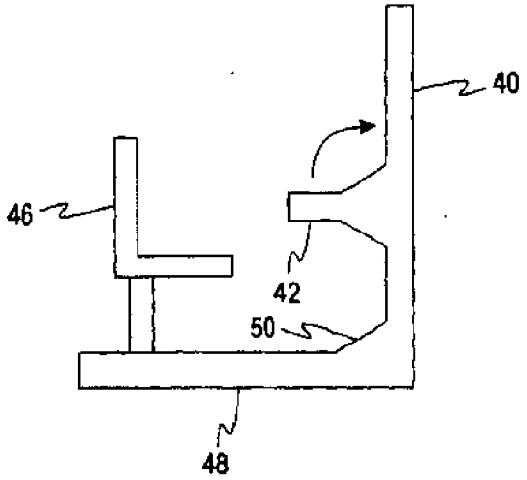


FIG. 5

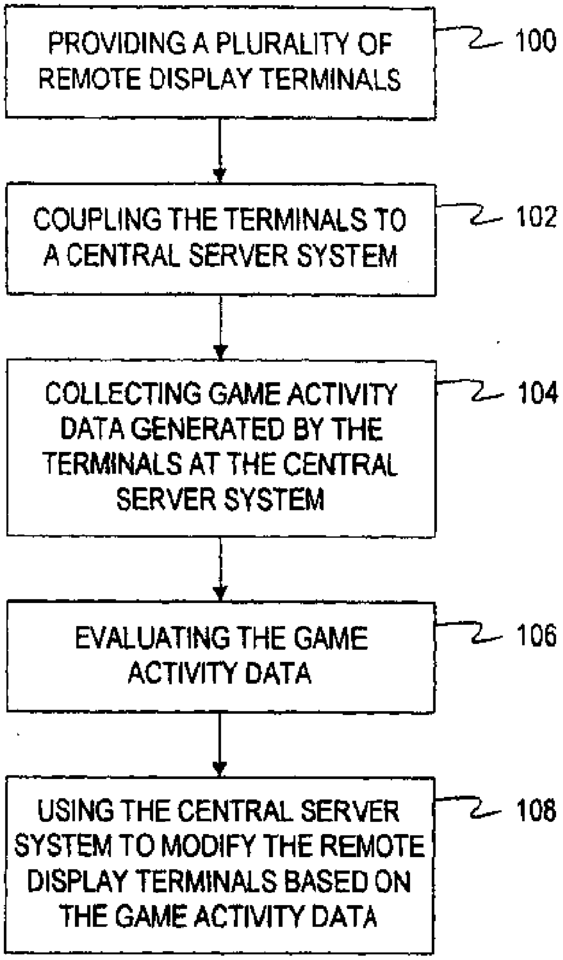

PROVIDING A PLURALITY OF REMOTE DISPLAY TERMINALS
100
COUPLING THE TERMINALS TO A CENTRAL SERVER SYSTEM
102
COLLECTING GAME ACTIVITY DATA GENERATED BY THE TERMINALS AT THE CENTRAL SERVER SYSTEM
104
EVALUATING THE GAME ACTIVITY DATA
106
USING THE CENTRAL SERVER SYSTEM TO MODIFY THE REMOTE DISPLAY TERMINALS BASED ON THE GAME ACTIVITY DATA
108

FIG. 6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 231 577 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
02.01.2003 Bulletin 2003/01

(51) Int Cl.7: G07F 17/32

(43) Date of publication A2:
14.08.2002 Bulletin 2002/33

(21) Application number: 01402888.0

(22) Date of filing: 09.11.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 07.02.2001 US 778351

(71) Applicant: WMS Gaming Inc
Waukegan, Illinois 60085 (US)

(72) Inventor: Giobbi, John J.
Northbrook, Illinois 60062 (US)

(74) Representative: Loisel, Bertrand
Cabinet Plasseraud,
84, rue d'Amsterdam
75440 Paris Cédex 09 (FR)

(54) Centralized gaming system with modifiable remote display terminals

(57) A centralized gaming system comprises a central server system and a plurality of display terminals remote from and linked to the central server system. The central server system includes a master game server, a game execution server, and a database server. The master game server stores a plurality of games of chance. Each game includes respective game play software and respective audiovisual software. In response to one of the games being selected for play at one of the display terminals, the game play software for the selected game is loaded from the master game server into the game execution server and is executed by the game execution server to randomly select an outcome. The audiovisual software for the selected game is selectively executed at the display terminal to visually represent the outcome on a display of the display terminal. The database server collects game activity data based on the outcome and maintains such data for report generation and player tracking purposes. The master game server may evaluate the collected game activity data and, in turn, modify one or more of the display terminals for maximizing earnings and target marketing.

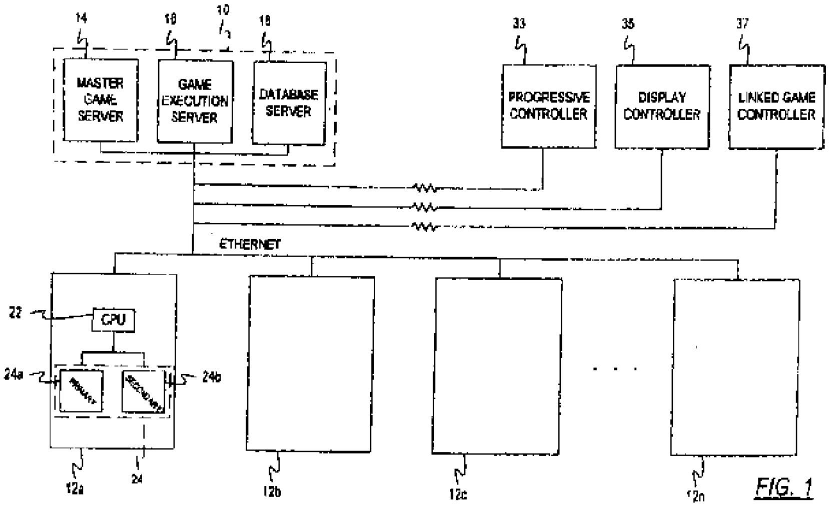


FIG. 1

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2888

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	EP 0 843 272 A (LVOV) 20 May 1998 (1998-05-20) * page 8, line 30 - line 40 * * page 8, line 47 - page 9, line 15; figures 1-7 *	1-26	G07F17/32
X	US 6 117 013 A (EIBA) 12 September 2000 (2000-09-12) * abstract * * column 6, line 30 - line 52; figures *	1-26	
X	WO 99 41718 A (JURACZKO) 19 August 1999 (1999-08-19) * page 3, line 18 - page 4, line 30; figures *	1-26	
X	WO 00 25281 A (GTECH RHODE ISLAND CORP.) 4 May 2000 (2000-05-04) * page 3, line 1 - line 24 * * page 7, line 2 - line 11; figures *	1-26	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
X	US 5 917 725 A (THATCHER ET AL.) 29 June 1999 (1999-06-29) * column 3, line 18 - line 22 * * column 8, line 21 - line 39 * * column 13, line 15 - line 19 * * column 15, line 51 - column 16, line 53; figures 1,2 *	27-54	G07F
X A	EP 1 004 970 A (INTERNATIONAL GAME TECHNOLOGY) 31 May 2000 (2000-05-31) * column 2, line 15 - line 37 * * column 4, line 3 - line 10 * * column 6, line 36 - column 7, line 28; figures *	27-38,54 39-53	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 October 2002	Neville, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

European Patent
Office

Application Number
EP 01 40 2888

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

□ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

□ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

□ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

□ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

□ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2888

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X A	US 5 759 102 A (PEASE ET AL.) 2 June 1998 (1998-06-02) * column 1, line 12 - line 23 * * column 2, line 12 - line 20 * * column 2, line 65 - column 3, line 7 * * column 3, line 51 - column 4, line 23 * * column 4, line 9 - line 16; figures *	27-38,54 39-53	
X	US 4 652 998 A (KOZA ET AL.) 24 March 1987 (1987-03-24) * column 4, line 42 - line 68 * * column 6, line 19 - line 29; figures *	27-38	
X	EP 0 556 840 A (RICOS CO. LTD.) 25 August 1993 (1993-08-25) * column 1, line 13 - line 22 * * column 1, line 40 - line 44 * * column 3, line 45 - line 56 * * column 12, line 13 - line 35; figures *	27-38	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 October 2002	Neville, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 01 40 2888

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1-26

   Gaming executed on a central station and accessed by means of remote display terminals.

2. Claims: 27-38

   Concurrent gaming on remote terminals enabled by download of game software.

3. Claims: 39-54

   Reconfiguration of gaming terminals from a central station according to data gathered concerning gaming activity.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2888

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-10-2002

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 843272	A	20-05-1998	RU	2095112	C1	10-11-1997
			RU	2102790	C1	20-01-1998
			EP	0843272	A1	20-05-1998
			WO	9705557	A1	13-02-1997
			US	6117011	A	12-09-2000
US 6117013	A	12-09-2000	DE	19502613	A1	01-08-1996
			AT	184721	T	15-10-1999
			AU	4664296	A	14-08-1996
			BR	9606847	A	25-11-1997
			CA	2211297	A1	01-08-1996
			CN	1174620	A	25-02-1998
			CZ	9702296	A3	17-12-1997
			DE	59603068	D1	21-10-1999
			WO	9623289	A1	01-08-1996
			EP	0806024	A1	12-11-1997
			FI	973046	A	19-09-1997
			HU	9800695	A2	28-07-1998
			JP	10512984	T	08-12-1998
			NO	973355	A	05-09-1997
			PL	321544	A1	08-12-1997
			SK	101397	A3	04-02-1998
WO 9941718	A	19-08-1999	CZ	9800434	A3	15-03-2000
			AU	2148299	A	30-08-1999
			WO	9941718	A1	19-08-1999
WO 0025281	A	04-05-2000	US	2002019260	A1	14-02-2002
			AU	1100600	A	15-05-2000
			BR	9914897	A	17-07-2001
			EP	1125263	A1	22-08-2001
			WO	0025281	A1	04-05-2000
US 5917725	A	29-06-1999	CA	1245361	A1	22-11-1988
			DE	3522136	A1	09-01-1986
			GB	2161629	A ,B	15-01-1986
			GB	2194369	A ,B	02-03-1988
			HK	101792	A	24-12-1992
			HK	138793	A	24-12-1993
			JP	2112753	C	21-11-1996
			JP	8029189	B	27-03-1996
			JP	61076182	A	18-04-1986
			US	5083271	A	21-01-1992
EP 1004970	A	31-05-2000	AU	5401399	A	20-04-2000
			EP	1004970	A2	31-05-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2888

This annex lists the patent family membersrelating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-10-2002

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 1004970	A		ZA	9906467	A	17-04-2000
US 5759102	A	02-06-1998	AU	705117	B2	13-05-1999
			AU	1267097	A	21-08-1997
			US	6135887	A	24-10-2000
US 4652998	A	24-03-1987	NONE			
EP 556840	A	25-08-1993	JP	5228259	A	07-09-1993
			JP	5237265	A	17-09-1993
			JP	3301634	B2	15-07-2002
			JP	5324509	A	07-12-1993
			JP	3268838	B2	25-03-2002
			JP	6044269	A	18-02-1994
			JP	3268839	B2	25-03-2002
			JP	6044159	A	18-02-1994
			JP	6044160	A	18-02-1994
			AU	672770	B2	17-10-1996
			AU	3312193	A	19-08-1993
			CA	2089774	A1	19-08-1993
			CN	1076537	A ,B	22-09-1993
			DE	69329160	D1	14-09-2000
			DE	69329160	T2	11-01-2001
			EP	0556840	A2	25-08-1993
			EP	0962900	A2	08-12-1999
			ES	2148187	T3	16-10-2000
			US	5547202	A	20-08-1996

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Offenlegungsschrift

(10) DE 199 41 504 A 1

(51) Int. Cl.^{7}:
G 06 F 19/00
H 04 L 12/22
// G06F 161:00

(21) Aktenzeichen: 199 41 504.8
(22) Anmeldetag: 31. 8. 1999
(43) Offenlegungstag: 1. 3. 2001

(71) Anmelder:
Internet Special Services Inc., Appenzell, CH

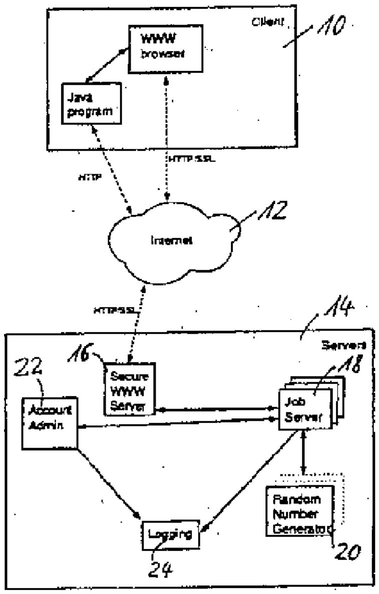
(74) Vertreter:
Brose und Kollegen, 82319 Starnberg

(72) Erfinder:
Meier, Vladimir, Dr., 82008 Unterhaching, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Durchführung von Spielen über das Internet

(57) Verfahren zur Durchführung von Spielen über das Internet mit mindestens einem Teilnehmer mit einem Rechner, wobei das Spiel selbst auf einem Server abläuft, jedoch die gesamt Animation und Benutzerschnittstelle durch ein Programm auf dem Rechner des Teilnehmers dargestellt wird und eine Datenübertragung zwischen Server und Rechner des Teilnehmers nur auf Anforderung des Programms auf dem Rechner des Teilnehmers erfolgt, und solche Anforderungen immer dann erfolgen, wenn der Teilnehmer einen Spielzug durchführt oder eine vorgegebene Zeit T abgelaufen ist.



Beschreibung

Die Erfindung betrifft ein Verfahren zur Durchführung von Spielen über das Internet mit mindestens einem Teilnehmer mit einem Rechner, wobei das Spiel selbst auf einem Server abläuft, jedoch die gesamte Animation und Benutzerschnittstelle durch ein Programm auf dem Rechner des Teilnehmers dargestellt wird.

Solche Verfahren sind im Stand der Technik bereits bekannt. Im einfachsten Fall wird ein Spielzug oder ein Einsatz zur Server übertragen, dieser überträgt dann sofort das Spielergebnis oder den Gewinn/Verlust zurück. Dies läßt sich auch problemlos mit der im Internet-http 1.0-Protokoll vorgesehenen Anfrage des Nutzers-Antwort des Servers-Struktur realisieren.

Sofern jedoch kompliziertere Spiele, wie beispielsweise Roulette oder Black Jack, bei denen das Spielgeschehen komplizierter ist als der Spielzug des Teilnehmer-Ergebnis, oder wenn gar mehrere Teilnehmer gemeinsam Spiele wie Black Jack oder Roulette über das Internet spielen sollen, wobei jeder Teilnehmer auch die Spielzüge der anderen Teilnehmer beobachten kann, ist diese Struktur ungeeignet.

Gemäß dem Stand der Technik war es dann nur möglich, eine permanente TCP-Verbindung zwischen dem Server und allen Teilnehmern aufzubauen und während des ganzen Spieles aufrecht zu erhalten.

Dies führte jedoch zu erheblichen Problemen, da einerseits die meisten an das Internet angeschlossenen Rechner heutzutage durch sogenannte "Firewalls" gegen Manipulationen geschützt sind. Diese Firewalls lassen jedoch lediglich eine ganz geringe Anzahl von gleichzeitigen TCP-Verbindungen zu. Außerdem unterstützt das Internet-Protokoll http 1.0 keine dauernden TCP-Verbindungen. Selbst wenn man diese Probleme jedoch löst, so ist für permanente Verbindungen ein großer Hardware-Aufwand und erhebliche Systemresourcen erforderlich, und die Betriebssysteme der meisten Server können nur eine geringe Zahl dauernd offener Verbindungen handhaben.

Es ist daher Aufgabe der Erfindung, ein solches Verfahren zur Durchführung von Spielen über das Internet vorzuschlagen, bei dem auch komplizierte Spiele mit mehreren Teilnehmern, die ihre Spielzüge gegenseitig beobachten können, möglich sind, ohne daß permanente Datenverbindungen zwischen den Teilnehmern und dem Server aufrecht erhalten bleiben müssen.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß eine Datenübertragung zwischen Server und Rechner des Teilnehmers nur auf Anforderung des Programms auf dem Rechner des Teilnehmers erfolgt.

Erfindungsgemäß ist es besonders bevorzugt, daß Anforderungen zur Datenübertragung immer dann erfolgen, wenn der Teilnehmer einen Spielzug durchführt, oder nach Ablauf einer vorgegebenen Zeit T seit der letzten Anforderung. Dadurch wird sichergestellt, daß für den Teilnehmer selber sein Spielzug, den er gerade durchgeführt hat, sofort auf dem Bildschirm sichtbar wird, während er die Spielzüge anderer Teilnehmer beispielsweise erst nach fünf oder zehn Sekunden auf seinem Bildschirm sieht. Dies stört aber nicht, da der einzelne Teilnehmer ja nicht weiß, wann genau der jeweils andere Teilnehmer seinen Spielzug durchgeführt hat. Scheinbar läuft das System dann so, als ob permanente Verbindungen zwischen den Teilnehmern und dem Server bestehen würden.

Es ist dabei weiter bevorzugt, daß das Programm auf dem Rechner des Teilnehmer jeder Aufforderung zur Datenübertragung einen Authentifizierungscode beifügen muß. Damit wird das Problem gelöst, daß jede Aufforderung zur Datenübertragung (und natürlich auch jeder Spielzug des Teilnehmers) einen neuen Aufbau einer Internet-Verbindung bedeutet. Dabei muß aber gegenüber dem Server jeweils eine Authentifizierung des anrufenden Teilnehmers ermöglicht werden, und gleichzeitig muß der entsprechende Anruf dem richtigen Teilnehmer zugeordnet werden, damit die richtigen Spielstandsdaten übertragen werden können.

Zur Vereinfachung der Abläufe ist es bevorzugt, daß der Authentifizierungscode dabei ursprünglich vom Server erzeugt und dem Rechner des Teilnehmers übermittelt wird.

Es ist dabei besonders bevorzugt, daß der Authentifizierungscode nur in verschlüsselter Form übertragen wird.

Da ohne permanent stehende Verbindungen nicht sichergestellt ist, daß jeder Anruf eines Teilnehmers aus dem Internet rechtzeitig beim Server eintrifft, ist es bevorzugt, daß jede Anforderung und jede Datenübertragung mit einer laufenden Nummer versehen ist. Dadurch können Teilnehmer, Rechner und Server feststellen, ob eine zwischenzeitlich gesendete Anforderung bzw. Datenübertragung verloren gegangen ist.

Bei komplexeren Spielen mit mehreren Teilnehmern besteht das Problem, daß das Spiel erst dann beendet werden kann, wenn jeder Teilnehmer bestimmte Spielzüge vorgenommen hat. Damit müßten alle anderen Teilnehmer auf den "Letzten" warten. Dies kann dann zum Problem werden, wenn beispielsweise die Internet-Verbindung zu diesem Teilnehmer abgerissen ist. Man könnte nun einfach den Einsatz dieses Teilnehmers für verloren erklären, und das Spiel mit den restlichen Teilnehmern zu Ende führen. Dies würde jedoch zu großer Verärgerung bei denjenigen Teilnehmern führen, die ihre Einsätze verlieren und die ja meist für ein Zusammenbrechen der Internet-Verbindung gar nichts können. Es wird daher vorzugsweise vorgeschlagen, daß ein Teilnehmer, der nicht innerhalb einer vorgegebenen Zeit seine Spielzüge durchführt, aus dem Spiel mit mehreren Teilnehmern ausscheidet, und für ihn allein ein weiteres Spiel auf dem Server erzeugt wird. Auf diese Weise kann er allein unter den gleichen Bedingungen weiterspielen, sobald seine Internet-Verbindung wieder hergestellt ist. Sein Einsatz geht ihm nicht verloren.

In diesem Zusammenhang ist es auch bevorzugt, daß dem Teilnehmer eine Zeitanzeige zur Verfügung gestellt wird, die anzeigt, wie lange er noch Zeit hat, seinen Spielzug durchzuführen, damit dieser noch beim gegenwärtigen Spiel vom Server berücksichtigt werden kann.

Da die Laufzeit der entsprechenden Spielzugdaten im Internet nicht präzise vorhergesagt werden kann, und umgekehrt auch eine präzise Synchronisation zwischen Server und Teilnehmer wegen der unterschiedlichen Nachrichtenlaufzeiten auf dem Internet nicht möglich ist, ist es bevorzugt, daß zur Erzeugung der Zeitanzeige der Server bei jeder Datenübertragung eine Information über die für den Spielzug verbleibende Zeit mitsendet, und das Programm auf dem Rechner des Teilnehmers die Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung davon abzieht.

Die vorgenannte Lösung gibt jedoch nur eine grobe Schätzung für die Laufzeit der Daten zwischen Teilnehmerrechner und Server, da sie davon ausgeht, daß diese der Gesamtlaufzeit der Daten zwischen Anforderung durch den Teilnehmerrechner und Ankunft der Daten beim Teilnehmerrechner entspricht.

Es ist daher weiter bevorzugt, daß verschiedene Zonen der Zeitanzeige erzeugt werden, nämlich eine erste Zone, in der die für den Spielzug verbleibende Zeit größer ist als die Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung, eine zweite Zone, in der die für den Spielzug verbleibende Zeit größer ist als die halbe Zeitdauer zwischen Absendung der Anforderung und der

Ankunft der Datenübertragung und eine dritte Zone, in der die für den Spielzug verbleibende Zeit kleiner ist als die halbe Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung.

Auf diese Weise verfügt der Spielteilnehmer über eine recht genaue Information, wie wahrscheinlich es ist, daß seine Spielzüge noch berücksichtigt werden können: So lange sich die Zeitanzeige in der ersten Zone befindet, ist mit größter Wahrscheinlichkeit damit zu rechnen, daß der Spielzug noch ausgeführt werden kann. In der zweiten Zone besteht lediglich eine gewisse Wahrscheinlichkeit dafür, und in der dritten Zone ist es nahezu ausgeschlossen, daß der Spielzug noch rechtzeitig durchgeführt werden kann.

Die vorliegende Erfindung wird im folgenden anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert. Es zeigt:

Fig. 1 den grundsätzlichen Aufbau der erfindungsgemäßen Datenverbindungen.

Der technische Aufbau der vorliegenden Erfindung umfaßt einen Client **10**, das heißt ein Programm, welches auf dem Rechner des Spielteilnehmers läuft. Dieses steht über http bzw. abhörgeschützte http/ssl-Verbindungen mit dem Internet **12** in Verbindung. Über das Internet **12** ist eine weitere Verbindung im http/ssl-Protokoll mit dem Rechner **14**, den beispielsweise ein Internet-Spielcasino betreibt, verbunden. Auf diesem Rechner **14** laufen verschiedene Server, wobei die Nachrichten aus dem Internet **12** zuerst einem sicheren www-Server **16** zugeleitet werden. Dieser steht mit den einzelnen Job-Servern **18**, das heißt, den Programmen, auf denen die einzelnen Spiele laufen, in Verbindung. Die Job-Server **18** sind mit einem Zufallszahlengenerator **20**, der Kontoverwaltung **22**, die die Konten der einzelnen Spieler verwaltet, und einer Protokolliereinheit **24** verbunden.

Das Client-Programm **10** ist ein Programm, das auf dem Spielercomputer läuft und das die Schnittstelle zum eigentlichen Spiel verkörpert. Es zeigt dem Spieler den aktuellen Spielstand an und kommuniziert für ihn mit dem Spiele-Server, der praktisch ein Bestandteil des Internet-Spielecasinos ist. Der Spiele-Server ist ein Programm, das für den Benutzer das Spiel realisiert. Er akzeptiert alle seine Spielzüge und reagiert auf sie. Ein Spiele-Server kann im Prinzip für eine beliebige Anzahl von Spielen zuständig sein. In der Regel wird jedoch ein Server nur einen bestimmten Spieltyp bedienen.

Der Spiele-Server kontaktiert die Datenbank für jeden Spielzug, um die Benutzerdaten zu überprüfen und das Resultat zu speichern. Diese Kommunikation ist für den Spieler transparent, denn er sieht keine Details aus der inneren Struktur des Spiele-Servers **18**.

Jeder Spieler benutzt ein lokales Programm **10**, das mit dem Spiele-Server **18** kommuniziert. Dieses benutzt entweder nur den www-Browser, den Browser erweitert durch "Plug In's", "Applets" oder ähnliches, oder ein selbständig ausführbares Programm. Jedes Spiel wird zuerst aus einer oder mehreren Spielauswahlseiten ausgewählt. Danach wird ein neues Spielfenster geöffnet, es zeigt die Spielgraphik an und der Spieler kann anfangen zu spielen. Er kann zuerst seinen Einsatz wählen, der ganz einfach (Slot-Machine), oder ganz kompliziert (Roulette) sein kann, und schließlich fordert er einen neuen Spielzug an. Das Spieler-Programm **10** kann dann eine Animation starten, z. B. das Roulette-Rad drehen, es sendet eine Nachricht an den entsprechenden Spiele-Server und wartet auf die Antwort. Wenn die Antwort des Servers kommt, stoppt das Programm die Animation, zeigt das Resultat an und wartet auf weitere Benutzeraktionen.

Auf diese Weise kann ein virtuelles Spielcasino im Internet realisiert werden, und bei entsprechender Absicherung der Datenkommunikation kann sogar um "richtiges" Geld gespielt werden.

Dabei müssen jedoch die Probleme der Kommunikation über das Internet berücksichtigt werden. Da die Internet-Kommunikation nicht 100-prozentig verläßlich ist, kann es passieren, daß die Server-Antwort zu spät, nur teilweise, oder überhaupt nicht ankommt. In diesem Fall muß der Spieler die Möglichkeit haben, den Spielzug zu wiederholen, so daß eine neue und hoffentlich erfolgreichere http-Verbindung mit dem Server zustande kommen kann. Dabei macht es keinen Unterschied, ob der Server die letzte Spieler-Nachricht bekommen hat, aber seine Antwort verloren ging, oder ob er sie überhaupt nicht bekommen hat, da erfindungsgemäß in beiden Fällen das Resultat richtig bearbeitet werden muß. Wenn ein Spielzug vom Server nicht ausgeführt wird, und daher keine entsprechende Rückmeldung erfolgt ist, muß der Spieler lediglich erneut das entsprechende Display-Element anklicken.

Während des Spiels kontaktiert das Client-Programm **10** den Server **18** in regelmäßigen Abständen und fordert den neuesten Spielstand an. Die Kommunikation wird dabei immer von dem Client-Programm **10** gestartet: Es sendet eine Nachricht an den Spiele-Server **18** und der Server **18** schickt ihm eine Antwort zurück.

Es ist daher erforderlich, daß ein entsprechendes Client-Programm **10** auf dem Rechner des Spielteilnehmers verfügbar ist. Dieses Programm kann entweder ebenfalls über Internet oder aber auf CD-Rom zur Verfügung gestellt werden. Im ersteren Falle kann das Programm einmal aus dem Internet geladen und dann auf der Festplatte des lokalen Rechners beim Teilnehmer gehalten werden.

Während eines Spiels mit mehreren Mitspielern muß jeder Mitspieler in der Lage sein, den gegenwärtigen Spielstand zu sehen, der Einsätze und andere Spielzüge aller anderen Mitspieler umfaßt. Nachdem jede Kommunikation nach dem Internet-Protokoll immer von dem Client angefordert werden muß, hat der Server keine Möglichkeit, dem Client mitzuteilen, daß sich der Spielstand geändert hat. Der Server muß vielmehr warten, bis der Client den aktuellen Spielstand abfragt. Daraus folgt, daß die Clients den Server in regelmäßigen Abständen abfragen müssen, auch wenn ihr Spieler keine Aktion ausführt. Dies könnte unbefriedigend erscheinen im Vergleich zu Spielstandsaktualisierungen, die durch den Server bei jeder Änderung des Spielstands veranlaßt werden. Es ist jedoch tatsächlich die einzig ausführbare Art, um im vorliegenden Fall Aktualisierungen des Spielstandes zu verbreiten. Wenn das Spiel P Mitspieler hat, und jeder von ihm B Einsätze oder andere Spielzüge während eines Spiels durchführt, müßte der Server $B \cdot P^2$ Aktualisierungsmeldungen an die Clients schicken. Bei Abfrage durch den Client, und unter Annahme von N Abfragen pro Spiel, muß der Server lediglich $P \cdot (B+N)$ Mitteilungen senden, wodurch Spiele mit wesentlich mehr Teilnehmern realisiert werden können.

Der Spielstand muß in regelmäßigen Abständen, beispielsweise im Abstand von 10 Sekunden abgefragt werden. Die Abfragen sollten jedoch nicht zu häufig erfolgen, damit nicht zuviel Datenverkehr beim Server anfällt. Die regelmäßige Abfragefrequenz von N Sekunden wird nur unterbrochen, wenn der eigene Spieler einen Spielzug macht: Mit der zugehörigen Antwort sendet der Server auch den gesamten Spielstand. Die nächste Erneuerung des Spielstandes kann deshalb nach N Sekunden nach der Antwort auf den Spielzug statt N Sekunden nach der letzten Erneuerung des Spielstandes erfolgen. Auf diese Weise hat der Spieler den Eindruck, daß die entsprechenden Spielzüge in Echtzeit angezeigt werden, da er seine eigenen Spielzüge sofort im Spielstand berücksichtigt findet. Hinsichtlich der Spielzüge der anderen Mitspieler fehlt ihm ja eine zeitliche Zuordnung. Das erfindungsgemäße Verfahren erweckt daher bei jedem Mitspieler den Eindruck eines "echten" Echtzeitbetriebs, obwohl die Spielstände eigentlich nur in Zeitabständen von 10 oder 15 Sekunden erneuert werden.

Ein weiteres Problem, welches das erfindungsgemäße Verfahren löst, beruht darauf, daß Spiele mit mehreren Mitspielern eine Synchronisation zwischen den Spielern und dem Server erfordern. Dies ist schon in einem lokal verteilten System schwierig genug, und ist natürlich in einem Internet-System noch schwieriger, da das Internet keine festen Nachrichtenlaufzeiten bietet.

Der Client muß nämlich beispielsweise wissen, wann der letzte Zeitpunkt gekommen ist, um eine Mitteilung zu schikken, so daß diese den Server vor dem Ablauf einer bestimmten Zeit, beispielsweise der Zeit zum Setzen im Roulette, erreicht. Dies bedeutet, daß der Client die Serverzeit als auch seine eigene Zeitdistanz zu dem Server kennen muß, um seine Aktionen mit dem Server zu synchronisieren.

Erfindungsgemäß wird diese Synchronisation mit einem sehr einfachen Verfahren erreicht, welches darauf beruht, daß die Rundlaufzeit gemessen wird, d. h. die Laufzeit zwischen der Absendung einer Nachricht vom Client bis zu dem Zeitpunkt, an dem die Antwort des Servers vorliegt. Zusätzlich enthält jede Nachricht des Servers bei Spielen mit mehreren Teilnehmern die Variable "Server-Zeit". Dies kann beispielsweise eine ganzzahlige Zahl sein, die jede Sekunde während der Betriebsdauer des Servers heraufgezählt wird. Die Clients nutzen diese zusammen mit der gemessenen Rundlaufzeit ihrer Mitteilungen, um daraus die aktuelle Server-Zeit abzuleiten. Wenn der Client beispielsweise einen Server-Zeit-Wert von 100 zurückgeschickt bekommt, und die Rundlaufzeit 6 Sekunden betrug, kann der Client mit einiger Sicherheit darauf schließen, daß zu dem Zeitpunkt, an dem er die Nachricht vom Server erhalten hat, die Server-Zeit 103 betragen hat, und daß es 3 Sekunden dauert, um den Server zu erreichen. Nehmen wir nun an, daß bei dem nächsten Nachrichtenaustausch die Rundlaufzeit 12 Sekunden beträgt. In diesem Fall weiß der Client, daß seine laufende Annahme hinsichtlich der Server-Zeit genauer ist als die neue, weil nun die Rundlaufzeit länger ist und es nicht möglich ist, festzustellen, ob beide Übertragungswege der Nachricht die gleiche Zeit gebraucht haben, oder ob einer nur eine Sekunde und der andere 11 Sekunden gebraucht hat. Andererseits weiß der Client nun, daß er die Nachricht 6, und möglicherweise sogar 12 Sekunden eher senden muß, um den Server noch rechtzeitig zu erreichen. Wenn der nächste Nachrichtenaustausch eine Rundlaufzeit von 4 Sekunden erreicht, kann der Client seine Annahme für die Server-Zeit korrigieren, aber er sollte den Sicherheits-Zeitabstand nicht korrigieren, es sei denn, daß die meisten der folgenden Nachrichten ähnliche Übertragungsgeschwindigkeiten erreichen.

Auf diese Weise sieht man, daß mit jedem neuen Nachrichtenaustausch der Client eine genauere Annahme hinsichtlich der Server-Zeit hat und über mehr Daten verfügt, um zu schätzen, wie lang es dauert, um den Server zu erreichen. Diese Daten sollten in einer bequemen Weise angegeben werden:

Die verbleibende Zeit bis zum Ablauf der Frist zur Durchführung eines Spielzuges (in Server-Zeit) sollte immer angezeigt und aufgefrischt werden,

der mittlere Abstand, also die Zeit, die notwendig ist, um den Server zu erreichen sollte ebenfalls angezeigt werden.

ein farbiges Kästchen kann zeigen, ob es ziemlich sicher ist, daß der Server rechtzeitig erreicht werden kann (grün), wann es weniger wahrscheinlich wird (gelb oder orange) und wenn es sehr unwahrscheinlich oder unmöglich ist (rot).

Alle diese drei Angaben könnten auch beispielsweise als Analog-Uhr mit zwei farbigen Zeigern oder als eine Digital-Uhr mit zwei Anzeigen dargestellt werden, wobei eine die Server-Zeit und die andere die Server-Zeit plus Laufzeit zwischen Client und Server anzeigt. Der farbige Hintergrund der Uhren kann dann seine Farbe entsprechend ändern.

Beim Roulette-Spiel ist diese Synchronisation im wesentlichen nur nötig, damit der Mitspieler weiß, bis wann er seine Einsätze noch setzen oder ändern kann und wann das "rien ne va plus" auftritt.

Wesentlich komplizierter ist die Situation jedoch bei Black Jack, da dieses Spiel definierte Spielabschnitte (Setzen, Spielen) hat, und alle Spieler ihre Aktionen rechtzeitig durchführen müssen. Bei einem Spiel übers Internet verzichtet man vorzugsweise auf die normale Regel, daß alle Spieler sequentiell nacheinander spielen müssen, da der Spiel-Server im Gegensatz zu einem menschlichen "Black Jack-Dealer" mehrere Spieler gleichzeitig bedienen kann und die Erzwingung einer Reihenfolge das Spiel wesentlich langsamer und wesentlich abhängiger von Spielern machen würde, die nur eine sehr langsame Internet-Verbindung haben.

Wenn ein Spieler trotzdem seine erforderlichen Aktionen nicht rechtzeitig durchführt, wird er aus dem Spiel mit mehreren Teilnehmern entfernt und an einen "Privat-Tisch" versetzt, wo er allein spielt und keine Zeitbeschränkungen zur Beendigung des Spiels hat. Er kann sogar das Spiel unterbrechen und später weiterspielen. Der Übergang von einem Spiel mit mehreren Teilnehmern an einen Privat-Tisch wird vom Server über ein "Private"-Flag an den Client mitgeteilt. Wenn das Client-Programm diese Meldung erhält, muß es den Spieler darüber informieren, daß er aus dem ursprünglichen Spiel entfernt worden ist. Dies muß in unmißverständlicher Weise geschehen. Üblicherweise passiert es dadurch, daß die Art, in der das Spiel am Bildschirm des Teilnehmerrechners dargestellt wird, geändert wird, so daß der Spieler weiß, was passiert ist.

Bei all diesen Spielen sendet der Server nach jeder Abfrage des Clients stets den gesamten Spielzustand, d. h. es werden keine inkrementellen Änderungen übertragen. Dadurch gibt es weniger Probleme, wenn eine Rückmeldung vom Server an den Client ausgefallen ist. Das Client-Programm muß prüfen, ob sich der Spielstand geändert hat, und dementsprechend die Anzeige aktualisieren. Wenn beim Roulette ein neues Spiel beginnt, wird der Tisch (wie im echten Casino) abgeräumt. Das würde normalerweise den letzten Einsatz des Spielers und das letzte Spielergebnis löschen, möglicherweise bevor der Spieler genügend Zeit hatte, das Spielergebnis zu betrachten, oder bei sehr langsamen und schlechten Internet-Verbindungen sogar bevor das Spielergebnis vollständig übertragen worden ist. Um dieses Problem zu lösen, schlägt die vorliegende Erfindung vor, diese Information dem Spieler zusätzlich auf bequeme Weise zugänglich zu machen. Beispielsweise kann der Spieler selbst entscheiden, wann der Tisch abgeräumt ist und ein neuer Spielstatus abgefragt ist, oder das letzte Ergebnis kann gespeichert und vom Spieler durch Anklicken einer Schaltfläche nochmals dargestellt werden. Ebenso könnte das Client-Programm auch einige oder alle frühere Einsätze und die entsprechenden Spielergebnisse zwischenspeichern und diese dem Spieler auf Anforderung zugänglich machen.

Wenn ein Spieler beim Roulette während einiger aufeinanderfolgender Spiele keine Einsätze macht, wird er ebenfalls an einen Privat-Tisch versetzt. Um den Benutzer zu warnen, daß er bald versetzt werden wird, sendet der Server mit allen Übertragungen von Spielzustandsdaten eine entsprechende Meldung während der letzten Runde vor Ablauf der Zahl der Spiele. Das Client-Programm kann dann rechtzeitig eine entsprechende Warnung ausgeben.

Erfindungsgemäß ist es auch möglich, daß ein Teilnehmer nur als "Gast" teilnimmt. Er benötigt dann kein Konto, kann dafür aber auch keine Einsätze machen. Das Client-Programm dieses Teilnehmers fragt dann nur alle N Sekunden den Spielstand ab und stellt diesen dann nach Übermittlung durch den Server auf dem Bildschirm dar. Wenn der Besucher zu lange bleibt, kann der Server ihn nach einiger Zeit entfernen und weitere Anforderungen des Client-Programms mit einer entsprechenden Fehlermeldung beantworten.

Hinsichtlich der Zeitsynchronisation ist es erfindungsgemäß besonders bevorzugt, daß der Server mit jeder Antwort die Server-Zeit überträgt, die noch übrig ist, bis das Spiel (oder der entsprechende Teil des Spiels) endet und die ursprüngliche Gesamtlänge des gesamten Zeitintervalls. Der Client muß die Rundlaufzeit einer Meldung berücksichtigen, die zwischen dem Client und dem Server ausgetauscht wird, und die verbleibende Zeit sowohl als Client als auch als Server-Zeit anzeigen. Mit jeder Meldung, die er von dem Server erhält, bekommt der Client eine genauere Schätzung der Server-Zeit und kann sich synchronisieren, selbst wenn die Rundlaufzeit sich ändert. Wenn die Zeit in einem graphischen Balken dargestellt wird, entspricht die gesamte Balkenlänge der Länge des Gesamtintervalls und die abgelaufene Länge der bereits vergangenen Zeit.

Das im Internet übliche http-Protokoll weist darüber hinaus noch die Problematik auf, daß es darin nicht möglich ist, Meldungen, die auf vorherigen Aktionen beruhen, zu identifizieren. Erfindungsgemäß wird daher vorgeschlagen, ein sogenanntes "Zugangs-Zertifikat" (Access Certificate = AC) jeder Meldung hinzuzufügen, um dem Kommunikationsverfahren Stabilität zu verleihen und gleichzeitig die Meldungen der einzelnen Spieler zu identifizieren. Das AC dient einem doppelten Zweck: Zuerst dient es dazu, Meldungen von Spielern zu identifizieren, die sich vorher erfolgreich eingeloggt haben, und zweitens zur Einführung von Stabilität. Wenn eine Meldung vom Client zum Server oder die Antwort des Servers verloren worden ist, weiß der Client nicht, ob seine Anforderung akzeptiert worden ist oder nicht und so kann er nicht wissen, ob er sie wiederholen soll oder nicht. Dies ist aber ein sehr wichtiger Unterschied, denn wenn der Server die Anforderung nicht erhalten hat, kann der Spieler ewig auf die Antwort warten. Wenn andererseits der Spieler die Anforderung wiederholt und der Server sie doppelt erhält, könnte er beispielsweise den Einsatz zweimal setzen oder zwei neue Karten ziehen, ohne dies zu wollen.

Das AC hilft dieser Problematik ab. Mit dem AC kann der Server Originalanforderungen von denen unterscheiden, die beispielsweise von einem ungeduldigen Benutzer erzeugt wurden, der eine Schaltfläche mehrfach angeklickt hat, bevor er eine Bestätigung erhalten hat. Die vorliegende Erfindung benutzt einen Meldungsparameter, um dem Benutzer mitzuteilen, daß seine Anforderung mehrfach empfangen worden ist und nur die erste Anforderung akzeptiert worden ist.

Erfindungsgemäß können die Access Certificates auch als Zugangskennung dienen. Nachdem ja auf dem Internet für jede Mitteilung vom Client zum Server eine neue Verbindung eröffnet werden muß, muß sich der Client jedes Mal authentifizieren, wenn er Kontakt mit dem Server aufnimmt. Es ist dem Benutzer aber nicht zuzumuten, jedes Mal ein Passwort einzugeben, wenn er einen Spielzug vornimmt.

Erfindungsgemäß wird daher vom Server an den Client eine Antwort geschickt, die ein Access Certificate enthält, wenn der Benutzer erfolgreich eingeloggt hat. Das Access Certificate ist eine Folge von Bytes, die bestätigen, daß dieser Benutzer sich erfolgreich eingeloggt hat und daß er berechtigt ist, an den Spielen unter Benutzung eines bestimmten Kontos teilzunehmen. Jedes AC gilt für einen bestimmten Zeitraum. Wenn es in diesem Zeitraum für mindestens ein Spiel benutzt worden ist, sendet das System dem Client ein neues, frisches AC. Auf diese Weise kann der Benutzer die ganze Zeit spielen, ohne sich erneut einzuloggen. Diese Möglichkeit läuft aber nach einer bestimmten Zeit, in der der Benutzer nicht gespielt, ab.

Es ist dabei zu beachten, daß das AC in einem gesicherten Übertragungsverfahren, beispielsweise mit der SSL-Technik übertragen werden muß, da jeder Dritte, der das AC abhört, auf Rechnung eines anderen spielen kann.

Da man durch Erraten eines gültigen AC's dieses zum Spielen verwenden könnte, muß das AC eine ausreichend lange Zufallsfolge von Bytes umfassen, um "Brute force attacks" durch ausprobieren entsprechend vieler Kombinationen sinnlos zu machen. Eine Kopie des AC wird in der Datenbank der Server gespeichert, so daß die Gültigkeit stets überprüft werden kann.

Ein Benutzer könnte zwar sein eigenes AC verwenden und damit Betrügereien versuchen. Die ist jedoch kein Problem, da die Lebensdauer eines AC's beschränkt ist und es auf jeden Fall nur für das eigene Konto des Benutzers verwendet werden kann.

Erfindungsgemäß enthält das AC folgende Daten:

1. Eine Zufallsfolge von Bytes
2. Einen Account Index, der es erlaubt, den Bereich der Datenbank zu finden, der die Daten des Benutzers enthält. Dies kann die Kontonummer oder ein weniger auffälliger Schlüssel dafür sein.

Die erfindungsgemäße Aufteilung der Spielprogramme auf Client und Server ermöglicht also Spiele ohne permanente Rechner-Verbindung, insbesondere mit mehreren Teilnehmern gleichzeitig, die gegenseitig ihr Spiel beobachten können, einen geringeren Telekommunikationsverkehr und eine Sprachunabhängigkeit des Servers, da alle Ausgaben die in Sprache erfolgen müssen, durch das Client-Programm durchgeführt werden können, während die Kommunikation mit dem Server nur durch einheitliche Codes erfolgt.

Patentansprüche

1. Verfahren zur Durchführung von Spielen über das Internet mit mindestens einem Teilnehmer mit einem Rechner, wobei das Spiel selbst auf einem Server abläuft, jedoch die gesamte Animation und Benutzerschnittstelle durch ein Programm auf dem Rechner des Teilnehmers dargestellt wird, **dadurch gekennzeichnet**, daß eine Datenübertragung zwischen Server und Rechner des Teilnehmers nur auf Anforderung des Programms auf dem Rechner des Teilnehmers erfolgt.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, daß Anforderungen zur Datenübertragung immer dann erfolgen, wenn der Teilnehmer einen Spielzug durchführt, oder nach Ablauf einer vorgegebenen Zeit T seit der letzten Anforderung.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Programm auf dem Rechner des Teilnehmers jeder Anforderung zur Datenübertragung einen Authentifizierungscode beifügen muß.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der Authentifizierungscode ursprünglich vom Server erzeugt und dem Rechner des Teilnehmers über-

mitteilt wird.

5. Verfahren nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß der Authentifizierungscode nur in verschlüsselter Form übertragen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß jede Anforderung und jede Datenübertragung mit einer laufenden Nummer versehen ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, mit mehreren Teilnehmern, dadurch gekennzeichnet, daß ein Teilnehmer, der nicht innerhalb einer vorgegebenen Zeit seine Spielzüge durchführt, aus dem Spiel mit mehreren Teilnehmern ausscheidet, und für ihn allein ein weiteres Spiel auf dem Server erzeugt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7 mit mehreren Teilnehmern, dadurch gekennzeichnet, daß dem Teilnehmer eine Zeitanzeige zur Verfügung gestellt wird, die anzeigt, wie lange er noch Zeit hat, seinen Spielzug durchzuführen, damit dieser noch beim gegenwärtigen Spiel vom Server berücksichtigt werden kann.

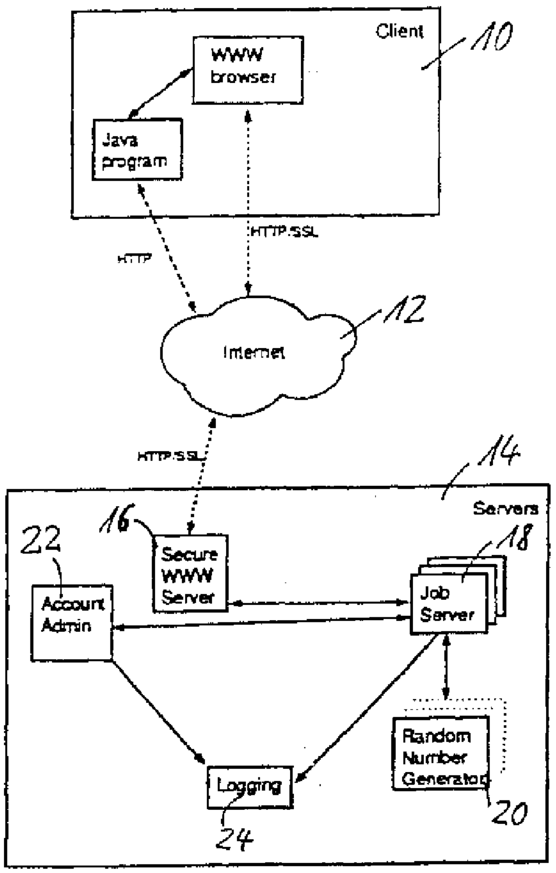
9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß zur Erzeugung der Zeitanzeige der Server bei jeder Datenübertragung eine Information über die für den Spielzug verbleibende Zeit mitsendet, und das Programm auf dem Rechner des Teilnehmers die Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung davon abzieht.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß verschiedene Zonen der Zeitanzeige erzeugt werden: eine erste Zone, in der die für den Spielzug verbleibende Zeit größer ist als die Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung, eine zweite Zone, in der die für den Spielzug verbleibende Zeit größer ist als die halbe Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung, und eine dritte Zone, in der die für den Spielzug verbleibende Zeit kleiner ist als die halbe Zeitdauer zwischen Absendung der Anforderung und der Ankunft der Datenübertragung.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Fig. 1


Client
10
WWW browser
Java program
HTTP
HTTP/SSL
Internet
12
HTTP/SSL
14
Servers
16
Secure WWW Server
18
Job Server
22
Account Admin
Random Number Generator
20
Logging
24

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 120 757 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.08.2001 Bulletin 2001/31

(51) Int Cl.7: G07F 17/32, G07C 9/00

(21) Application number: 01101836.3

(22) Date of filing: 26.01.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 27.01.2000 US 491899

(71) Applicant: International Game Technology
Reno, Nevada 89511 (US)

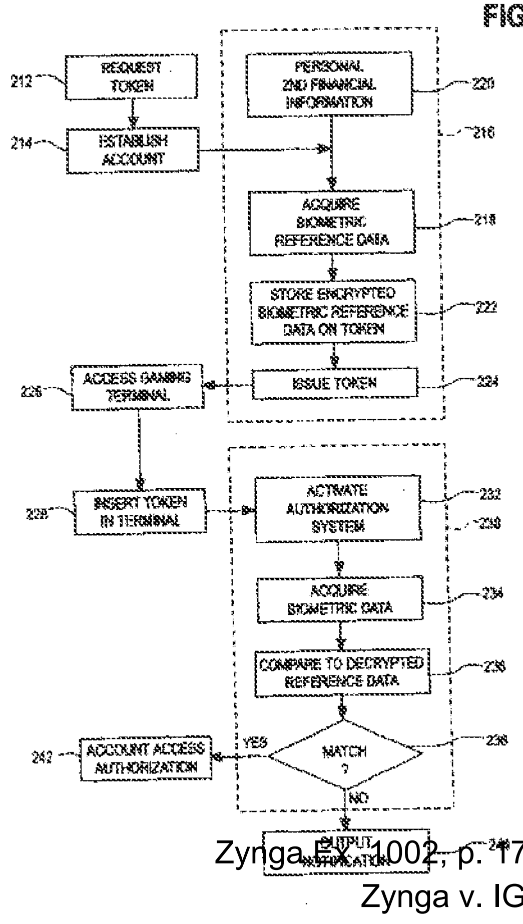
(72) Inventors:
- Wells, William R.
  Reno, Nevada 84502 (US)
- Wilder, Richard
  Sparks, Nevada 89436 (US)
- Mattice, Harold E.
  Gardnerville, Nevada 89410 (US)
- Griswold, Chancey W.
  Reno, Nevada 89509 (US)

(74) Representative: Manitz, Finsterwald & Partner
Postfach 22 16 11
80506 München (DE)

(54) Gaming terminal and system with biometric identification

(57) A gaming system is provided with biometric facilities for identifying or verifying the identity of a player or perspective player. In one aspect reference biometric data is stored in a portable biometric data storage device such as a smart card, PCMCIA card or the like and is preferably left in the possession or control of the individual or individuals to whom the biometric data relates. The reference biometric data is read in individual gaming terminals and compared, in individual gaming terminals to measured biometric data of a player or perspective player. In one aspect, gaming terminals use biometric verification or indication to implement a practical and feasible cashless gaming terminal.

FIG. 2


212
REQUEST TOKEN
214
ESTABLISH ACCOUNT
PERSONAL 2ND FINANCIAL INFORMATION
220
216
ACQUIRE BIOMETRIC REFERENCE DATA
218
STORE ENCRYPTED BIOMETRIC REFERENCE DATA ON TOKEN
222
226
ACCESS GAMING TERMINAL
ISSUE TOKEN
224
228
INSERT TOKEN IN TERMINAL
ACTIVATE AUTHORIZATION SYSTEM
232
230
ACQUIRE BIOMETRIC DATA
234
COMPARE TO DECRYPTED REFERENCE DATA
236
242
ACCOUNT ACCESS AUTHORIZATION
YES
MATCH ?
238
NO
OUTPUT NOTIFICATION
244

Description

[0001] The present application claims priority in U.S. Provisional Patent Application Serial Number 60/153,745, filed Sept. 13, 1999, incorporated herein by reference.

[0002] The present invention relates to a gaming system organizer terminal, such as a slot machine, electronic card game terminal and the like, including a biometric facility and, in particular, a gaming system or terminal and biometric facility identifying, or verifying identity of, a player or wagerer.

BACKGROUND INFORMATION

[0003] The majority of gaming terminals including casino gaming terminals such as mechanical or electronic slot machines, keno machines, poker, blackjack or other card playing machines, and the like operate on a coin, cash or token basis, i.e., accept wagers in the form of government-issued coins, casino-minted tokens, and/or standard cash. Although some gaming devices or systems permit wagers based on standard credit or debit cards, there has been some reluctance in the gaming industry to wide-spread adoption of such devices, both on the part of casinos (and other gaming operators) and on the part of players. It is believed that at least some part of the reluctance arises from a perception that wide-spread adoption of credit or debit cards for gaming could lead to unauthorized usage of such cards, such as use of stolen or lost cards. If it was possible to implement a system which could prevent, reduce or detect unauthorized card usage, a number of benefits could be realized. The entertainment value of a gaming device to a player would be enhanced because there would be reduced need for a player to obtain, transport, control and use relatively bulky and/or cumbersome coins, or cash. Game operators could potentially benefit by developing gaming terminals or systems which had little or no need for cash or coin handling, thus simplifying or eliminating items such as the design, fabrication, installation, and maintenance of coin or cash handling devices, resupplying devices with coins or cash, developing and maintaining appropriate security procedures and systems for handling relatively large amounts of coins and cash and the like.

[0004] In many current gaming terminals, a relatively large portion of the volume, mass and cost of a gaming terminal is attributed to coin or cash handling devices. If the need for such devices is reduced or eliminated, a resultant reduction in volume, size and cost of gaming terminals can not only be of immediate benefit in context of current casinos and other gaming systems but also provides an opportunity to develop additional gaming markets. Accordingly, it would be useful to provide a gaming terminal and system which can facilitate the development of and/or use of gaming terminals while reducing or eliminating the need for coin or cash handling devices, such as to facilitate a card-based or other cashless gaming terminal.

[0005] In non-gaming contexts a number of systems have been proposed for implementing machine-measurement of human features or characteristics. For example, biometric measurement devices are available for use in connection with automatic teller machines and for use with personal computers. Such biometric systems include retinal, iris, or fingerprint scans, voice print or voice recognition systems, facial recognition systems and the like. In a typical biometric system, reference biometric data for known individuals is stored in a central computer or other central data repository. When it is desired to identify or verify identity of a person, appropriate biometric data for such individual is measured and such measurements are compared to the previously-stored data in the central repository. Although such systems are useful in many contexts, they are believed to be less than ideal for use in the gaming industry for a number of reasons. It is believed that many gaming industry patrons (as well as many members of the general public) are reluctant to use a system which requires personal information such as fingerprint, retinal scan, iris scan or other biometric information, to be stored in a central location, effectively out of the individual's possession and control. Accordingly, it would be useful to provide a system for biometric identification or identity verification (authentication) which permits a user to effectively maintain possession and control of his or her biometric information.

[0006] Systems which store reference biometric data in a central computer or other central repository necessarily require access to such reference data in performing a verification or authentication or identification. In the context of the gaming industry, where players typically wish to have freedom to move from terminal to terminal, or game to game, with relative ease, previous approaches would require each terminal to have the facility for remote access to the central data repository. Providing remote access in a system that potentially has thousands of gaming terminals would involve a computer network or other remote access system with a relatively high (and accordingly expensive) bandwidth and, even with relatively advanced communication systems, it was believed such a system would involve substantial delay for a player each time the player moves from one terminal to another. It is believed that, while individuals might tolerate a degree of delay in certain non-gaming biometric verification or identification procedures, it is likely there would be relatively low tolerance for delay in the gaming industry. Accordingly, it would be useful to provide a (preferably lightweight, portable and low cost) biometric identification or authentication system in which cost of bandwidth and delay associated with the central storage of biometric data on a computer or similar system can be reduced or eliminated.

SUMMARY OF THE INVENTION

[0007] The present invention involves a recognition of certain problems and deficiencies in previous approaches, including as described herein. According to one aspect, reference biometric information, rather than being stored in a central repository, is stored in a small portable biometric data storage device ("BDSD") which the player can readily retain in his or her possession and under his or her control. In one aspect, the portable BDSD also stores debit, credit or other financial information and thus can operate as a credit card or debit card. The BDSD preferably is substantially in a standard format such as in a "smart card" format, PCMCIA format or the like. In this manner, when a player wishes to employ the BDSD for placing a wager or other gaming purposes, appropriately configured gaming terminals can obtain (measure) biometric data of the person attempting to use the BDSD and can compare such data with the previously-stored biometric data of the authorized user of the BDSD. In this way it is possible to use the safeguards afforded by biometric systems while allowing players to retain possession and control of the biometric data and avoiding costs and delays associated with central or remote storage of biometric reference data.

[0008] According to one aspect of the invention, a practical cashless gaming terminal is provided which includes biometric identification or verification. According to this aspect of the invention, a gaming terminal is provided in the absence of some or all components of typical coin handling or cash handling apparatus and systems. As used herein, coin handling, BDSD handling an currency handling equipment refers to equipment for physically moving and/or recognizing physical coins, physical BDSDs or physical paper currency.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009]

Fig. 1 is a schematic perspective view of components of a gaming system according to one embodiment of the present invention;

Fig. 2 is a flow chart depicting a process involving biometric identification or verification according to one embodiment of the present invention;

Fig. 3 is a perspective view of a cashless gaming terminal of the type which may be used in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0010] In one embodiment, as illustrated in Fig. 1, a user wishing to engage in gaming using the systems described herein would initiate or request a issuance or validation of a smart card or other BDSD. Although a number of registration procedures can be used, including those described below, in one scenario provided as an example, a user would request or initiate registration, e.g., from a registration desk 112 for example at a customer service counter or location in a casino, hotel or other location. In some configurations registration is performed by a hotel and may be accomplished substantially simultaneously with, or as part of a hotel registration procedure, e.g., such that all guests are issued a gaming smart card or other BDSD, e.g., having a small complimentary balance, augmentable on the casino floor, to introduce or encourage use of a smart card or BDSD.

[0011] When a prospective player approaches a registration desk 112 and requests a BDSD 212, if the prospective player has not already established an account, account establishment will be initiated 214. The registration entity will perform a number of steps including, in the depicted embodiment, acquiring biometric reference data 218 and, in at least some embodiments, obtaining personal and/or financial information 220 relative to the prospective player. The personal and financial information can include information such as name, address, social security or tax identification number, local hotel or other address, credit card or bank account information and the like. In some embodiments, the smart card or other BDSD will be used to store information indicative of a current balance available to the prospective player for wagering. In these embodiments, the player may provide funds directly to the registration entity in the form a check, account charge and/or cash payment, whereupon the appropriate balance will be recorded on the smart card or other BDSD.

[0012] The type of biometric reference data acquired 218 will depend on the system being used. Examples include storing the results of a fingerprint scan, retinal scan, iris scan, voice print, earfold scan, facial scan and the like. In the embodiment depicted in Fig. 1, a finger or thumb print scan window 114 is provided at the registration site 112. A number of thumb print or fingerprint scan devices can be used including those sold under the trade name "Uru" available from Digital Persona .

[0013] The reference biometric data thus-obtained may be stored and/or processed in a number of fashions including compressing and/or encrypting the data, as will be clear to those of skill in the art after understanding the present disclosure. Typically, a computer, such as an IBM-type personal computer, work station, laptop, and the like, can be used for this purpose. The preferably encrypted or otherwise processed biometric reference data is then stored on the smart card or other BDSD 222. A smart card device, typically having a profile about the size of a typical credit card (although generally somewhat thicker), typically includes a data storage device such as flash memory, electronically erasable programmable read only memory (EEPROM) or similar small and lightweight storage device, typically coupled to a microprocessor and/or application specific integrated circuit (ASIC). A number of devices can be used for data input and output including well-known pin and socket arrangements, inductive, infrared, radio or other wireless communication systems and the like. Other types of BDSDs capable of storing biometric data can also be used such as cards or other devices with magnetic surfaces or strips, PCMCIA devices, and the like. A number of types of information, in addition to biometric reference information, can be stored on the BDSD, if desired, including, for example, account balance information, name, identity number or frequent player number or other personal identifier numbers, hotel identification and/or room number. The smart card or BDSD can also be used for storing user preference information such as indications of types of games, drinks, entertainment and the like preferred, food, smoking/nonsmoking preferences, preferred machine denominations and the like. When the desired information has been stored on the BDSD, the BDSD is issued 224, e.g., by a BDSD recording or generation device 116.

[0014] Thereafter, when the player wishes to access a gaming terminal 226, the player may insert 228 the BDSD 119 in a gaming terminal 122, e.g., using a slot or other opening 124 provided for the purpose. The gaming terminal 122 may be configured to be used only in connection with a BDSD 119 or may be configured for use either with the BDSD or with other conventional gaming systems such as coin systems, cash systems and the like. Although it is possible to configure a system in which some or all of the biometric data acquired during the registration process 218 is stored centrally such as in a casino, computer, bank computer and the like, in at least one embodiment, at least some, and preferably substantially all of the biometric information acquired from measuring the prospective player during the registration process is stored only on the BDSD and thus is possessed by, and under the control of, the individual or individuals to whom the biometric data relates.

[0015] In response to receipt of the BDSD 118, the gaming terminal 122 will perform a number of steps 230. In response to receipt of the BDSD 118, the gaming terminal 122 actuates an authorization system or subroutine 232. In this configuration, the gaming terminal 122 includes not only a smart card reader (or other device for reading the biometric reference data from the BDSD), but also includes electronic data processing capabilities such as including one or more microprocessors. The gaming terminal 122 also includes a device for obtaining biometric data from players, of a type similar to at least some of the biometric data stored on the BDSD 118. In the embodiment illustrated in Fig. 1, since the biometric data stored is (or includes) finger or thumb scan information 114, the gaming terminal 122 also includes a finger or thumb print scan device 126. Accordingly, the player is prompted to place his or her finger or thumb on the scanner 126 for appropriate biometric measurements (in this case a finger or thumb scan) in order to allow the terminal 122 to acquire the appropriate biometric data to 34. The data measured at the terminal 122 is then compared 236 to (decrypted) reference data from the BDSD 118. If there is a match, 238, the terminal 122 microprocessor outputs an authorization allowing the player to access his or her account and/or use the debit card balance 242. If there is no match, the microprocessor 122 may output a notification 244, e.g., to casino personnel to investigate possible use of a lost or stolen BDSD, or may prompt the user to repeat the finger or thumb scan or other biometric measurement step and/or to insert a different BDSD. Preferably the microprocessor is configured such that the match need not be exact, i.e., such that the measured and received biometric data is considered to match if the received and measured biometric data are within a predetermined tolerance of one another, as will be understood by those of skill in the art.

[0016] In one embodiment, all of the players' wagers are charged to, and all of the players' prizes or winnings are credited to, the players' account and/or debit card balance. Accordingly, such a system permits effective and efficient gaming in a cashless system, i.e., without the use of coins, tokens, currency or other cash.

[0017] By eliminating the need for coin handlers, currency handlers and the like, it is possible to provide effective gaming terminals which are relatively small, lightweight and low cost. Fig. 3 depicts a gaming terminal which can be implemented according to an embodiment of the present invention having a width 312 of about 20 inches or less, preferably about 12 inches or less, a depth 314 of about 6 inches or less, preferably about 4 inches or less and a height 316 of about 24 inches or less, preferably about 20 inches or less, including a BDSD slot 318 and finger or thumb print scanner or other biometric measurement device 322. The gaming device may include a video display such as an LCD display, CRT display or the like which may be a touch screen device, although other input/output devices or controls can also be provided, along with other items common in the industry, if desired, such as speakers or other audio output devices, lights, reels or other moving parts, signage, instructions, displays, attract components, etc. The gaming terminal illustrated in Fig. 3, however, does not include coin handling (coin receipt and/or coin payout and handling, currency handling or other cash handling components) and accordingly is a cashless gaming terminal. The cashless gaming terminal, according to the present invention (which includes biometric measurement components, may, optionally include a BDSD reader or receiving unit), is sufficiently small, lightweight and/or with sufficiently low power consumption that it can be employed in numerous fashions previously infeasible for the larger and heavier gaming terminals which include coin handling and/or cash handling. In one embodiment, a cashless gaming terminal has a mass of less than about 5 lbs, preferably less than about 2 pounds (less than about 1 kg). The small size of the cashless gaming terminal and the fact that there is no need to access the gaming terminals for adding or removing coins, currency and the like, allows a relatively large number to be positioned in a given floor space or footprint (compared to traditional gaming terminals which include coin handling and/or currency handling) and/or allow gaming terminals to be positioned in locations not normally used for gaming terminals in current usages such as being hung or mounted directly on a wall or similar vertical surface such as in restaurant, cafes, hotel guest room walls, aircraft or automobile seat backs, theater seat backs or sporting arena seat backs or similar locations. In one embodiment, it is preferred to use the BDSD as the sole means for physical output of winnings or account information and, in this way it is possible to provide a gaming terminal which also does not include a printer.

[0018] Even though the present invention can make it feasible to provide a relatively small gaming terminal, it is possible to implement embodiments of the present invention in which standard-sized gaming terminals are used. For example there may be regulations or standards which affect the size or positioning of gaming terminals. Even in such situations, however, the ability to eliminate, e.g. coin handlers or to otherwise reduce or eliminate the need for certain gaming terminal components can contribute to an advantageous reduction in the cost and/or weight of a gaming terminal.

[0019] In light of the above description, a number of advantages of the present invention can be seen. The present invention provides an easy to use and highly secure system for implementing gaming without the need for coins, tokens or currency. The present invention affords the security and accuracy associated with biometric identification or authentication systems in a context of a gaming environment. The present invention provides the security and accuracy associated with biometric systems while allowing individuals to retain possession and control of the biometric data. The present invention reduces the amount of storage necessary to implement a biometric identification or verification system by distributing the biometric data in a plurality of storage devices which are carried by users. The present invention avoids cost and delays associated with remote access of a central database since at least some, and preferably all, of the biometric-based identification or verification is performed at each individual gaming terminal, substantially without the need to access a central system. The present invention makes cashless gaming terminals feasible by providing a practical system which addresses concerns of both players and casinos. The present invention provides a practical cashless gaming system which is relatively small, lightweight, energy efficient and low cost and makes it practical to provide gaming terminals having substantially all non-cash functions of a traditional casino gaming terminal, but in locations previously substantially unavailable or unused for gaming terminals (e.g. because of size, weight or power constraints). The present invention can achieve a relatively small, lightweight and inexpensive, practical gaming terminal or system, e.g., for use in new or emerging gaming markets such as hotel in-room gaming, small-footprint casino gaming, transportation-based gaming such as automobile or aircraft (e.g., seat back) gaming terminals, cruise ship or other shipboard gaming terminals of a relatively compact and/or lightweight nature, wall-mounted and/or thin-profile gaming terminals, wireless (e.g., satellite, radio or infrared-based) gaming terminals and/or multi-terminal gaming systems, practical gaming systems for implementation on small or portable computing devices such as laptop computers, personal digital assistance (PDAs) palm-top computers or computing devices, Internet appliances or Internet-coupled computers, including in-home computers, television-based systems (interactive television and/or "Web TV") television cable systems (interactive cable, Internet cable and the like) and similar systems.

[0020] A number of variations and modifications of the present invention can be used. It is possible to use some features of the invention without using others. For example, it is possible to use a gaming terminal having a biometric measurement device without using biometric data storage devices inserted into the gaming terminals. It is possible to provide gaming terminals which implement biometric identification or verification but which are not cashless.

[0021] Although features of the present invention have been described in the context of, and with regard to, a particular usefulness in, the gaming industry, there is no theoretical reason why some or all features of the present invention can not be used in other context such as the banking industry, purchase of goods or services, e.g., at retail locations, through the Internet or other electronic commerce channels and the like. Although the present invention has been described in the context of a system which stores at least some biometric data on a portable card or other BDSD, it is also possible to provide gaming terminals which can measure and/or use biometric data without comparing to reference data stored on a card or other BDSD (such as by comparing measured data to data stored in a central computer or other central repository). For example, in one embodiment a cashless gaming terminal can be used by any individual who has previously registered appropriate biometric data, e.g., with a casino or other registry, and without using or inserting a card, such that a player can merely approach a terminal, be measured for biometric data and be permitted to place wagers after the biometric data is verified, e.g., by comparing to a centralized data base. The biometric system described above can be used substantially as the sole identification or verification system or can be combined with other systems. For example, it is possible to configure a system such that a player is permitted to place wagers only after the system has both authenticated biometric data and authenticated a player-input personal identification number (PIN), password or similar code. It is possible to use the biometric identification system only under certain conditions, such as when the total wagers for a player or given time period or at given terminal is less than a threshold amount, greater than a threshold amount or the like. It is possible to combine two or more different authentication systems or identification systems which have different levels of trust or security, different costs or time delays and the like. For example, a system could be configured such that for a relatively low amount of total wagers, a low-security verification of a fingerprint scan versus data stored on a player's credit or debit card is used but, if a player wishes to make wagers greater than a threshold, a more rigorous identification system, such as comparison of retina scans, iris scan, a comparison of or detailed fingerprint scan information and the like is performed, possibly using processing capabilities and/or data at a central location (and possibly involving greater delay). Although, in at least one embodiment described above, the initial reference biometric data is stored onto the user's card or other BDSD during a separate registration process, it is also possible to provide for automatic registration such as registration at gaming terminals. For example, a system can be provided in which, if a user uses a smart card or other appropriate BDSD which has no biometric data, the user's biometric data will be measured and appropriate data stored (preferably in encrypted form) on the card, the first time the user attempts to use a (appropriately configured) gaming terminal. Thereafter, any subsequent use of the card will involve the recognition that the card has biometric data stored thereon. In some cases, it may be desirable to provide for two or more persons to access a given account or use a given BDSD. In one embodiment, the BDSD stores biometric data from two or more different authorized account holders or BDSD-users. In some cases, it may be desirable to provide the same (or similar) biometric data for a given person, on two or more different cards or other BDSDs, e.g., so that a user may, if desired, play on two or more different gaming terminals at one time or so that two or more persons, both authorized may play at two or more different terminals at the same time.

[0022] Although examples have been described herein involving biometric data representing a single characteristic, such as a fingerprint, it is possible to implement systems according to the present invention in which two or more different biometric data sets are used such as using both fingerprint and voice print information, retina scan and iris scan information and the like. Although the invention has been described in connection with an embodiment involving issuance of a BDSD by a casino, the present invention can also be implemented using numerous other types of registration or issuing identities. For example, smart cards, credit cards, debit cards or similar BDSD which may be used in connection with the present invention can be issued by financial institutions such as banks, credit card companies, tourism bureaus, airlines, ocean liner companies and the like. In some systems, it may be desirable to provide different BDSDs for use in different casinos, or groups of casinos while in other systems it may be desirable to provide smart card or other BDSD which can be used in substantially any casino, e.g., in a given city or geographic location, or at substantially any location. Cashless gaming terminals according to the present invention can be stand-alone (i.e., not coupled to other gaming terminals) or can be part of a network of gaming terminals such as a coupled to a casino cluster controller and/or for implementation of a multi-terminal prize system such as a progressive prize system. Although examples have described configurations in which biometric data is stored electronically, it is also possible to use other machine-readable methods of storing biometric data such as digital optical storage and the like. Although embodiments described above have provided numerous components, including biometric scanning components or BDSD receivers or readers positioned internally to, or formed as part of, the gaming terminal, it is also possible to provide these or other components in separate and discrete locations or housings, e.g., communicating with the gaming terminal by cables or wireless communication links.

[0023] Any of a number of registration procedures can be used in connection with embodiments of the present invention, as will be understood by those of skill in the art after understanding the present disclosure. As illustrative examples, in one scenario, a user may pre-register using a process similar to player tracking registration, but also including biometric (e.g. fingerprint) registration. If desired, pre-registration can include establishing a credit or debit account, e.g. for use in connection with cashless gaming terminals. In a second scenario, registration can occur directly at gaming terminal locations. It is anticipated this option may be attractive to players who which to have the convenience of using a debit card, but only for his or her day winnings. In this scenario, a gaming terminal may be configured with a bill validator, a smart card reader and a biometric sensor. In response to receipt of currency, using the bill acceptor, the device will dispense a (programmable) smartcard. The player will be prompted to insert the smart card in a card reader and will prompt the player to place a finger on a fingerprint sensor (or otherwise provide biometric data). It will register and verify the fingerprint data, then program (preferably in encrypted form) the fingerprint data and will credit an amount on the smart card and will send this data, via the casino or other network to a central computer system. When the player leaves, the player can go to a casino cashier or kiosk for cashing out any remaining credit left on the card. During registration, gaming and cash-out transactions, the casino's central system performs debiting and crediting on the player's account and at least the balance is stored on the player's smart card. If a card is lost or stolen, a casino cashier can verify identity of a player by his or her fingerprint and then access the player's account. In another scenario, a smartcard is not needed. All transactions are maintained on the casino computer system, with biometric sensors being used for authentication. In this scenario, the casino (or other) computer system must be operational for the transactions to occur (as opposed to a system using a smart card, in which the card can be used to provide the media for the transaction). Those of skill in the art will understand how to modify e.g. the scenario depicted in Fig. 2 in order to implement such other registration scenarios.

[0024] The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g. for improving performance, achieving ease and\or reducing cost of implementation. The present invention includes items which are novel, and terminology adapted from previous and/or analogous technologies, for convenience in describing novel items or processes, do not necessarily retain all aspects of conventional usage of such terminology.

[0025] The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. Although the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g. as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

Claims

1. A gaming apparatus comprising:

   a portable biometric data storage device storing first biometric data for at least a first user;
   a gaming terminal, configured for playing at least first game;
   a reader, coupled to the gaming terminal which receives said first biometric data stored on said biometric data storage device;
   a biometric measurement device for measuring biometric data of a user to provide measured biometric data; and
   a comparator for comparing said measured biometric data to said first biometric data and outputting at least a first notification if there is an absence of match.

2. Apparatus as claimed in Claim 1, wherein:
   said iometric data storage device is provided in a card having a thickness less than about 0.05 inches.

3. Apparatus as claimed in Claim 2, wherein:
   said card includes a microprocessor.

4. Apparatus as claimed in Claim 2, wherein:
   said card is a debit card.

5. Apparatus as claimed in Claim 2, wherein:
   said card further stores the current account balance for an account established for said first user.

6. Apparatus as claimed in Claim 1, wherein:
   said biometric measurement device is selected from among:

   a thumb print scanner;
   a fingerprint scanner;
   a retina scanner;
   a iris scanner;
   an ear scanner;
   a voice data sensor;
   a facial scanner; or
   an infrared scanner.

7. A gaming terminal comprising:

   at least a first control device which initiates or controls playing of a game;
   at least a first output device which outputs results of game play;
   a biometric measurement device which obtains biometric measured information relating to a prospective game player;
   a microprocessor which compares said measured biometric information to stored biometric information;
   said microprocessor configured to charge wagers, in connection with said game, against a pre-established account only if said measured biometric information sufficiently closely matches said stored biometric information; and wherein said gaming terminal is provided in the absence of coin handling, token handling or

currency handling equipment.

8. A gaming method comprising:

storing first biometric data for at least a first user in a portable biometric data storage device;
a gaming terminal;
coupling a reader to a gaming terminal, configured for playing at least first game, wherein said reader receives said first biometric data stored on said biometric data storage device;
measuring biometric data of a user to provide measured biometric data; and
comparing said measured biometric data to said first biometric data and outputting at least a first notification if there is an absence of match.

9. A method as claimed in Claim 8, wherein:
said step of storing includes storing in a card having a thickness less than about 0.05 inches.

10. A method as claimed in Claim 9, wherein:
said card includes a microprocessor.

11. A method as claimed in Claim 9, wherein:
said card is a debit card.

12. A method as claimed in Claim 8, further comprising
storing, on said biometric data storage device, the current account balance for an account established for said first user.

13. A method as claimed in Claim 8, wherein:
said step of measuring includes a step selected from among:

scanning a thumb print;
scanning a fingerprint;
scanning a retina;
scanning an iris;
scanning an ear;
sensing voice data; or
scanning a face.

14. A gaming method comprising:

initiating or controlling playing of a game using at least a first control device;
outputting results of game play using at least a first output device;
obtaining biometric measured information relating to a prospective game player using a biometric measurement device ;
comparing said measured biometric information to stored biometric information;
charging wagers, in connection with said game, against a pre-established account only if said measured biometric information sufficiently closely matches said stored biometric information; and
wherein said gaming terminal is provided in the absence of coin handling, token handling or currency handling equipment.

15. A gaming apparatus comprising:

portable means for storing first biometric data for at least a first user;
gaming terminal means for playing at least first game;
reader means for receiving said first biometric data stored on said portable means for storing;
means for measuring biometric data of a user to provide measured biometric data; and
means for comparing said measured biometric data to said first biometric data and outputting at least a first notification if there is an absence of match.

16. Apparatus as claimed in Claim 15, wherein:
said means for storing is provided in a card having a thickness less than about 1/4 inch.

17. Apparatus as claimed in Claim 15, wherein:
said means for storing includes a microprocessor.

18. Apparatus as claimed in Claim 15, wherein:
said means for storing further stores the current account balance for an account established for said first user.

19. Apparatus as claimed in Claim 15, wherein:
said means for measuring is selected from among:

a thumb print scanner means;
a fingerprint scanner means;
a retina scanner means;
a iris scanner means;
an ear scanner means;
a voice data sensor means; or
a facial scanner means.

20. A gaming terminal comprising:

means for initiating or controlling playing of a game;
means for outputting results of game play;
means for obtaining biometric measured information relating to a prospective game player;
means for comparing said measured biometric information to stored biometric information;
means for charging wagers, in connection with said game, against a pre-established account only if said measured biometric information suf-

ficiently closely matches said stored biometric information; and

wherein said gaming terminal is provided in the absence of coin handling, token handling or currency handling equipment.

FIG. 1

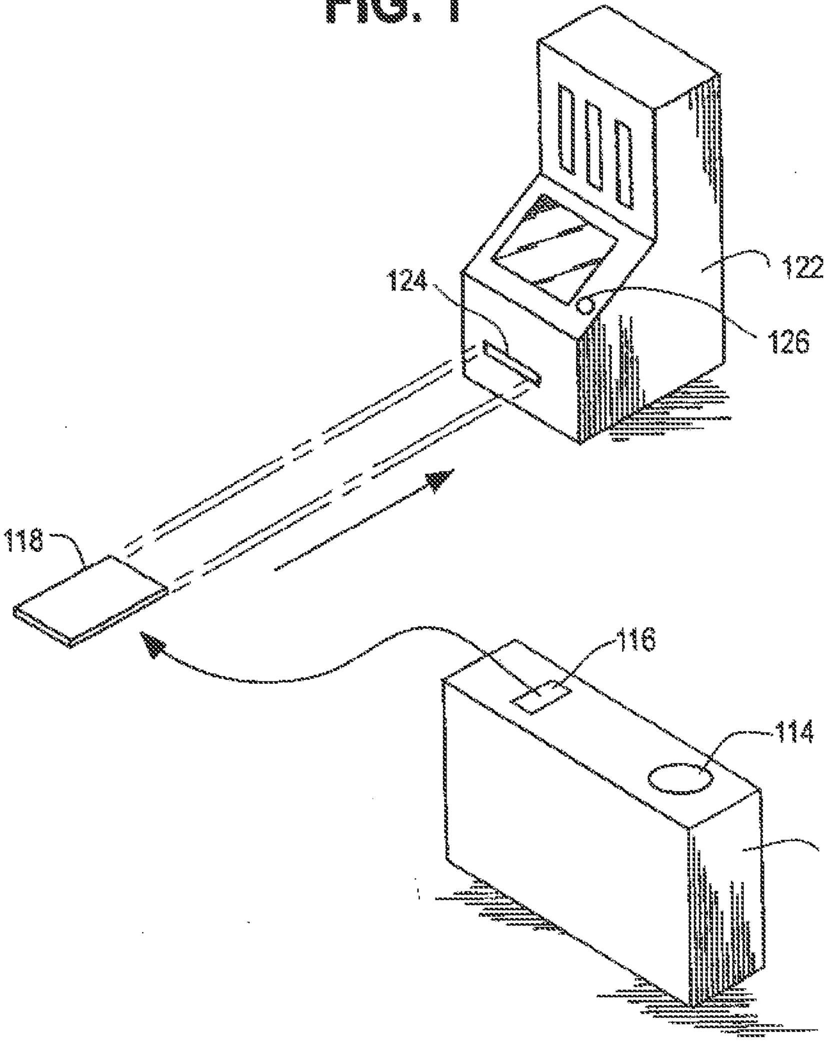


FIG. 2

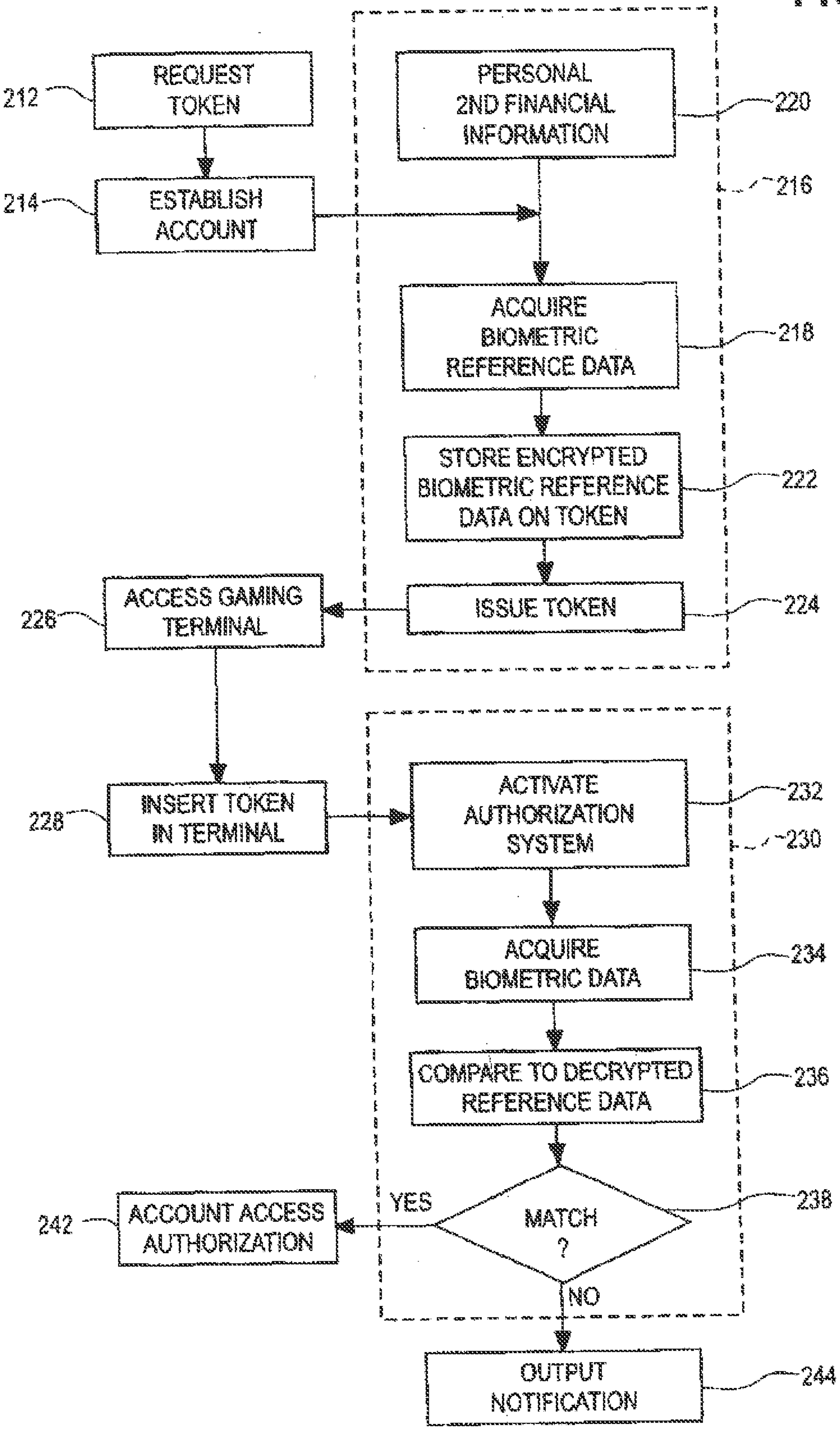
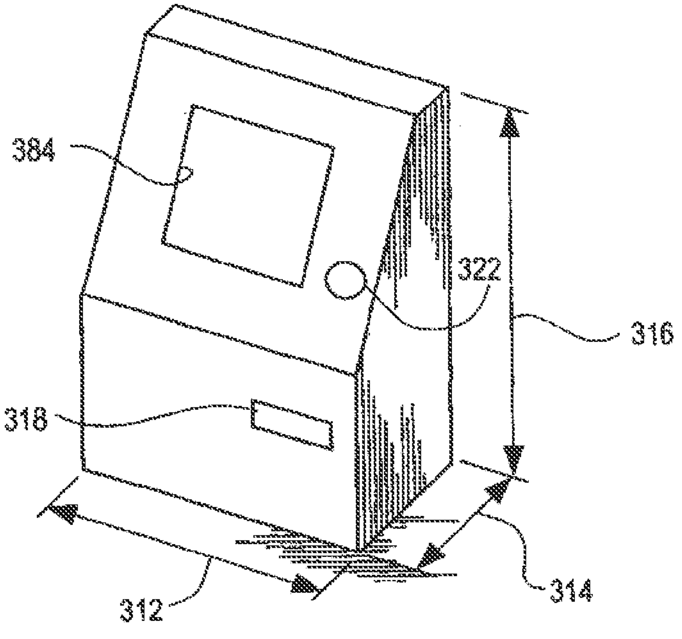

REQUEST TOKEN
212
ESTABLISH ACCOUNT
214
PERSONAL 2ND FINANCIAL INFORMATION
220
216
ACQUIRE BIOMETRIC REFERENCE DATA
218
STORE ENCRYPTED BIOMETRIC REFERENCE DATA ON TOKEN
222
ISSUE TOKEN
224
ACCESS GAMING TERMINAL
226
INSERT TOKEN IN TERMINAL
228
ACTIVATE AUTHORIZATION SYSTEM
232
230
ACQUIRE BIOMETRIC DATA
234
COMPARE TO DECRYPTED REFERENCE DATA
236
MATCH ?
238
YES
NO
ACCOUNT ACCESS AUTHORIZATION
242
OUTPUT NOTIFICATION
244

FIG. 3



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 120 757 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
04.09.2002 Bulletin 2002/36

(51) Int Cl.7: G07F 17/32, G07C 9/00

(43) Date of publication A2:
01.08.2001 Bulletin 2001/31

(21) Application number: 01101836.3

(22) Date of filing: 26.01.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: International Game Technology
Reno, Nevada 89511 (US)

(72) Inventors:
- Wells, William R.
  Reno, Nevada 84502 (US)
- Wilder, Richard
  Sparks, Nevada 89436 (US)
- Mattice, Harold E.
  Gardnerville, Nevada 89410 (US)
- Griswold, Chancey W.
  Reno, Nevada 89509 (US)

(74) Representative:
Manitz, Finsterwald & Partner GbR
Postfach 31 02 20
80102 München (DE)

(54) Gaming terminal and system with biometric identification

(57) A gaming system is provided with biometric facilities for identifying or verifying the identity of a player or perspective player. In one aspect reference biometric data is stored in a portable biometric data storage device such as a smart card, PCMCIA card or the like and is preferably left in the possession or control of the individual or individuals to whom the biometric data relates. The reference biometric data is read in individual gaming terminals and compared, in individual gaming terminals to measured biometric data of a player or perspective player. In one aspect, gaming terminals use biometric verification or indication to implement a practical and feasible cashless gaming terminal.

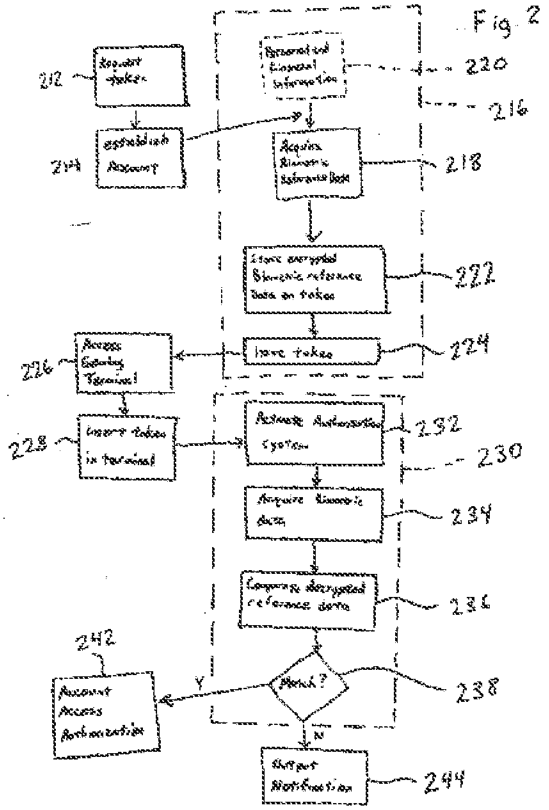

212
Request token
214
establish Account
Personalized Biometric Information
220
216
Acquire Biometric Reference Data
218
Store encrypted Biometric reference Data on token
222
Issue token
224
226
Access Gaming Terminal
228
Insert token in terminal
Activate Authorization System
232
230
Acquire biometric data
234
Compare decrypted reference data
236
Match?
238
Y
N
242
Account Access Authorization
Output Notification
244

Fig 2

EP 1 120 757 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 10 1836

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 94 10658 A (COMS21 LTD ;GREEN GRAEME A (AU)) 11 May 1994 (1994-05-11) * abstract; claims 1,2,6-8,10; figures * * page 1, paragraph 1 * * page 3, line 36 - page 5, line 10 * * page 7, line 35 - page 9, line 6 * * page 10, line 10 - line 14 * * page 11, line 10 - line 37 * * page 13, line 8 - page 18, line 38 * -----	1-20	G07F17/32 G07C9/00
X	WO 94 16416 A (SPECIALITEITEN B V ;ALPHEN JOHANNES W G (NL)) 21 July 1994 (1994-07-21) * abstract; figures * * page 2, line 12 - line 28 * * page 5, line 12 - page 6, line 32 * * page 8, line 3 - line 23 * -----	1-20	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			G07F G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	15 July 2002	Buron, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 10 1836

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-07-2002

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
WO 9410658	A	11-05-1994	AU	5170193	A	24-05-1994
			WO	9410658	A1	11-05-1994
			BR	9307500	A	01-06-1999
			CA	2148236	A1	11-05-1994
			CN	1091844	A	07-09-1994
			CN	1228567	A	15-09-1999
			EP	0673534	A1	27-09-1995
			JP	8503087	T	02-04-1996
			NZ	257489	A	20-12-1996
			NZ	299616	A	19-12-1997
			RU	2121162	C1	27-10-1998
			US	5954583	A	21-09-1999
WO 9416416	A	21-07-1994	NL	9300030	A	01-08-1994
			AU	5867094	A	15-08-1994
			WO	9416416	A1	21-07-1994
			NL	9400033	A	01-08-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 087 323 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.03.2001 Bulletin 2001/13

(51) Int Cl.7: G06F 19/00, H04L 29/06,
A63F 13/12
// G06F161:00

(21) Application number: 00660160.3

(22) Date of filing: 19.09.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 24.09.1999 US 406596

(71) Applicant: Nokia Corporation
02150 Espoo (FI)

(72) Inventors:
- Schulz, Paul David
Kirribilli, New South Wales 2061 (AU)
- Sinclair, Matthew Frazer
Neural Bay, New South Wales 2089 (AU)
- Larsen, Kenneth Bo
Carrs Park, New South Wales 2221 (AU)

(74) Representative: Johansson, Folke Anders
Nokia Corporation,
P.O. Box 319
00045 Nokia Group (FI)

(54) A wireless system for interacting with a virtual space

(57) A wireless communication system for interacting with a virtual space. The wireless system may include some or all of the following: a mobile station, a server supporting the virtual space, a gateway, a game center, and a game service. The virtual space may be an interactive fiction game where the user of a mobile station may interact with other players and software entities in the virtual space. The virtual space may be used for other purposes such as a virtual tour of a real world city, guided perhaps by a software entity or agent. The virtual space may be used for business activities such as a virtual conference that allows participants who are physically remote from each other to interact in the virtual space.

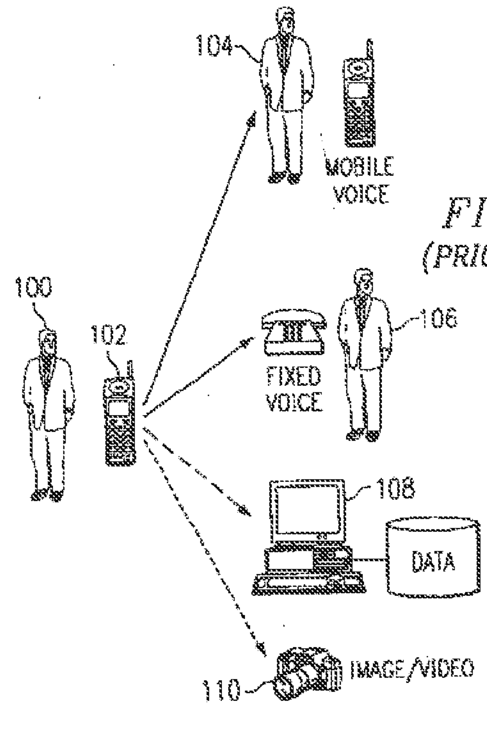


FIG. 1
(PRIOR ART)

Description

Field of the Invention

[0001] The invention relates to the field of wireless communications, and in particular, to a system whereby a user of a wireless terminal can efficiently and simply interact with a virtual space. In one aspect, this relates to the field of wireless games, and in particular, to interactive multi-player games played using a hand-held wireless terminal.

Background of the Invention

[0002] Electronic games have become a major part of the entertainment industry in today's modern world. The playing of electronic games on stand-alone terminals has long been popular. However, in recent years these games have migrated into a network environment.

[0003] As the complexity of electronic games, powered by increasingly sophisticated hardware and software, improves game-players often find themselves playing games which are not necessarily suited to their particular temperaments, habits, and reactions. Clearly, designers and manufacturers of electronic games must cater to the broadest possible commercial market. However in so doing there are many game players who are less than satisfied with the final result.

[0004] The restrictive user interfaces presented by mobile stations present a particular challenge when considering game-playing across a mobile network. In particular, when considering network games of the "interactive fiction" or "adventure" style, a game-player typically suffers from a limited perceptual consciousness of the potential context of the game, being constrained by the limited user interface presented by the typical mobile station. The richness of environmental variables which can potentially be brought into the context of an adventure game are not easily incorporated into such games in current mobile station systems.

Summary of the Invention

[0005] The present popularity of electronic games makes it desirable that such games migrate technologically from stand-alone, hand-held or PC based terminals to network based games utilizing wireless communication systems.

[0006] Disclosed herein is a wireless system for interacting with a virtual space. In the presently preferred embodiment, the virtual space is an interactive multiplayer game. The interactive game of the presently preferred embodiment is played in a wireless environment using a mobile station as a user interface. The game is tracked and controlled using the mobile station and a game server. The game server is typically at a location remote from the mobile station. Moreover, communication between the game server and the mobile station is typically performed using a base station connected to a telecommunications network. The game server supports a game center and executes a software application that defines the virtual space. Individual games are managed within the context of this software application. The virtual space encompasses those users and elements of which the mobile station user can have a perceptual awareness. Interaction with the virtual space can be had by textual or voice communications. Perceptual awareness is realized by textual, graphic, or audio communications.

[0007] In the presently preferred embodiment, the games are text based. A command set is provided for each state of the virtual space within the game. The choice of a command from the command set changes the game state. Individual games are designed to be customizable. That is, attributes of the mobile station interface can be used to adjust gaming parameters. The game parameters can be adjusted based on, for example, attributes such as current location of the mobile station, call usage on the mobile station, or wireless services utilized by the mobile station.

Brief Description of the Drawings

[0008] The disclosed embodiments will be described with reference to the accompanying drawings, which are incorporated in the specification hereof by reference, wherein:

Figure 1 shows a prior art system wherein a user of a mobile station communicates with another mobile station user and a fixed terminal voice user;
Figure 2 depicts enhanced mobile telecommunications according to a preferred embodiment;
Figure 3 presents a system configuration of a wireless communication system which can support a "virtual space" communication paradigm;
Figure 4 depicts aspects of a mechanism by which the simple intuitive dynamics previously described may be implemented;
Figure 5 presents a more detailed view of the infrastructure supporting the virtual space;
Figure 6 depicts various participants "inhabiting" the virtual space; Figure 7 represents a process flow for a segment of an interactive fiction game as in the presently preferred embodiment;
Figure 8 shows further detail of the story segment;
Figure 9 depicts the interactive segment in more detail;
Figure 10 depicts another embodiment of an interactive fiction game;
Figure 11 depicts network-related mobile station usage information associated with the player 100 which is used to enhance the realism and enjoyment of the game of the presently preferred embodiment;
Figure 12 depicts how information regarding the

manner in which player 100 plays the interactive fiction game of the presently preferred embodiment being incorporated into the game;

Figure 13 depicts a lightweight interactive fiction engine language (LIFE) used to create the virtual space in a cost effective and well documented manner;

Figure 14 depicts a game player 1100 using a mobile station 1102 to play an interactive fiction game on a mobile network;

Figure 15 depicts the profiling of mobile station activity in order to customize the service context;

Figure 16 depicts deployment of virtual voice-based characters in a game setting within a wireless game environment;

Figures 17A-N depict a working example of the presently preferred embodiment showing user information displayed on the display of a mobile station;

Figure 18 depicts a block diagram of a mobile station 1800 that can be used in the disclosed embodiments; and

Figure 19 depicts a block diagram of a cellular communications system suitable for implementing the disclosed embodiments.

Detailed Description of the Preferred Embodiments

[0009] The numerous innovative teachings of the present application will be described with particular reference to the presently preferred embodiment. However, it should be understood that this class of embodiments provides only a few examples of the many advantageous uses of the innovative teachings herein. In general, statements made in the specification of the present application do not necessarily delimit any of the various claimed inventions. Moreover, some statements may apply to some inventive features but not to others.

[0010] Figure 1 depicts a prior art system wherein a user **100** of a mobile station **102** communicates with another mobile station user **104** and a fixed terminal voice user **106**. Voice communication between the initial user **100** and the other two users **104** and **106** is well served by the present mobile network and terminal infrastructure. However, the user **100** has only limited access to data services **108** and even less to image/video services **110**. Figure 1 graphically illustrates how the mobile station user **100** is provided with only very restricted access to a rich communications environment.

[0011] Figure 2 depicts enhanced mobile telecommunications according to a preferred embodiment of the invention. A number of additional elements, depicted by shaded boxes **200**, **202** and **208**, are introduced. These additional elements provide the mobile station user **100** with an enhanced access capability to the telecommunications environment. The shaded block **200** depicts a simpler and more effective man/machine interface between the mobile station user **100** and his or her mobile station **102**. A mobile station user interface is designed primarily for setting up voice communications, therefore, it is inherently unsuited to the task of providing a rich environment for perception of a virtual space. The new element **200** is described in more detail in the discussion of Figure 4.

[0012] The element **202** depicts the use of "profiling" to adapt the telecommunications environment to the habits, tendencies, and history of the user **100**. The use of profiling enables services within the broader telecommunications environment to be "customized". This customization effectively tailors the services to the particular user **100**. Thus, instead of generic telecommunications services being provided to users who are anything but generic, the services become individually tailored. Tailoring the services serves to streamline and make more effective communications with the user **100**. This effect is explained in more detail in relation to Figures 11 and 12.

[0013] The element **208** depicts use of adjunct support equipment, such as interactive voice response systems. Such equipment is used to augment and support services being provided from the telecommunications environment to the user **100**. This equipment is explained in more detail in Figure 16.

[0014] The abstract concept of "virtual space" representing the telecommunications environment within which the mobile station user can interact is introduced in the following figures. This abstract concept is first outlined in general terms, and then a specific example of a virtual space is used for a more detailed description. The virtual space in the presently preferred embodiment is described as being an interactive fiction game which is played across a wireless network. However, it should be noted that most if not all of the features described in the presently preferred embodiment are useful to a mobile station user for other pursuits, such as, business activities, for example.

[0015] As will be explained further, interactive fiction games can enable a user 100 to interact with other users **104** and **106**, with various data structures, and with intelligent software entities which can be supported on data services 108.

[0016] Figure 3 presents a system configuration of a wireless communication system which can support a "virtual space" communication paradigm. A mobile user **100** communicates, by means of a mobile station **102**, which in turn uses a wireless connection to a network **306**. The network **306** in turn, is connected to a server **310**. The server **310** is described in more detail in Figure 5. In the presently preferred embodiment, the elements described in Figure 3 constitute interacting component parts supporting a virtual space **312**. In the presently preferred embodiment, the virtual space **312** provides a mobile station user **100** with a perceptual awareness of other mobile station users **104**, as in a telephone voice call. The virtual space **312** also provides a mobile station user **100** with a perceptual awareness of the various othdirected to the interactive segment **(Step 708)**.

[0023] Figure 9 depicts the interactive segment 708 in more detail. In the multi-player interactive fiction game of the presently preferred embodiment, the interactive segment 708 takes place in a cafe, where the various players 100 and 104 can "meet" and interact. Furthermore, the software agents 612 and 614 can also participate and the various objects 610 and 608 can be found. Therefore, while the story segment 704 provides a mechanism by which the player 100 can navigate spatially among a geographic set of connected locations, the interactive segment 708 is a process whereby the player 100 interacts with the various players and features in the virtual space 312. In Figure 9, a decision **(Step 900)** presents a number of options to the player 100. Unlike the decision block **(Step 800)** of Figure 8, this decision block **(Step 900)** allows the player 100 to select one or more of the options. Thus, assuming that the player 100 is required to obtain a certain amount of money, he may elect to play poker **(Step 904)**. If he wins the game, the winnings constitute the needed cash. The player could also elect to take cash from the office **(Step 908)**. The process can then be directed back to the decision option **(Step 900)**. The player 100 can now elect to pick up a key **(Step 912)** and take it into his possession. Alternatively, the player 100 can elect to enter a shelter and purchase a disguise **(Step 918)**. However, in order to enter the shelter, a key is required. In order to purchase a disguise, a certain amount of cash is required. Therefore, the prior actions of the player 100 determine his ability to proceed onwards in the process or his need to return and retrace his steps, if he is so able to do by the definition of the game software.

[0024] Figure 10 depicts another embodiment of an interactive fiction game. Figure 10 includes an expanded version of a virtual world with possible courses of navigation.

[0025] Figure 17 depicts a working example of the presently preferred embodiment showing user information displayed on the display 414 of a mobile station 102. The user 100 can interact with the game via the presented options by way of scroll and input keys 402 forming a part of the reduced keypad 400. Conventional mobile stations have such keys. Voice commands may also be used for interaction with the game. Voice commands may be used, for example, when responding to a prompt, such as, from a character in the game.

[0026] To commence the game, the player 100 must login with a user name and password using the Login screen **1702**. The user name and password are preconfigured on the game server. The game server validates the user name and password. If successful, the player is logged into the game and is presented with an initial set of instructions **1704**. In the presently preferred embodiment, the instructions are: "Welcome, <player name>! You can use the roller key to scroll text and menus. The scrollbar on the right indicates when more text is available for viewing. Select the "Options" menu to begin a new game, restore a previous game or to get more instructions on how to play."

[0027] The player may elect to start a new game, resume a saved game, get the full set of instructions for the game, or quit the game completely **1706**. If the player elects to play a new game, the story begins. The first story element is presented to the player **1708**. A story element can read, for example, "You arrived at the office this morning in a state of despondency. You were dissatisfied. Happy and successful, but at the same time there is a nagging feeling of something being wrong. Here you are in this job that isn't quite right. It was a job that you had to accept to pay the bills. You'd wanted to be a painter really, but your mother said at the time 'no-one gives you any money 'til you're dead'. And what good is money to a dead guy." At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story **1710**. The selected action will determine the next course to be taken in the story, for example, "Do you go downstairs, go to the window, or go back to work?"

[0028] The story element related to the selection, for example, to go downstairs, is presented **1712**. The story element can read, for example, "You go to the elevator and head down to the lobby. You walk slowly across it toward the street but cannot see anybody that you recognize through the glass facade. You step out through the automatic door and onto the street. The crowd seems to part and you see a woman by the curb. She is talking to a policeman with his back turned diagonally toward you. You circle around to your right a little in order to see the woman's face from front on. The policeman is saying 'Do you know who did this?' The woman looks up and over the policeman's shoulder and in your eye with a look of reproach and your stomach falls. She points straight at you and says 'He did!'. The police move quickly. They are heading straight towards you."

[0029] At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story **1714**, for example, "Do you stay or do you run?" The story element related to the selection, for example, to run, is presented **1716**. The story element can read, for example, "You stand there in amazement as several police walk over to you and grab you. Pinning your arms behind you they put handcuffs on your wrists and drag you off to a waiting car. When you arrive at the station they tell you that you are accused of industrial espionage - citing your briefcase as evidence. You insist that it is your briefcase and they say 'We'll soon see'. They open it and papers that are clearly not yours are revealed. You protest but it falls on deaf ears. On the way to the cells, now with your handcuffs removed, the guard stops to talk to someone else. He has his back turned and behind you is an open door to the carpark. You can't believe this turn of events. Arrested!"

[0030] At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story **1718**, for example, "Do you remain calm or try to escape?" The story element related to the selection, for example, to escape, is presented **1720**. The story element can read, for example, "You don't really know why you do this but you turn and run. Somehow you know what will happen if you stay. You will be falsely accused and will have to go through a whole load of legal rigmarole. Your life and all you have worked for could be erased in the ensuing publicity. The policeman again calls on you to stop but you just keep running. You duck into an alley with the policeman not far behind. As you run past a doorway you hear laughter that somehow seems to be directed at you. You turn another corner and it's a dead end. You can hear the running boots of the cops right behind. You look around desperately for an escape. There is a garbage skip right beside you with a fire escape above it. If you leap to the top of the bin you might just reach the ladder. Or perhaps now might be the right time to give yourself up."

[0031] At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story **1722**, for example, "Do you give up or climb the ladder?" The story element related to the selection, for example, to give up, is presented **1724**. The story element can read, for example, "You can't believe this turn of events. Arrested!" At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story **1726**, for example, "Do you remain calm or try to escape?" The story element related to the selection, for example, to remain calm, is presented **1728**. The story element can read, for example, "You spend most of the day and night in the cell, furious at what has happened. The next morning bail is posted for you by a mysterious person who will not allow themselves to be identified. As you leave the police station you feel quite confused. You do not want to go home or back to work just yet. You have to work out what to do about all of this. You step into a café across the street from the police station. What you really need is a quiet coffee and some time to figure all of this out. There is an enormous amount on your mind. This has been an incredibly confusing day." When the story segment is complete, the player is given the option to continue with the game and move into the interactive environment attached to this story segment **1730**.

[0032] The mode of game play now changes from a directed story into navigating and taking actions within a planned environment. To move through the interactive environment and complete the episode, the player 100 will need to get enough money to buy a costume as a disguise. Once acquired, the player 100 must get a photo taken with the costume on, buy a passport from a man in the bar, take a taxi to the airport, buy a ticket, and board a plane to Helsinki. At each location in the interactive environment, a description of the location is presented along with a list of items that can be seen at the location and the actions that the player can take at that location. If the player 100 chooses to continue, the next story element is presented **1732**.

[0033] In the presently preferred embodiment, a description of the café is presented, for example, "You are in a café. There are booths by the wall and tables in the center. A bar runs along another wall. There are two women sitting at one of the tables, deeply engaged in conversation." At the end of this story element, the player is presented with a list of actions that can be taken at this stage in the story. The story element related to the selection, for example, to look around, is presented. The story element can read, for example, "At the café, you see a proximity card and a one dollar coin." **1734**.

[0034] At the end of this description, the player is presented with a list of actions that can be taken **1736**, for example, go, look, drop, examine, or use an object. A list of options pertaining to the action elected, for example, go, is presented **1738**. The options can include, for example, go outside the café. The player is presented with a description of the environment that they can move into, the items that they can see, and the actions that they can take at this time **1740**. The description can read, for example, "You are in an old lane. The backs of several buildings face onto it. Bare, black metal ladders lead from the ground up into the haze. Dirty red brick walls with graffiti, soot and bird droppings likewise rise up out of sight. It smells bad. A few rats slip into the shadows as you approach. In front of you is the entry to what looks like a costume shop."

[0035] At the end of this description, the player is presented with a list of actions that can be taken **1742**, for example, go, look, drop, examine, or use an object. A list of options pertaining to the action elected, for example, go, is presented **1744**. The list can include places to go, for example, into the costume shop, east, west or back into the café. The story element related to the selection, for example, go into the costume shop, is presented **1746**. The story element can include, for example, a list of things that the player 100 can see in the costume shop and actions that he can take. The story element can read, for example, "You see a shop cluttered with masks and wigs, costumes and hats. Racks of body parts are on the east wall behind the counter. Also behind the counter stands a middle-aged man with lank black curly hair. You don't notice him at first because he blends in with the noses, ears, false moustaches, and wigs behind him. He ignores you, pointedly, it seems. In the south wall a door with dirty glass leads to the main street."

[0036] At the end of this story element, the player is presented with a list of possibilities **1748**. The list can include, for example, seeing a shopkeeper. A list of actions that can be taken at this stage in the story is displayed **1750**, for example, the player 100 can go, talk to, look, examine or use an object at this location. The characters related to the selection, for example, talk to someone, are presented **1752**. The dialogue related to the person the player 100 chooses to speak to is displayed **1754**. The dialogue with the shopkeeper from the player's 100 perspective, for example, can read: "'I need a disguise.' He says. 'Disguises, disguises? That's all anybody ever wants these days, whatever happened to the good old days of just getting dressed up for fun. What you like, I have a whole bunch of disguises, some are better than others and their prices reflect that. I mean, a cheap disguise is really easy to see through but the more expensive ones are impossible - your own mother won't recognize you. Here's the list with the prices clearly shown in red beside them. By the way, weren't you just in here?'"

[0037] At the end of this story element, the player is presented with a list of actions that can be taken **1756**. The list can include, for example, go, look, drop, examine, buy, or use an object at this location. A list of items pertaining to the chosen action, for example, buy an object is displayed **1758**. The display can read, for example, "You can buy any one of three different costumes, each at a different price, and each associated with a different level of probability that the police won't recognize you when they see you. If you buy the $100 outfit, you won't be seen. If you buy the cheapest outfit, there is a great chance that you will be recognized by the police. If you buy a reasonable costume, you have a reasonable chance of fooling the police."

[0038] At the end of this explanation, the player is presented with a story element relating to the choice of, for example, attempting to buy the most expensive costume **1760**. The story element can read, for example, "You can pay with cash or with your credit card. You only have $45 in your wallet (you can see this if you look at your inventory). Being short of cash, you hand the shopkeeper your credit card. After a brief phone call from the back room, the shopkeeper returns and pointedly informs you that the card has been cancelled. He promptly cuts the card in half and throws it into the bin. To buy the costume, you will need to find some money. Perhaps you have some money in your office or you can win some money at the poker machines in the bar."

[0039] At the end of this story element, the player is presented with a list of possible actions **1762**. The list can include, for example, go, talk to, look, examine or use an object at this location. The locations related to the selection, for example, go, are presented **1764**. The available location, for example, can read "You can only go out into the lane from the costume shop." A list of actions pertaining to the selection is displayed **1766**. Because the player 100 has already been to the lane, only a short description of the lane is presented along with the actions possible.

[0040] At any point in the game, the player can review his inventory **1768**. When the player reviews his inventory, a list of items in the inventory is presented **1770**. The inventory can read, for example, "You have a leather wallet and a mobile phone." Any item in inventory can be examined. A description of the item examined **1772**, for example, the wallet, can be that your leather wallet is an expensive looking leather wallet containing $45 and little else.

[0041] The game is continued after examining the inventory items. The player may, for example, move from the lane back into the café." A list of items that may be seen at the café is displayed **1774**. The list may include, for example, a proximity card and a one-dollar coin. Objects are taken using the take action **1778**. When an object is taken from a location, it is added to the player's inventory. Selecting the take option displays a list of items that the player can see **1780**. Items to be taken are selected form the list. When an item is taken, feedback indicating success or failure is displayed **1782**. Taking the proximity card, for example, can yield the feedback "You manage to swipe the card from the table without anybody noticing."

[0042] The player may look around any current location **1784**. Looking around a hotel, for example, will yield a description of what can be seen **1786**. The description can read, for example, "In the south wall is a screen door leading to the kitchen of a hotel. You can hear the chef singing and see cooks wandering to and fro across your field of vision. In the north wall, above your head is a barred window that you know is a cell window at the police station."

[0043] If the player, for example, moves into the hotel lobby, a description of the lobby is presented **1788**. The player is told that there is a photo booth in the corner, for example, "In the south wall a rotating door leads to the main street. In the corner is a photo booth. You step into a quiet alcove behind a palm...." The Take Photo action will appear in the list of allowed actions at the end of the location description.

[0044] If the player proceeds into the bar, a description of the bar will be displayed, for example, a guy in a raincoat and a poker machine **1790**. Obtaining a passport requires talking to the guy in the raincoat. Playing the poker machine requires select the use action for the coin **1792**. Selecting the use item from the list of actions retrieves a list of items from the player's inventory **1794**. Selecting an item, for example, the coin, displays a list of items upon which the coin can be used **1796**. If the poker machine is selected, a description of the resulting action is displayed **1798**. The description can read, for example, "You insert the coin in the slot and pull the handle. Against all odds, '777' appears an ear-piercing horn announces you as the winner of the jackpot. The barman lumbers over, hands you 5 big ones and ..." The game can be saved in its current state at anytime **1799**.

[0045] Figure 11 depicts network-related mobile station usage information associated with the player 100 which is used to enhance the realism and enjoyment of the game of the presently preferred embodiment. In Figure 11, "mobile usage profiling" information, namely information regarding the patterns of use of mobile communications by the player 100, is communicated from the network 306 to the server 310. Such profile information includes, for example, the fact that player 100 is currently actually located in the city of Los Angeles. This information can be used in the multi-player interactive fiction game of the presently preferred embodiment by creating a virtual space 312 made up of locations in the city of Los Angeles, thus lending additional realism and interest to the game. The game itself can be designed with profiling information in mind. For example, within the definition of a virtual world, *e.g.*, lightweight interactive fiction engine language (LIFE), profile tags can be specified. The profile tags are used to indicate that the virtual world should be customized at the tag point. Customizing can include extracting relevant information from the mobile station or from a profiling database on a server. For example, if the game space dictates that a player is moving (or walking) towards, *e.g.*, a train station, a profile tag can be used to indicate that a relevant station name be inserted into the virtual world. For example, Waterloo Station in London can be inserted into a virtual space built around a London theme.

[0046] Figure 12 depicts how information regarding the manner in which player 100 plays the multi-player interactive fiction game of the presently preferred embodiment is incorporated into the game. This information is called "game play profiling" information. Thus, if the player 100 shows, during the course of a game, a preference for a particular type of action, say one associated with travel, this preference can be conveyed between the lightweight language application 406 and the server 310. The game can then be adapted to include more options of this type for the player 100 on a real time basis. Thus adding additional credibility and interest to the game.

[0047] Figure 13 depicts a lightweight interactive fiction engine language (LIFE) used to create the virtual space in a cost effective and well documented manner. Thus, allowing the virtual space to be evolved over time. LIFE is a generic description language which utilizes the Java™ environment.

[0048] A LIFE world **1312** which forms the basis for the game of the presently preferred embodiment, is one of the set of worlds **1300** which can be supported in the system. The world **1312** is made up of a set of "levels" **1302**, one of which can, for example, be defined as "Los Angeles" **1316**.

[0049] Each level, *e.g.*, **1316** is made up of a number of connected "locations", e.g., The Grand Hotel in Los Angeles **1320**. The Grand Hotel is one of the set of locations **1304** in Los Angeles **1316**. Within each location is a set of objects **1306** *e.g.*, a door **1326** in the hotel on the second floor, which is a subset of the set of objects **1306**. Each such object **1306** is "interactable" and the user may interact with the object through associated actions. An action, in a set of actions **1308**, can be, for example, "to open" **1330**. Finally, associated with each action is a set of object attributes **1310**, for example, "opened" **1334**. Thus the specific world being considered 1312 is divided into a set of levels, for example, Los Angeles 1316. Each level has a set of locations, for example, The Grand Hotel 1320. The Grand Hotel 1320 has a set of objects, for example, a door 1326 on the second floor with which a player may interact. Interaction rules are defined by a set of actions, for example, to open 1330, that may be associated with either objects or locations. The consequence of the action is an attribute, for example, door opened 1334. A player can either be a human player 100 or a software agent 614. The "view" of the virtual space which is presented to the player 100 or 614 will vary according to the current actual location of the player 100 or 614. The available interaction options and objects will vary correspondingly.

[0050] Locations, for example, The Grand Hotel 1320, define the fabric of the LIFE world. Locations describe all rooms, places, etc. which are accessible to players 100, 104, or 604. Each location has a description which allows a player to determine his position. Each location has a set of connections to other locations, for example, an airport **1322**. Connections define the topology of the LIFE world and are used by the LIFE engine to define the navigational options available to a player. Location specific interaction is defined via a set of specific actions.

[0051] Object definitions, for example, the door 1326, are used to describe items with which a player can interact. Like locations, objects have a description allowing players 100, 104, or 604 to know what the object is. The players are made aware of a set of actions defining permitted, object specific, interaction rules, for example, to open 1330. A set of object attributes 1310 representing the state of the object, for example, door is open 1334, is also provided.

[0052] In the presently preferred embodiment, actions, for example, to open 1330, may require more advanced interaction than merely applying them to an object. As an example, a key may be required to open a locked door. LIFE handles these situations by allowing actions to have arguments of a specific type. For example, the "unlock" action on the "door" would require a "key" as an argument.

[0053] Figure 14 depicts a game player 100 using a mobile station 102 to play an interactive fiction game on a mobile network. In the presently preferred embodiment, the mobile station 102 establishes a connection through a mobile network **1408** to a game server **1412**. A user agent **1404** is a simulacrum of the user 100. The user agent 1404 is a software entity acting for the game player 100 (or for the mobile station 102). It should be appreciated that reference is made to the user 100 and/or the user terminal 102 in an interchangeable manner, the intended meaning being clear from the particular context. The user agent 1404 is thus responsible for presenting a current state of the interaction fiction game to the user 100, and equivalently, acts as a communication intermediary between the user 100 and the game server 1412. The mobile network 1408 supports a connection between the mobile station 102 and the game server 1412. An interactive fiction engine (wireless game center) **1414** runs on the game server 1412. The engine 1414 supports the execution of a virtual world 1406 on the game server 1412. From an implementation perspective, in the presently preferred embodiment, the virtual world **1406** is an executable software component running on the interactive fiction engine 1414. The virtual world 1406 updates states which define it based on action requests received from the user 100 by means of the user agent 1404. Actions which can be taken in the game by the user 100 are determined by the state of the virtual world 1406. In the presently preferred embodiment, the virtual world is based upon a structured definition of content as described in Figure 13. The game server 1412 also contains a presentation engine **1416** which processes data relating to the game and the virtual world 1406 into a format that can be presented by the user agent 1404 on the mobile station 102. The presentation engine 1416 output can be tailored according to the limited man/machine interface available on the user terminal 102.

[0054] The virtual world 1406 can be defined using an XML schema, which is run through a world compiler, generating a computer language specific version of the particular virtual world 1406 definition being used. The language specific world is thus compiled into an executable form. Support for both the language and the virtual world concepts embodied in the definition of the virtual world, exist on the game server 1412.

[0055] It should be appreciated that the utilization of menu text presentations and icon display elements combined with hypertext user selectable menu items significantly ameliorates or substantially overcomes the complexities and difficulties of typing in free text commands on a mobile station keyboard. The particular issues encountered in a wireless communication environment, for example, low data rates, significant error rates, and wireless communication protocols, require particular technical solutions to present the aforementioned menu/icon/hypertext base system.

[0056] Predefined game options both within the story segment 704 and the interactive segment 708 result in a "tree" type of structure. The structure reprsents possible "routes" which a game player can travel depending on his or her choices as they move through the game. This type of game structure supports a "predictive command style implementation" thus, providing a streamlined form of interaction. In particular, by optimizing the options presented during game play, the amount of data transmitted to the mobile station is decreased. Thus, a more effective response time results. This result is particularly useful when utilizing low bandwidth, high latency networks.

[0057] Figure 15 depicts the profiling of mobile station activity in order to customize the service context. In the presently preferred embodiment, customization relates to the playing of an interactive fiction game. As a player 100 makes use of a mobile station 102, we note that there is a distinction between the virtual world within which the player plays the game, and the real world within which the player actually functions. Having made that distinction, it is noted that while fantasy is typically a desired characteristic of games, a degree of reality or mapping between the "real world" and the "virtual world" can, in fact, add a drama and a realism to the fantasy which enhances the entertainment impact. In one embodiment, the mobile station 102 maintains key environment information **1514-1516** in a storage memory 1504. This environment information 1514-1516 relates to the real world in which the player actually is situated. For example, the mobile station 102 can store in the onboard memory 1504 statistics such as call frequency, average call duration, top five local locations visited (that is, locations in the player's home country), top five global locations visited, top five wireless services accessed (for example, "follow me" enables calls directed to a particular mobile station to be forwarded to another mobile station), top five local numbers called, top five countries called, etc. These statistics can be constantly maintained, updated and stored in the memory 1504 of the mobile station 102. Thus they are available to be used in customizing a service which is required by the user from the user terminal 102.

[0058] Placing this information 1514-1516 into the game context, the various story segments can take place in particular, and familiar cities. The particular city provided as a virtual world when the user chooses to play a game can be made to correspond with the particular city in which the user is actually residing at the time. For example, if the user is presently in Sydney, Australia, the game context can be placed in Sydney and the virtual world, its various connected locations, and even the particular objects within the virtual world can all be tailored to provide a feeling of pleasing familiarity with the actual city in which the user is currently located. A native of Sydney will be able to actually recognize aspects of the virtual world if this is desired. In the presently preferred embodiment, when a game is started, a set of locations, that is, cities, can be automatically selected based upon the information in a user profile stored in the memory **1504**. If a player calls London and Helsinki frequently, instead of selecting the city where the player currently resides, these cities could be selected instead. This feature is particularly pertinent if the user uses his mobile station when he is in those cities, as it provides an insight that the player has actually visited those cities, and would thus be expected to have some familiarity with their physical surroundings.

[0059] It is possible to use this profiling of mobile station activity both at the level of city selection, and/or at the level of particular location profiling within a given city. Thus, the virtual world 312 can be customized to include those locations that the game player frequents, such as suburbs, streets, cafes etc. This level of customization depends upon the level of accuracy associated with the location statistics which are gathered. The usage profile of a mobile station can include many attributes aside from telephone calls. For example, usage profiling can include information from the calendar, address book, contacts list, messages, and other non-phone applications that reside on the mobile station 102. This type of profiling can be seen in the following example: when a player receives notification that "They need to meet the fat man on the comer of 5th and Park Avenue at 5pm", a booking for that time is placed into the mobile station calendar. Another example from an interactive fiction game: when two people sit down at a table in a cafe and exchange business cards. In such a scenario, each player's contacts list would be updated by the server with the business card of the other player. Thus, the usage profile can affect the game state and the game state can be made to affect the usage profile.

[0060] In addition to usage profiling, the mobile station itself can be used to introduce real world data to affect the game state. For example, the clock in the mobile station could be used to set the time in the virtual game space. In another instance, a mobile station equipped with a sound recorder and voice detection facilities can be used to modify the state of a game. For example, the game may require the player to proceed to a particular location and obtain a clue. The clue could be a sound segment that when "found" (that is, recorded and transmitted), changes the state of the game. Thus, the mobile station can affect the game state and the game state, in turn, can affect the mobile station.

[0061] Mobile station activity profiling is a software component 1520 which resides in the mobile station 102, and can include an optional software component 1518 residing on a remote server 1412. The flexibility to distribute this information between information gathered by the mobile station 102 itself and information gathered within a network 1500 is extremely useful. While information gathered by the mobile station 102 will have a first level of accuracy and detail, being gathered by the mobile station 102 itself, there is no issue in gaining privileged access to information which a network operation may be unwilling to provide. This latter type of information would reside on the remote server 1412. On the other hand, the richness of information available to the operator of a network 1500 is undoubtedly greater than that afforded by information gathering capabilities within a mobile station 102. The present embodiment thus enables these two types of information to be mixed and matched as desired.

[0062] It is appreciated that while mobile station activity profiling has been described above in the context of a network based electronic game, this type of profiling can equally be applied to other types of services which are accessed by means of the mobile station 102. Other services can include, for example: a restaurant guide in which is restaurants are listed according to mobile station location; an entertainment guide in which options are listed according to time and mobile station location; a virtual city tour can be presented based on location of the mobile station or destinations called; or a travel service which notifies a user of travel deals based on call history, contact list information, calendar entries, roaming locations, etc.

[0063] [illegible]arly, the user can be given the ability to turn automa[illegible]ofile data acquisition and processing on and off [illegible]n the mobile station, and within the broader network [illegible]text, as he desires. This feature enables users to have control over their own personal information and, more to the point in the present context, information which is secondary but nonetheless derived from their own behavior patterns.

[0064] In order to incorporate user profile information in a game, user profile information retrieved from the memory 1504 in the mobile station 102 is sent to the server 1412. The server 1412 incorporates this profile information into the game service 1414. The virtual world 1406 is then constructed while taking account of the user profile information. It is appreciated that maximum user control over confidential information is provided by maintaining the above described capability primarily within the mobile station 102 itself.

[0065] Figure 16 depicts deployment of virtual voice-based characters in a game setting within a wireless game environment. A voice character, which can for example, be entity 612 makes use of an interactive voice response unit (IVRU) 1600 in order to incorporate voice content into the game. The game runs on the game server 1412 to which a connection has been established by the mobile station 102 being used by the user 100. The IVRU 1600 interacts with the server 1412, enabling the server 1412 to incorporate voice response elements at the correct "time and place" within a game taking place within the virtual world 1406. As will be explained in more detail below, the IVRU 1600 interacts also with the mobile network 1408. This interaction is required to provide the actual voice input to the game and also to provide call connection and establishment facility.

[0066] The game player 100 playing a game encompassing a virtual world 1406 using a mobile station 102 can arrive at a point in the game where interaction with a voice based virtual character is possible. At this point, the game player 100 interacts with the character by vocalizing a game action, *i.e.*, speaking into the mobile station. The IVRU 1600 acts as a voice recognition unit to convert the vocalized command to a text response that can be sent to the game server 1412 across the connection. The game server 1412 receives the command and updates the game state (virtual world) 1406 accordingly. The game server 1412 then issues a command to the mobile station 102 to update the game context being presented on the mobile station 102. Should the game now require that the virtual voice based character vocally respond to the game players command, the game server 1412 issues a command to the IVRU 1600, directing the IVRU 1600 to generate a vocal response. An IVRU 1600 residing on the game server 1412 can send that vocal response to the mobile station 102 by means of a voice channel on the wireless. If an IVRU 1600 resides on the on the mobile station, a command can be sent to the mobile station 102 by the game server 1412 and then converted to a voice response.

[0067] In reference to the game described in Figure 17, at some point in the story segment, the player 100 may be presented with a prompt such as "your mobile phone is ringing". The game server 1412 could then place a call to the player's mobile terminal. Upon answering the call, the player will be greeted by a virtual voice character. The IVRU 1600 is used to realize the virtual voice character. The virtual voice character represents a virtual character in the game rendered in voice form. The character can be rendered in a textual format as well. An example realization of a virtual voice character can be, for instance, "Hi <player name>, it's the Commissioner here. Seems like we have a little problem and need your help. Someone is trying to frame you." The player 100 may then be prompted on the text display with a series of options. The series of options can be, for example, "What do you mean, someone is trying to frame me?" The player 100 may either select the option via the input keys 400 or may speak the phrase. The IVRU 1600 is used as a voice recognition unit to determine the selected option, in the event the player 100 chooses to speak the phrase, to be sent to the game server 1412.

[0068] In response, the game server 1412 chooses the appropriate story segment to deliver to the player 100. The story can be, for example, that the commissioner continues to warn the player. The commissioner's words are synthesized by an IVRU 1600 and can be, for example, "Look <player name>! We think it's Joe Diamond, but we can't be sure. If I was you, I'd watch my back and try to find out what he's up to." The player 100 can then be presented with a series of options on a textual display. The options can be, for example:

> "1. Thanks for the pointer Commish. I will watch my back. Let me know if you hear anything more."
> 2. Give me a break! Joe's in the slammer. Anyway, why would he want to set me up?"
> 3. Don't be stupid Commissioner. Joe would never do that to me. Goodbye, and bye the way, don't call me again!"

[0069] The player 100 can speak the options into the mobile station 102 or use the text input keys 400 to make a selection. Speaking the options invokes the voice recognition of the IVRU 1600.

[0070] As another example, the game player 100 can get to a point in the game where some type of advice is required. The game player can ask "what can I do here? " by directing this question to the mobile station microphone. This question is translated to text by the IVRU 1600 and sent to the game server 1412 over the connection. A software entity resident in the game examines the various options available to the player at this point, and replies "you can either take the left stairs down to the ground floor to escape the police or you can go up to the roof and catch the helicopter", via a voice call to the station.

[0071] In another example, a player can be initially drawn into a game via a series of phone calls placed to the player 100. Phone calls initiated by software entities to a player 100 inviting him to initiate a game would, typically, be based upon a user profile indicating that such calls would be welcome.

[0072] To facilitate use of the IVRU 1600, an interactive application, for example, the game described in Figure 13 can be configured with tags (or flags) which indicate that the IVRU 1600 can be used. For example, in the game described in Figure 13, either the game universe or a particular segment (or segments) of the game can be flagged as voice interactive. In this example, when the game server 1412 process a game or story segment that can utilize the IVRU 1600, the IVRU 1600 is activated for the particular game or story segment.

[0073] The IVRU 1600 can be resident on the mobile station 102 in order to implement the translation between voice commands from the game player 100 and the character strings which are sent over the connection to the game server 1412.

[0074] In an alternative embodiment, the IVRU 1600 can be resident in the game server 1412.

[0075] It should be appreciated that voice and cellular (GSM, CDMA, or TDMA) short message service can coexist, supporting the voice/data mix which is required in the aforementioned description. This is only one embodiment using a particular set of technologies to implement this type of functionality. It should further be appreciated that conversion from speech to text, or rather to character, can be implemented at the mobile station 102, thus enabling data only to be carried on the connection to the game server 1412. Alternatively, voice can be carried directly between the mobile station 102 and the game server 1412 over the connection and converted at the server. Various tradeoffs between processing power and network bandwidth enable different solutions to be found.

[0076] Figure 18 depicts a block diagram of a mobile station **1800** (and 102) that can be used in the disclosed embodiments. The mobile station 1800 includes, in this example:

[0077] A control head **1802** containing an audio interface, i.e. a speaker 1804 and microphone **1806**. The control head 1802 generally includes a display assembly **1808** allowing a user to see dialed digits, stored information, messages, calling status information, including signal strength, etc. The control head generally includes a keypad **1810**, or other user control device, allowing a user to dial numbers, answer incoming calls, enter stored information, and perform other mobile station functions. The keypad 1810 functions as the reduced keypad of the presently preferred embodiment. The control head also has a controller unit **1834** that interfaces with a logic control assembly **1818** responsible, from the controller unit 1834 perspective, for receiving commands from the keypad 1810 or other control devices, and providing status information, alerts, and other information to the display assembly 1808;

[0078] A transceiver unit **1812** containing a transmitter unit **1814**, a receiver unit **1816**, and the logic control assembly 1818. The transmitter unit 1814 converts low-level audio signals from the microphone 1806 to digital coding using a codec (a data coder/decoder) **1820**. The digitally encoded audio is represented by modulated shifts, for example, in the frequency domain, using a shift key modulator/demodulator **1822**. Other codes transmission utilized by the logic control assembly 1818, such as station parameters and control information, may also be encoded for transmission. The modulated signal is then amplified by RF amplifier **1824** and transmitted via an antenna assembly **1826**;

[0079] The antenna assembly 1826 contains a TR (transmitter/receiver) switch 1836 to prevent simultaneous reception and transmission of a signal by the mobile station 1800. The transceiver unit 1812 is connected to the antenna assembly 1826 through the TR switch 1836. The antenna assembly contains at least one antenna **1838**;

[0080] The receiver unit 1816 receives a transmitted signal via the antenna assembly 1826. The signal is amplified by receiver amplifier 1824 and demodulated by shift key demodulator 1822. If the signal is an audio signal, it is decoded using the codec 1820. The audio signal is then reproduced by the speaker 1804. Other signals are handled by the logic control assembly 1818 after demodulation by demodulator 1822; and

[0081] A logic control assembly 1818 usually containing an application specific integrated circuit (or ASIC) combining many functions, such as a general purpose microprocessor, digital signal processor, and other functions, into one integrated circuit. The logic control assembly 1818 coordinates the overall operation of the transmitter and receiver using control messages. Generally, the logic control assembly operates from a program that is stored in flash memory **1828** of the mobile station. Flash memory 1828 allows upgrading of operating software, software correction or addition of new features. Flash memory 1828 is also used to hold user information such as speed dialing names and stored numbers. The mobile station 102 aspects of the gaming environment can be stored in this memory.

[0082] Additionally, an IVRU 1600 can be connected to the logic control assembly or IVRU software can be executed by the logic control assembly in order to perform the voice input aspects of he presently preferred embodiment.

[0083] In addition to flash memory 1828, the mobile station will typically contain read only memory (ROM) **1830** for storing information that should not change, such as startup procedures, and random access memory (RAM) 1832 to hold temporary information such as channel number and system identifier.

[0084] Figure 19 depicts a block diagram of a cellular communications system suitable for implementing the disclosed embodiments. A cellular telephone system 10 has a plurality of mobile switching centers (MSC) 12, 14, 16, or mobile telephone switching offices (MTSO), that are connected to each other and to a public switched telephone network (PSTN) 18. Each of the mobile switching centers is connected to a respective group of base station controllers (BSC) 20, 22, 24. Each base station controller is connected to a group of individual base transceiver stations (BTS) 26, 28, 30. Each base transceiver station of the groups 26, 28, 30 defines an individual cell of the cellular telephone system.

[0085] Each base transceiver station of the groups 26, 28, 30 includes hardware and software functions required to communicate over communications channels of the system 10; and includes transmitters and receivers for communication with mobile telephone units. Each base transceiver station 26, 28, 30 also includes a plurality of individual standard receivers (StdR) 31 and scanning receivers (SR) 32 for scanning selected portions of the communications channel. Each base transceiver station 26, 28, 30 further includes digital multiplex equipment for transmission of audio traffic to its associated base station controller. It is the base transceiver stations 26, 28, 30, along with their associated base station controllers 20, 22, 24 and mobile switching centers 12, 14, 16 that perform the steps described herein in order to carry out one embodiment of the invention.

[0086] A plurality of digital mobile stations 1800 (or 102) is used with the system 10 for communication over the communications channel (or radio frequency traffic channel) with a particular base transceiver station of a particular cell in which the particular base transceiver station is located. According to the various disclosed embodiments, associated with each digital mobile station 1800 is a scanning receiver for scanning selected portions of the communications channel between the mobile station 1800 and the base transceiver station of serving and neighboring cells.

[0087] Each base station controller of the groups 20, 22, 24 implements audio compression/decompression, handles call establishment, disconnect, and handoff procedures, and allocates system resources between the individual base transceiver stations 26, 28, 30 associated with each of the base station controllers 20, 22, 24. More specifically, each base station controller 20, 22, 24 performs handoff execution for transferring ongoing communications from one cell to another within the group of base transceiver stations 26, 28, 30 connected to the particular base station controller 20, 22, 24. Each base station controller 20, 22, 24 communicates with its associated mobile switching center 12, 14, 16 for effecting a handoff involving a cell or base transceiver station 26, 28, 30 associated with a different base station controller. Each mobile switching center 12, 14, 16 processes all requests for calls, switching functions, as well as the mobility functions of registration, authentication and handoff.

[0088] As will be recognized by those skilled in the art, the innovative concepts described in the present application can be modified and varied over a tremendous range of applications, and accordingly the scope of patented subject matter is not limited by any of the specific exemplary teachings given.

[0089] For example, the disclosed embodiments are described as using a reduced keypad. Such keypads can be found on conventional mobile stations. However, any suitable input device may be used, such as a touchpad or voice-based system, for example.

[0090] For another example, the disclosed embodiments are described as providing an entertainment environment. However, the method and system described can be used for educational purposes as well. Moreover, a city selection made on the basis of a city the user would like to visit may be used to create an opportunity for travel or tourism promotion.

[0091] For another example, the disclosed embodiments are described in the context of a mobile station. However, it should be obvious to one skilled in the art that any suitable wireless terminal may be substituted for the mobile station described herein.

[0092] For another example, the disclosed embodiments are described as providing a text based game. However, the game could be played in the context of a graphical user interface and retain its customizable qualities.

Claims

1. A wireless system for interacting with a virtual space, comprising:

    a server, said server supporting a virtual space;
    a mobile station for allowing a first user to interact with said virtual space, said mobile station having at least a display for displaying information about said virtual space to said first user and data entry means to allow said first user to interact with said virtual space; and
    a communications network coupled between said server and said mobile station, said network having a wireless link to said mobile station.

2. The system of Claim 1, wherein said server hosts a game service.

3. The system of Claim 1, wherein said network further comprises a data link, said data link supporting software entities.

4. The system of Claim 1, wherein said network further comprises a video link to said mobile station.

5. The system of Claim 1, wherein said virtual space is an interactive fiction game.

6. The system of Claim 1, wherein said virtual space is an interactive tour.

7. The system of Claim 6, wherein said interactive tour covers at least one portion of a city where said first user is physically located at the time of said interactive tour.

8. The system of Claim 1, wherein said virtual space is a business activity.

9. The system of Claim 8, wherein said business activity is retail shopping.

10. The system of Claim 8, wherein said business activity is a virtual conference between said first user and at least a second physically remote user.

11. The system of Claim 8, wherein said business activity is wholesale shopping.

12. The system of Claim 1, wherein said virtual space provides said first user with a perceptual awareness of a second user, said second user being physically remote from said first user.

13. The system of Claim 1, wherein said virtual space provides said first user with a perceptual awareness of a software entity, said software entity being supported by said server.

14. The system of Claim 1, wherein said virtual space provides said first user with a perceptual awareness of objects in said virtual space, said objects representing features in said virtual space.

15. The system of Claim 1, said virtual space further comprising a lightweight language application.

16. The system of Claim 1, wherein said communication network further comprises a connection to a public switched telephone network.

17. The system of Claim 1, wherein said mobile station has a reduced keyboard, for accepting input from a user; and said server has means for running an interactive language application, for creating said virtual space.

18. The system of Claim 1, wherein said mobile station has been arranged to allow a user to establish an interactive session with said virtual space; said server has been arranged to host a game center; and wherein the system further comprises
a wireless application protocol gateway connected between said network and said server; anda game service running on said game center

19. The system of Claim 1, wherein said server has means for running a software application comprising a plurality of related segments,

said mobile station has been arranged to allow interaction with said software application by means of said display and said data entry means,

wherein said plurality of related segments is comprised of:

a story segment, said story segment further comprising action options that allow a first player to navigate spatially within said virtual space;

an interactive segment, said interactive segment allowing said first player to interact with features of said virtual space via said data input means; and

a decision process segment, said decision process segment allowing said first player to choose to continue to a new story segment or to quit interacting with said virtual space.

20. The system of Claim 19, wherein said interactive segment further allows said first player to interact with other players in said virtual space.

21. The system of Claim 1, wherein:

said server is a remote server; and the system further comprises an interactive language, operative within at least one of said mobile station and said remote server, for defining a virtual representation of said first user; and wherein said communication network links said mobile station and said remote server, wherein said first user establishes an interactive session with said server, wherein said mobile station receives data concerning said virtual space to be displayed on said display, and further wherein said first user can effect a change in a state of the virtual space by inputting data via the data entry means.

22. The system of Claim 21, wherein said mobile station data entry means includes at least a select key means and an enter key means.

23. The system of Claim 22, wherein a state of said virtual space is changeable by said first user using the said select key means to select an item, then said enter key means to interact with the selected item, at least some of the interactions effecting a change in state of said virtual space.

24. The system of Claim 23, wherein the items in the virtual space are selected from the group consisting of a world, a level, a location, an interactable object and an attribute of the object, a virtual representation of a second user of another terminal, a virtual representation of a software entity, and a software agent.

25. The system of Claim 23, wherein said items in said virtual space comprise a plurality of selectable locations, wherein said virtual representation of said first user is movably located at a first location, and further wherein said virtual representation of said first user can selectably move to a second location.

26. The system of Claim 21, wherein said display can display a visual representation of one or more items in said virtual space.

27. The system of Claim 21, wherein said selection means include scroll up and scroll down keys.

28. The system of Claim 21, wherein an item within said virtual space is changed dependent upon a particular profile of said first user.

29. The system of Claim 28, wherein said profile is dependent upon a manner in which said first user utilizes the network.

30. The system of Claim 28, wherein said profile is dependent upon a manner in which the user changes the state of said virtual space.

31. The system of Claim 21, wherein said interactive session comprises a multi-player interactive fiction game.

32. A wireless terminal having a display and a selection means, said terminal being operable to communicate with a remote server and to provide a user with an interactive session with said server, said server being configured to support a virtual space through which at least one virtual representation of said user can move, and wherein said terminal receives data concerning said virtual space to be displayed on said display, and wherein said user can input data via said selection means to effect a change to the state of said virtual space

33. The terminal of Claim 32, wherein said wireless terminal selection means includes at least a select key means and an enter key means, and wherein said display can display a visual representation of one or more items in said virtual space, and wherein a state of said virtual space is changeable by said user using said select key means to select an item, then the enter key means to interact with the selected item, at least some of the interactions effecting a change in a state of said virtual space.

34. The terminal of Claim 32, wherein said wireless terminal can support at least one of voice or data communications.

35. The system of Claim 1, wherein:

said mobile station comprises a transceiver for sending and receiving a signal to and from a base station;
said base station comprises a transceiver for sending and receiving a signal to and from said mobile station, wherein said base station is coupled to said communications network;
said virtual space is a game;
said server has means for running a game center software application, said application running said game;
wherein said base station is adapted to communicate with said game center software application;
wherein said mobile station is adapted to communicate a game state to said first user, to receive a command from said first user in response to said game state, and to convey a predetermined instruction associated with said command across a network to said server; and
wherein said server is adapted to change said game state dependent upon said instruction, and to communicate the changed state to said mobile station.

36. The system of Claim 35, wherein the changed state is communicated to said user via a menu, and wherein a menu selection by said user produces the associated predetermined instruction.

37. The system of Claim 36, wherein said menu comprises text and graphics.

38. The system of Claim 35, wherein the change in game state by said server is dependent upon an earlier mobile station use by said user.

39. The system of Claim 35, wherein said base station communicates with said game center software application through a gateway.

40. The system of Claim 35, wherein said server is adapted to change the game state from a first game state to a second game state; wherein said first game state and said changed game state are respective states of said virtual space.

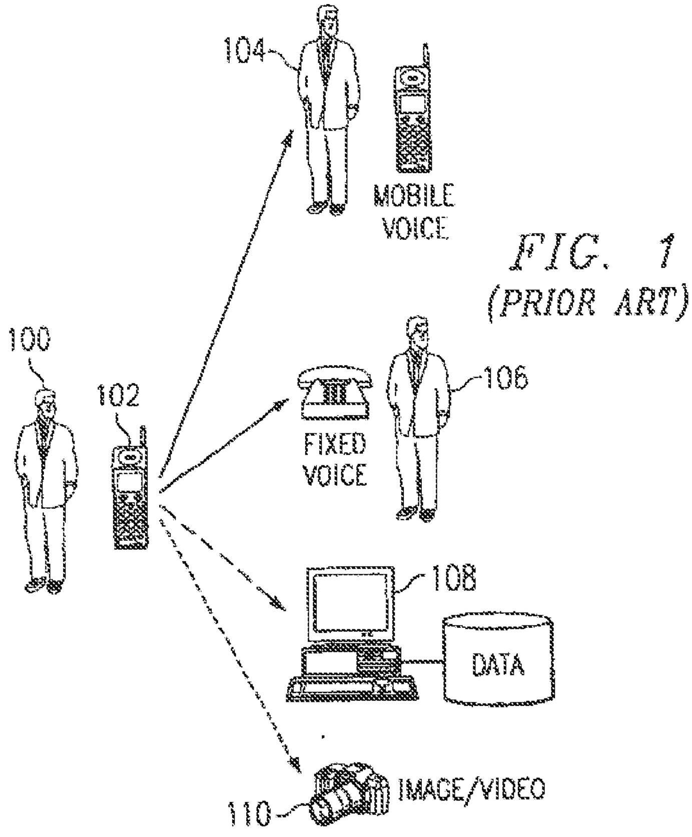
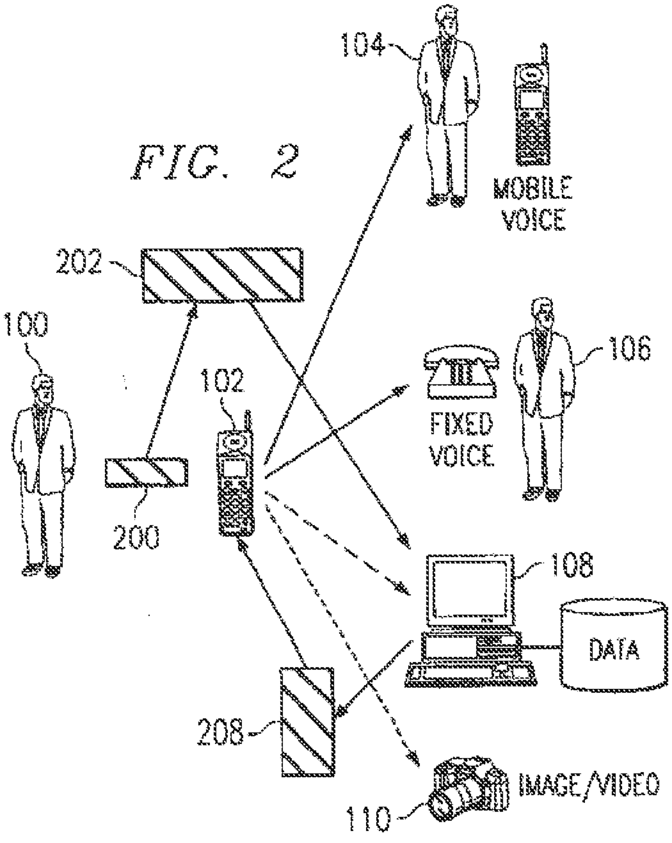


FIG. 1
(PRIOR ART)

FIG. 2



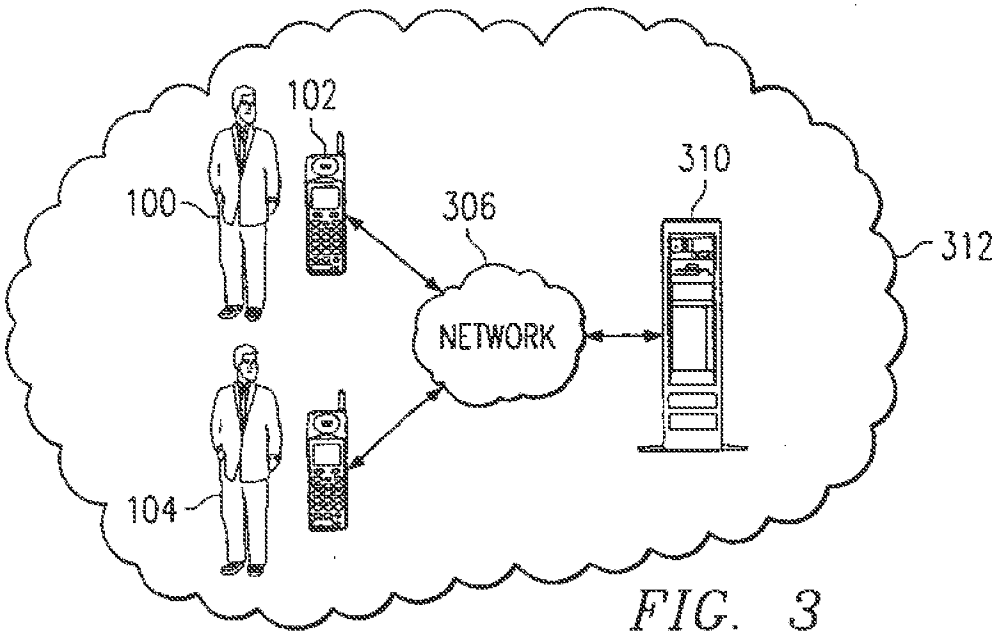

102
310
100
306
312
NETWORK
104

FIG. 3

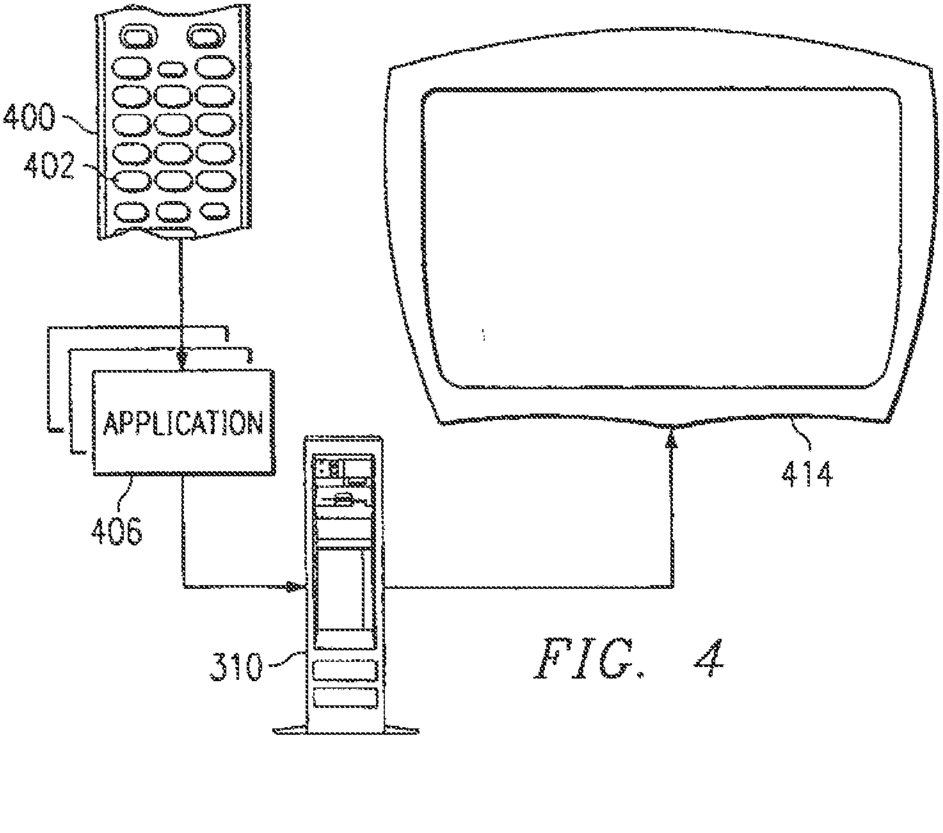

400
402
APPLICATION
406
414
310

FIG. 4

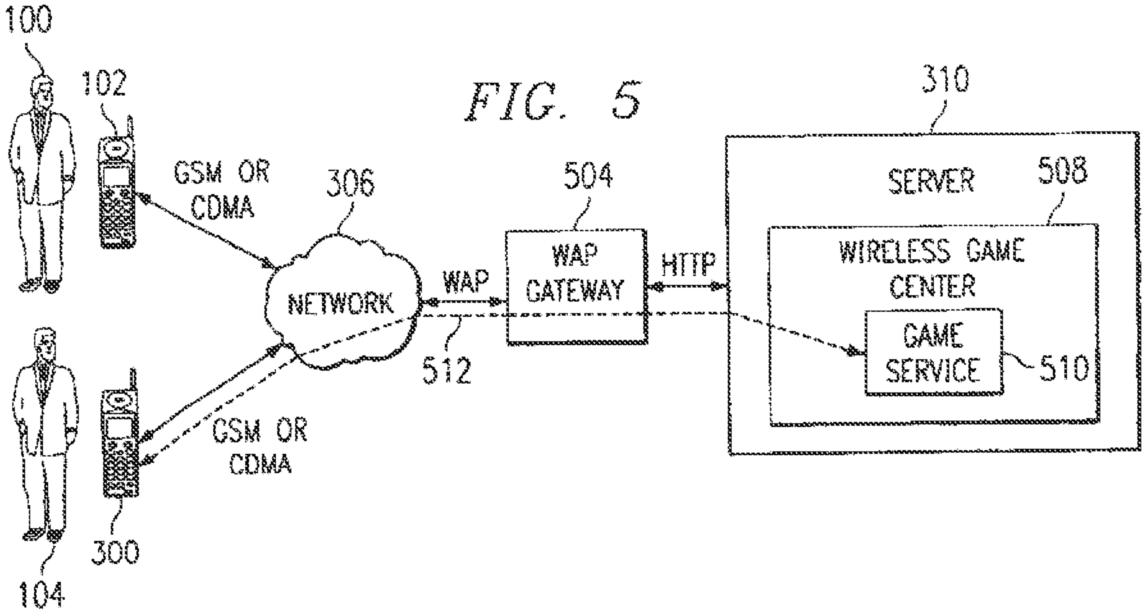

100
102
GSM OR CDMA
306
NETWORK
WAP
504
WAP GATEWAY
HTTP
310
SERVER
508
WIRELESS GAME CENTER
GAME SERVICE
510
512
GSM OR CDMA
300
104

FIG. 5

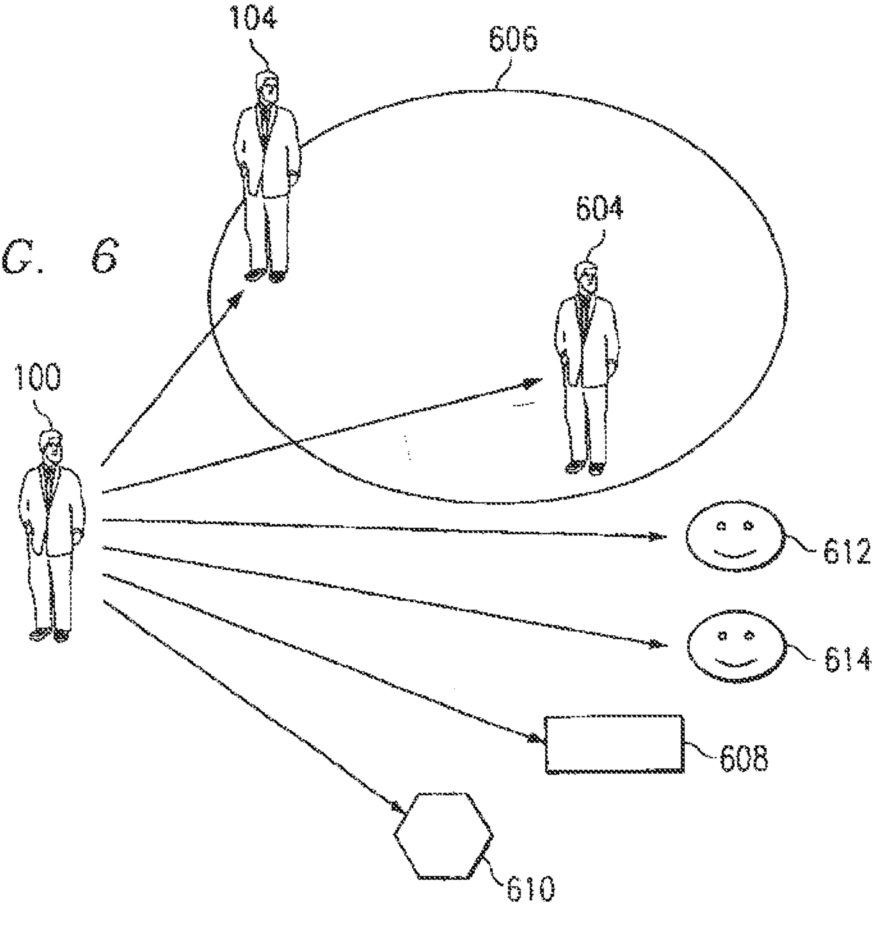

104
606
604
100
612
614
608
610

FIG. 6

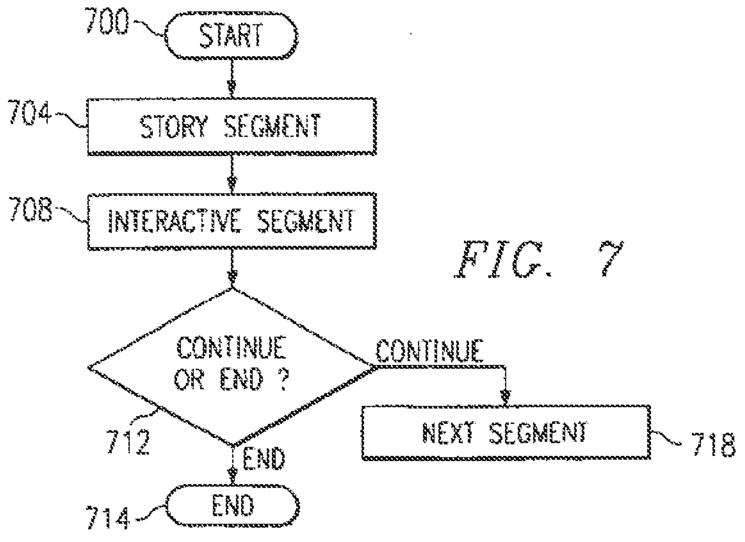


FIG. 7

FIG. 8

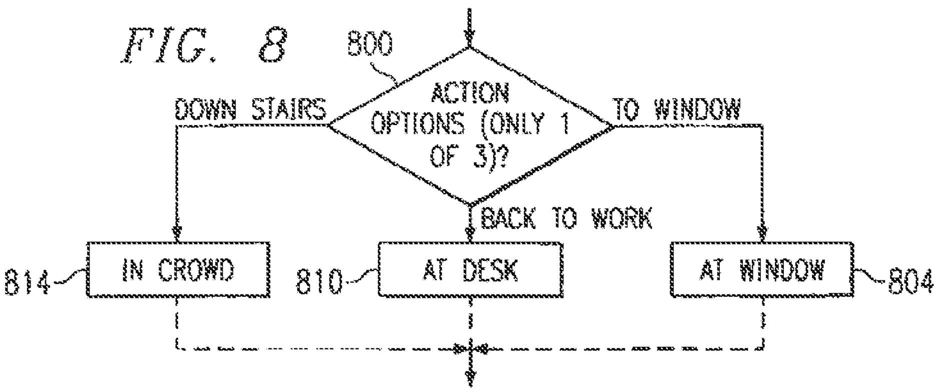
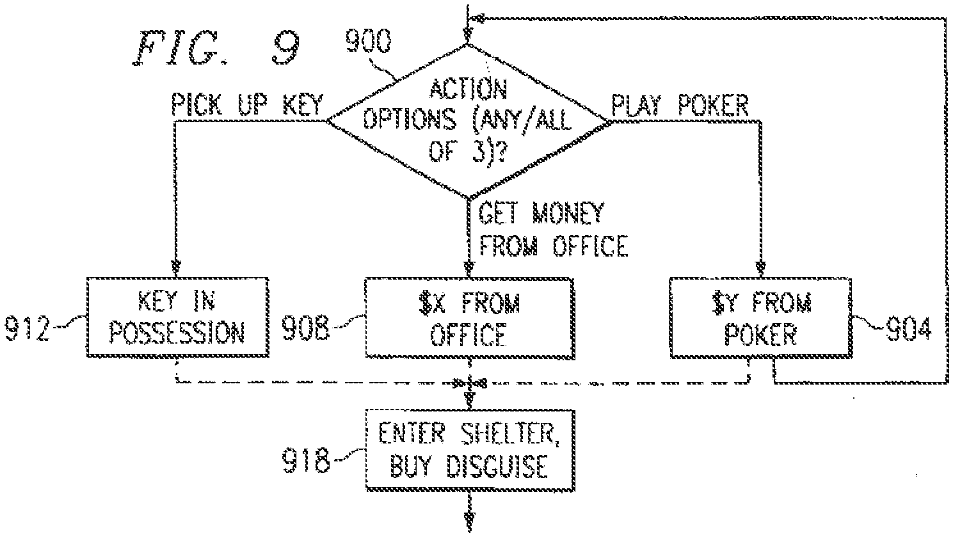


FIG. 9



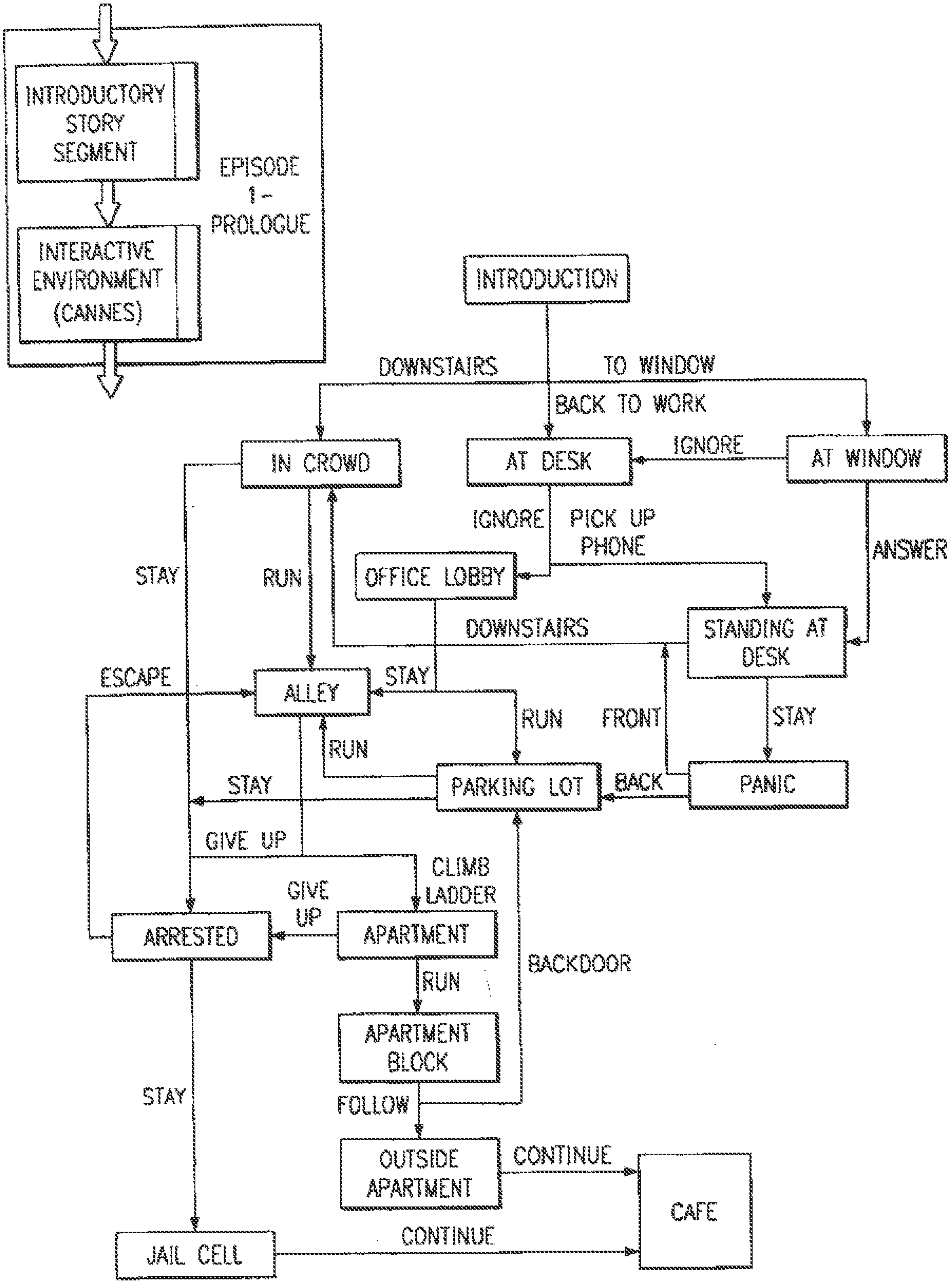

INTRODUCTORY STORY SEGMENT
INTERACTIVE ENVIRONMENT (CANNES)
EPISODE 1 - PROLOGUE
INTRODUCTION
DOWNSTAIRS
TO WINDOW
BACK TO WORK
IN CROWD
AT DESK
IGNORE
AT WINDOW
IGNORE
PICK UP PHONE
ANSWER
STAY
RUN
OFFICE LOBBY
DOWNSTAIRS
STANDING AT DESK
ESCAPE
ALLEY
STAY
RUN
FRONT
STAY
RUN
PARKING LOT
BACK
PANIC
STAY
GIVE UP
CLIMB LADDER
GIVE UP
ARRESTED
APARTMENT
RUN
BACKDOOR
APARTMENT BLOCK
STAY
FOLLOW
OUTSIDE APARTMENT
CONTINUE
CAFE
JAIL CELL
CONTINUE

FIG. 10

FIG. 11

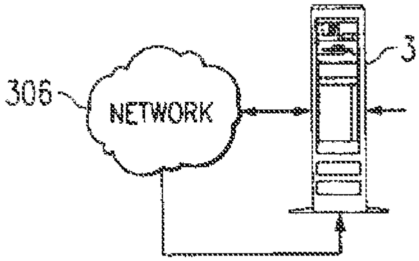


FIG. 12

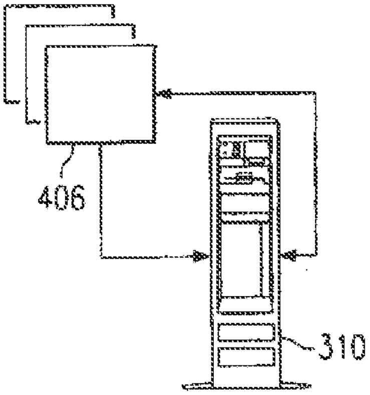
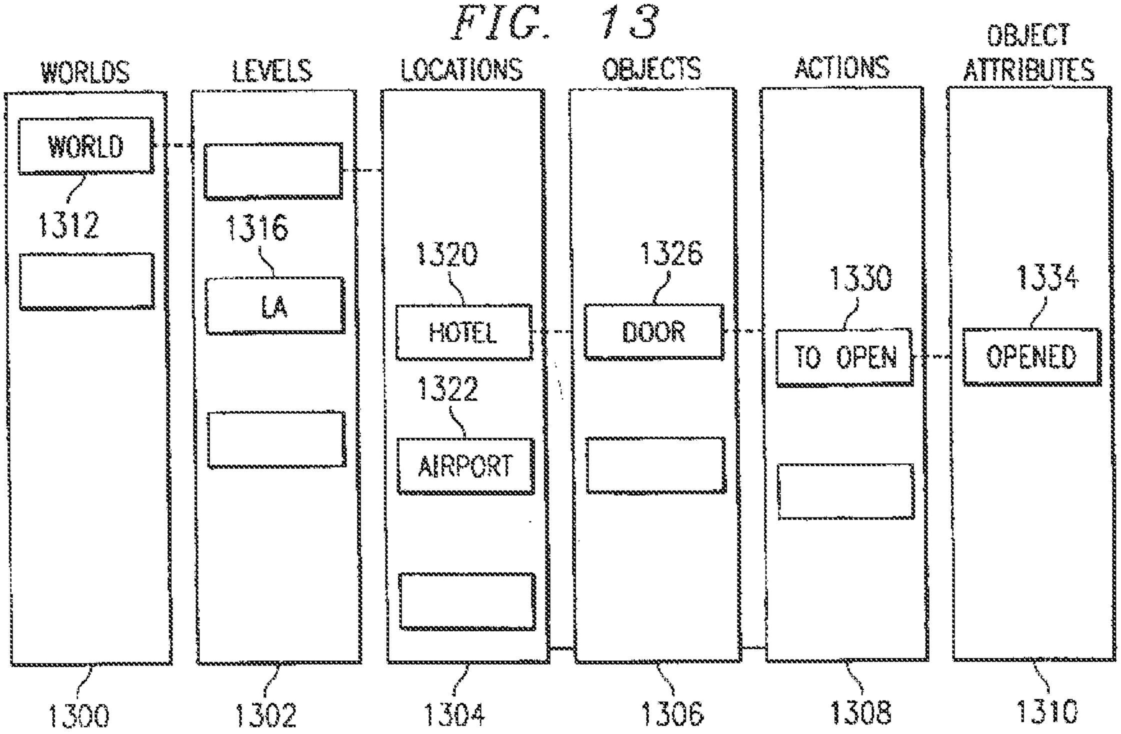


FIG. 13



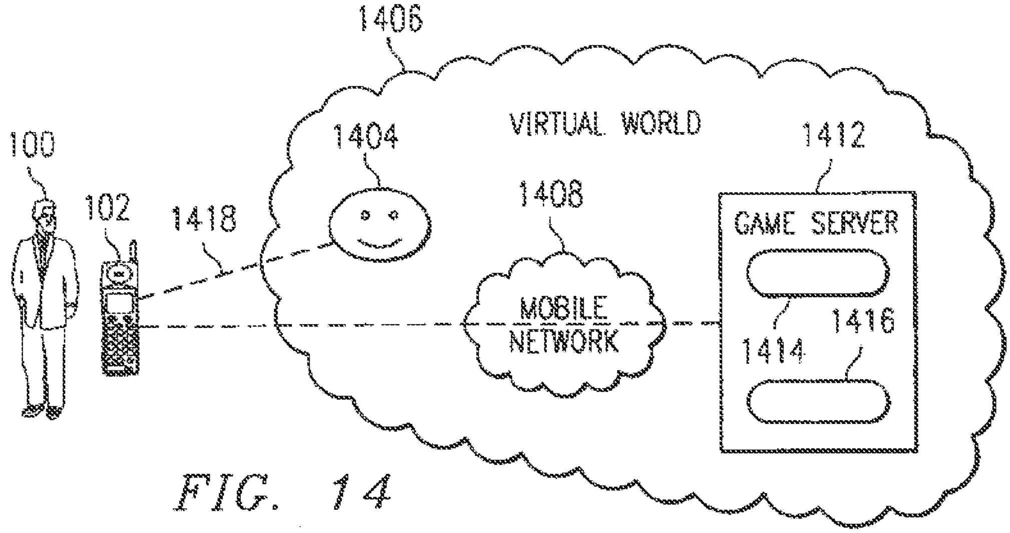

1406
VIRTUAL WORLD
100
1404
1412
102
1418
1408
GAME SERVER
MOBILE NETWORK
1414
1416

FIG. 14

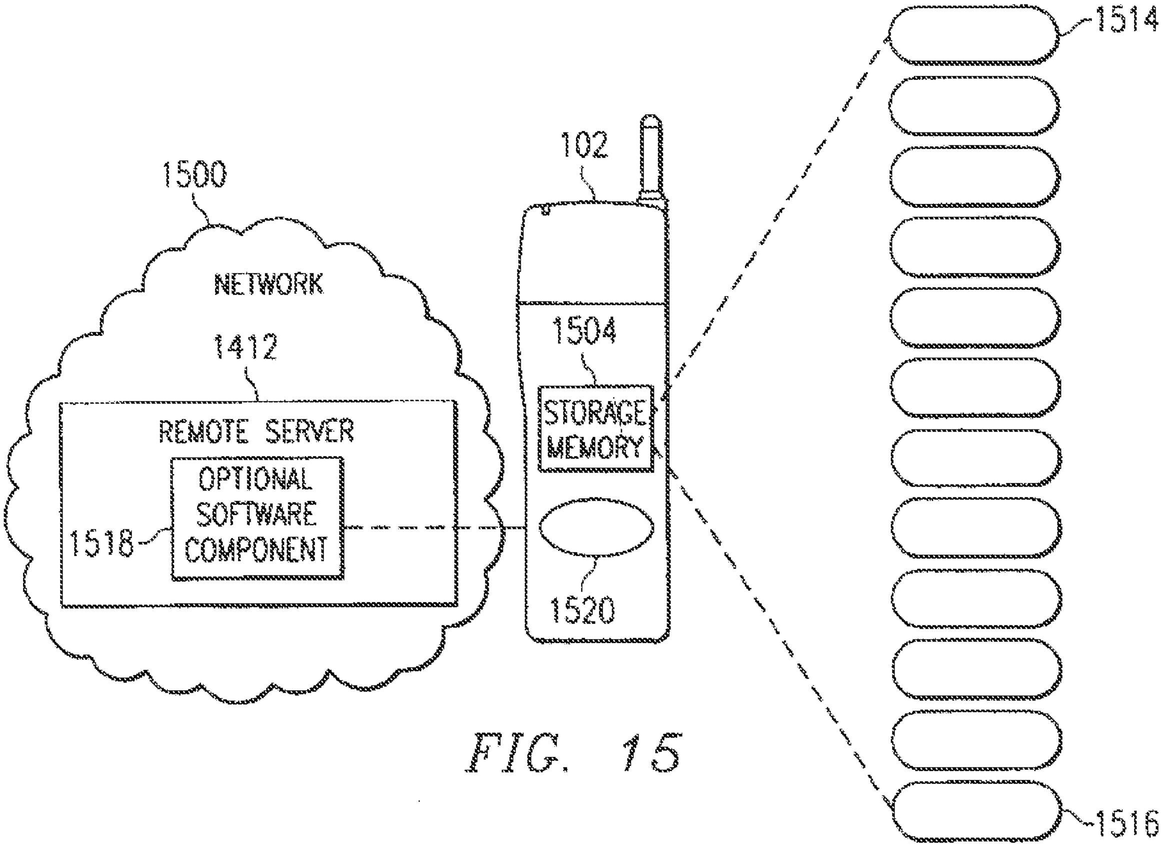

1514
102
1500
NETWORK
1504
1412
STORAGE MEMORY
REMOTE SERVER
OPTIONAL SOFTWARE COMPONENT
1518
1520
1516

FIG. 15

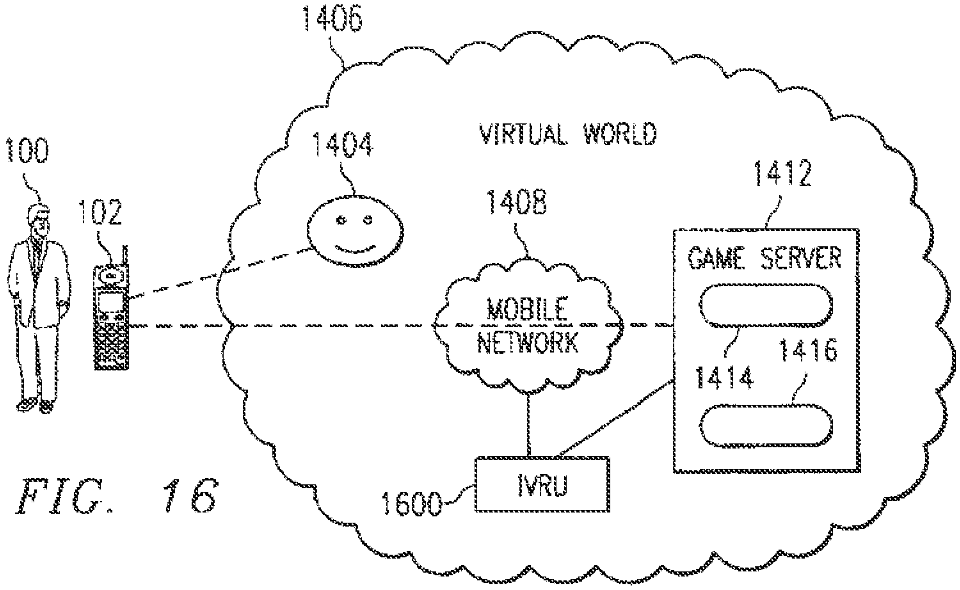
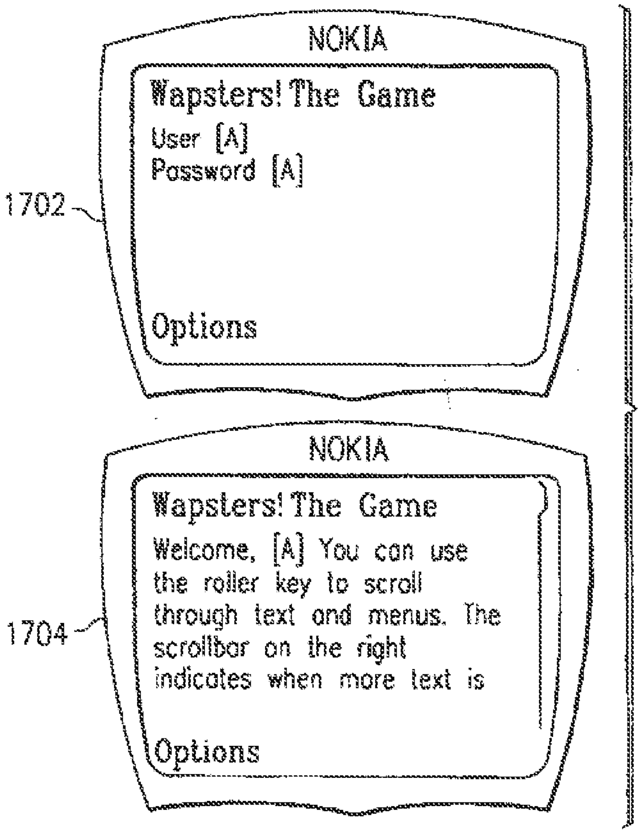


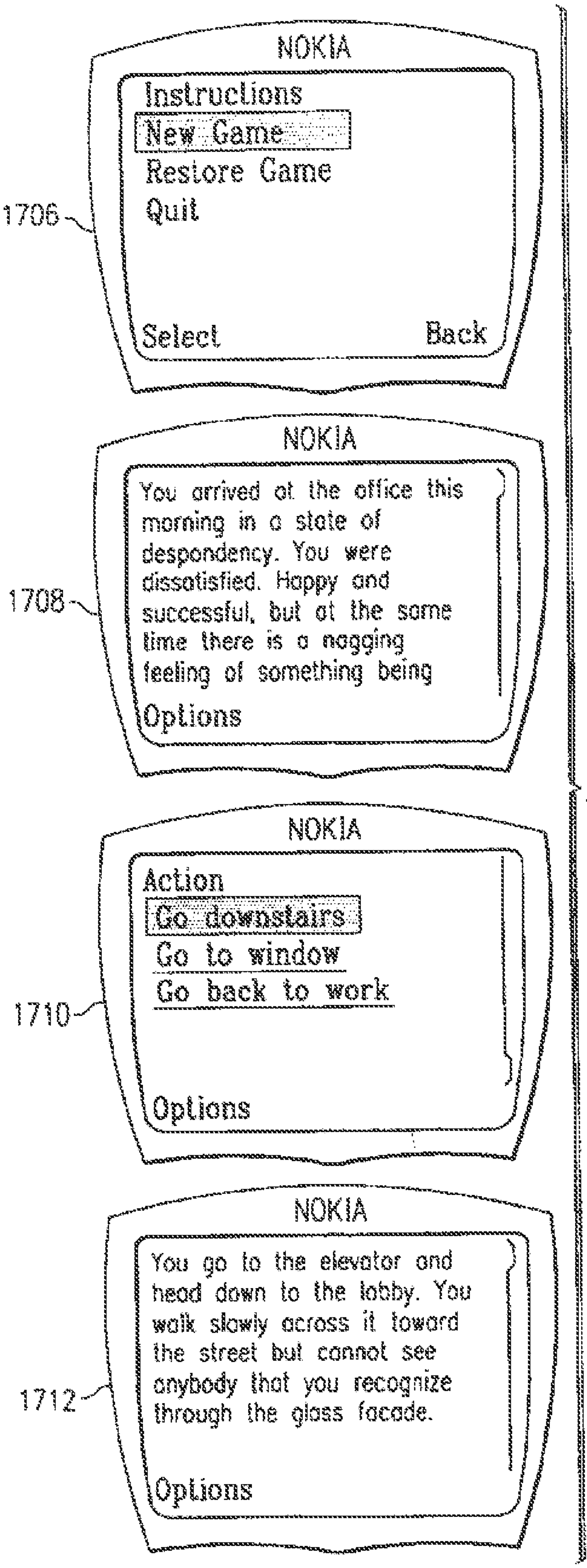
FIG. 16



Wapsters! The Game
User [A]
Password [A]
Options

Wapsters! The Game
Welcome, [A] You can use the roller key to scroll through text and menus. The scrollbar on the right indicates when more text is
Options

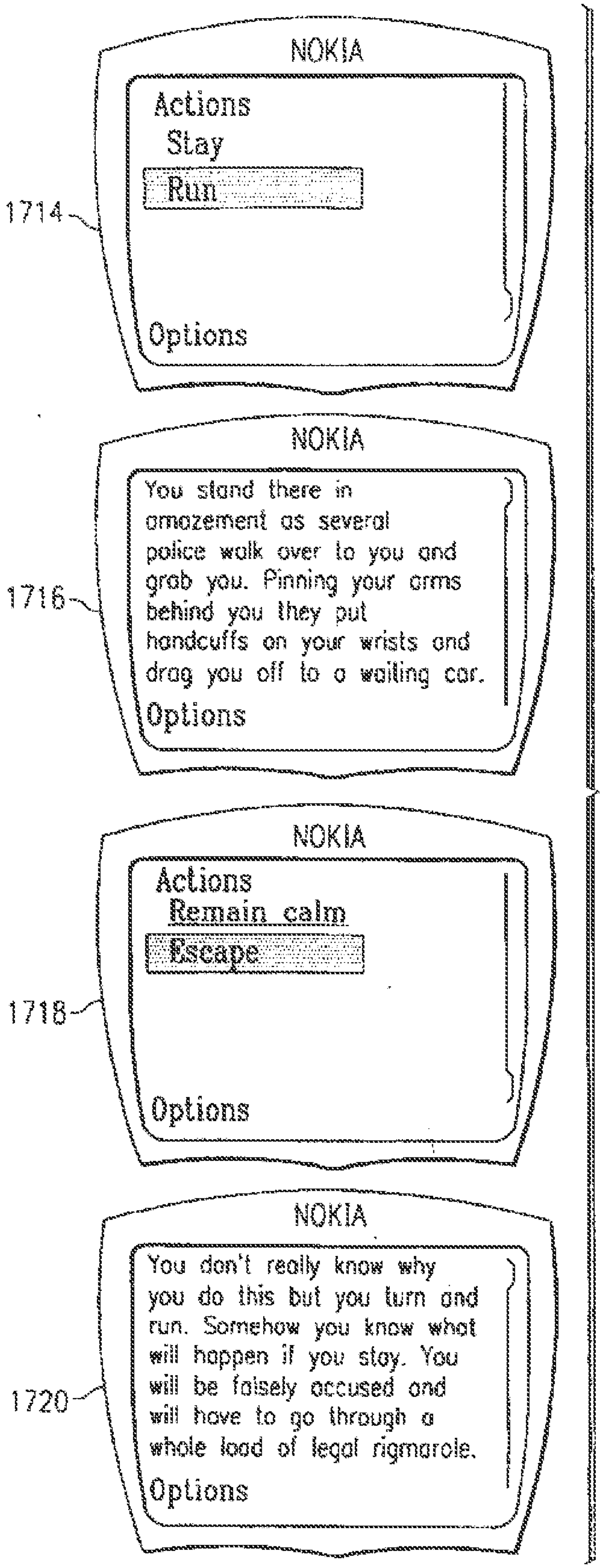
FIG. 17A



You arrived at the office this morning in a state of despondency. You were dissatisfied. Happy and successful, but at the same time there is a nagging feeling of something being

You go to the elevator and head down to the lobby. You walk slowly across it toward the street but cannot see anybody that you recognize through the glass facade.

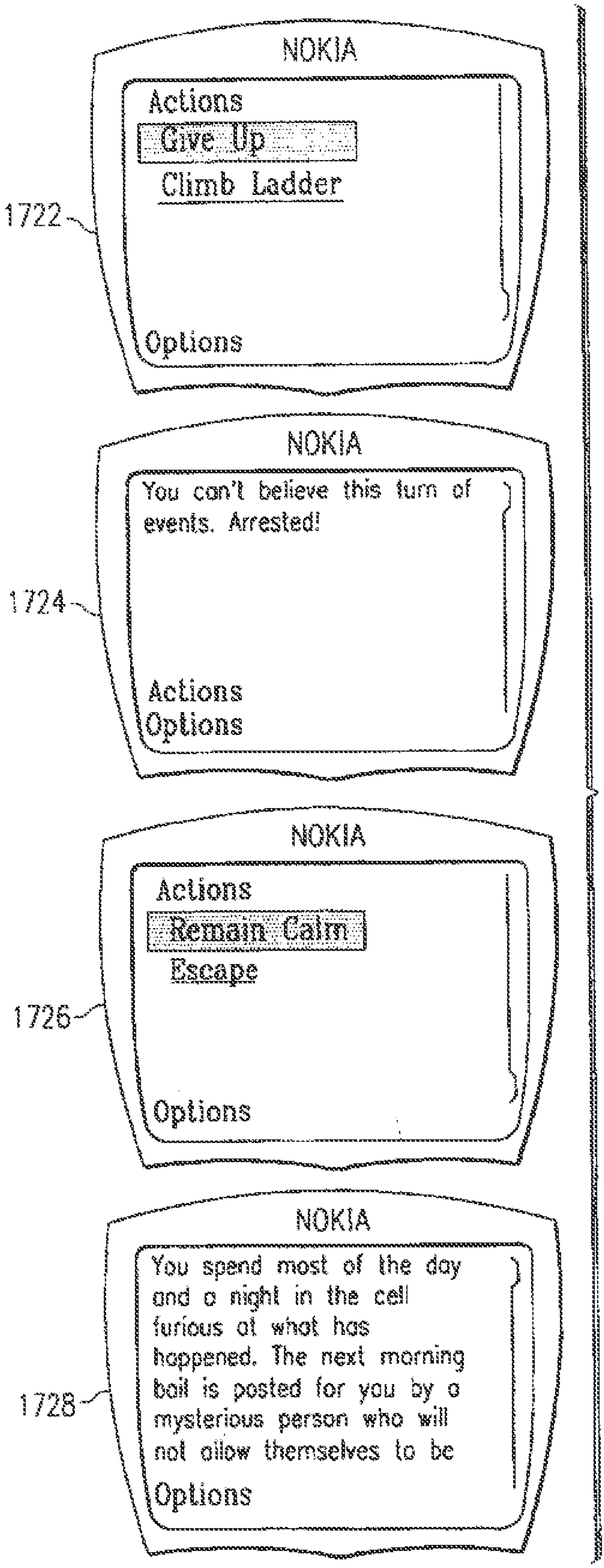
FIG. 17B



You stand there in amazement as several police walk over to you and grab you. Pinning your arms behind you they put handcuffs on your wrists and drag you off to a waiting car.

You don't really know why you do this but you turn and run. Somehow you know what will happen if you stay. You will be falsely accused and will have to go through a whole load of legal rigmarole.

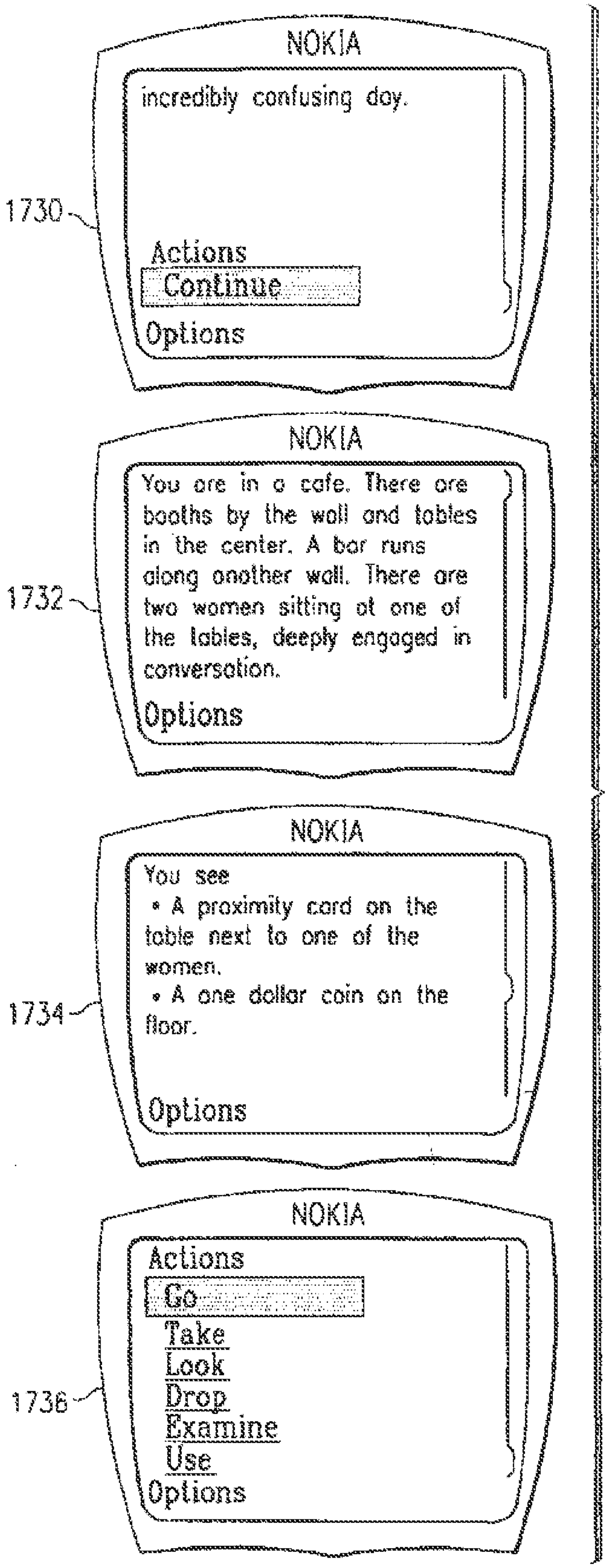
FIG. 17C



You can't believe this turn of events. Arrested!

You spend most of the day and a night in the cell furious at what has happened. The next morning bail is posted for you by a mysterious person who will not allow themselves to be

FIG. 17D



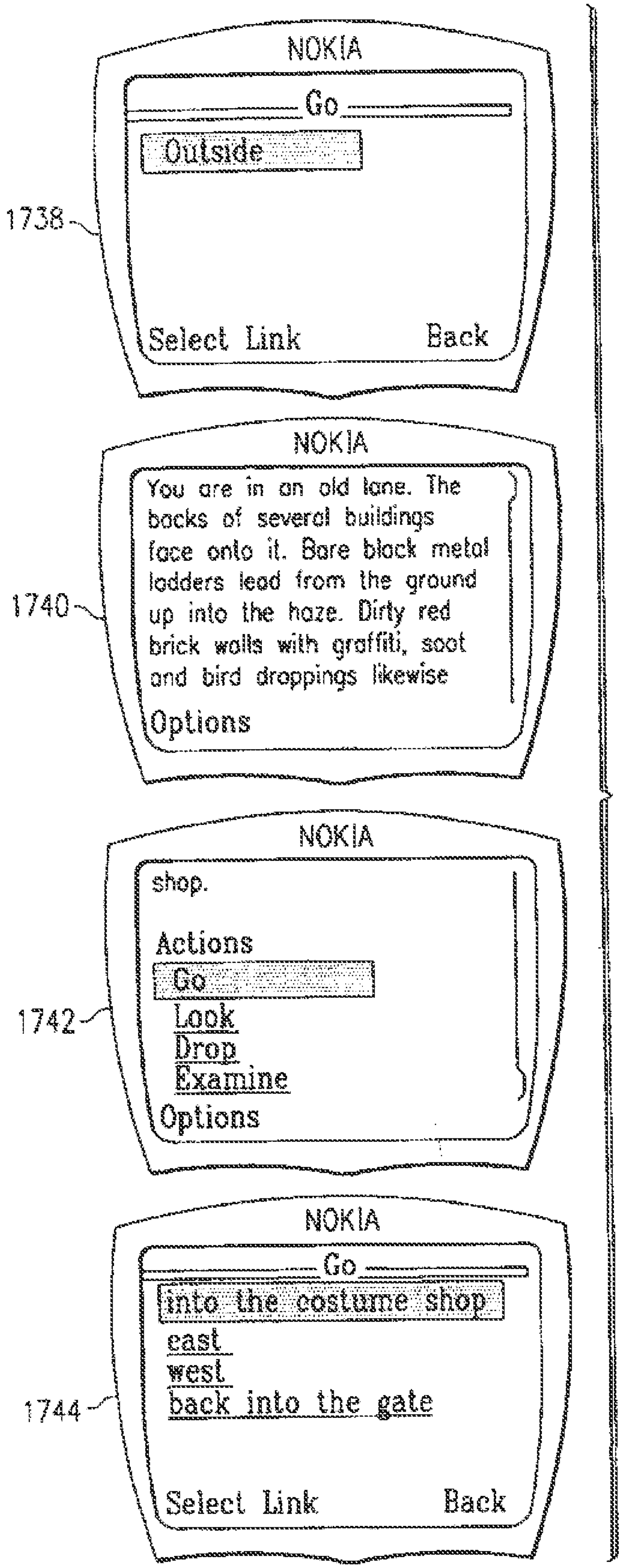
incredibly confusing day.

You are in a cafe. There are booths by the wall and tables in the center. A bar runs along another wall. There are two women sitting at one of the tables, deeply engaged in conversation.

You see

- A proximity card on the table next to one of the women.
- A one dollar coin on the floor.

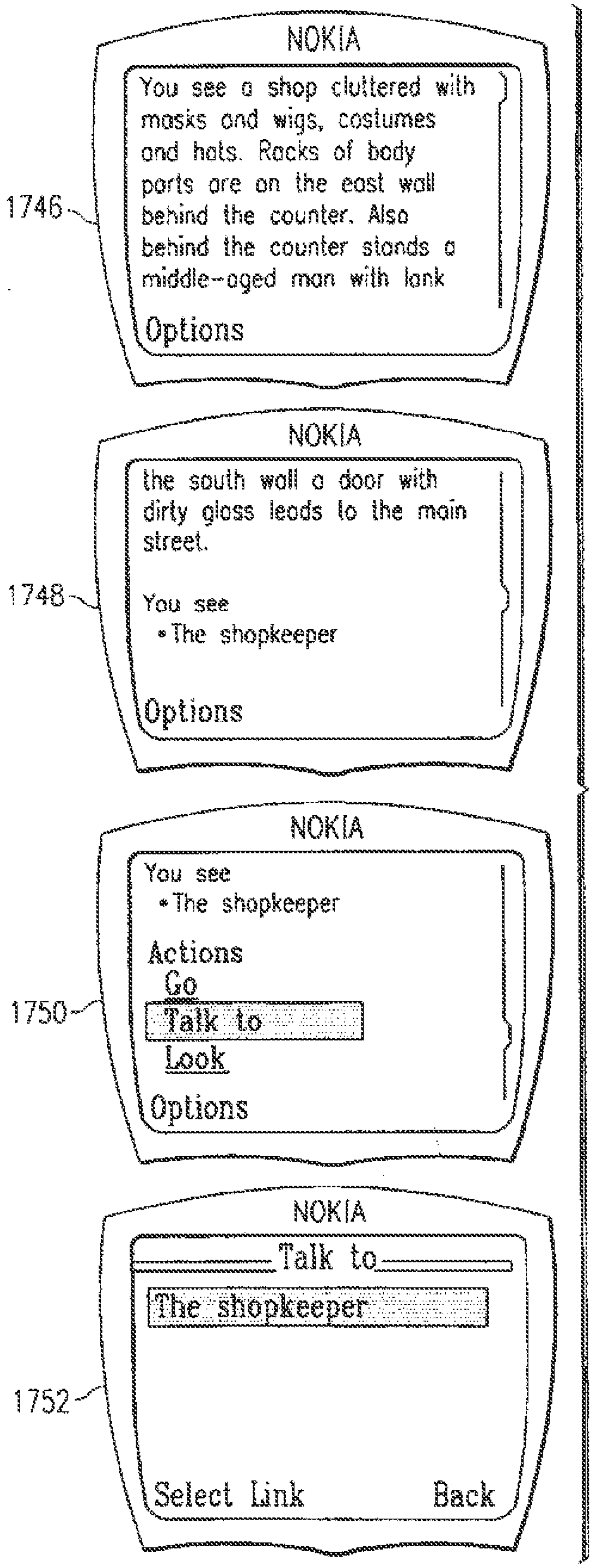
FIG. 17E



You are in an old lane. The backs of several buildings face onto it. Bare black metal ladders lead from the ground up into the haze. Dirty red brick walls with graffiti, soot and bird droppings likewise

shop.

FIG. 17F



NOKIA

You see a shop cluttered with masks and wigs, costumes and hats. Racks of body parts are on the east wall behind the counter. Also behind the counter stands a middle-aged man with lank

Options

NOKIA

the south wall a door with dirty glass leads to the main street.

You see

- The shopkeeper

Options

NOKIA

You see

- The shopkeeper

Actions

Go

Talk to

Look

Options

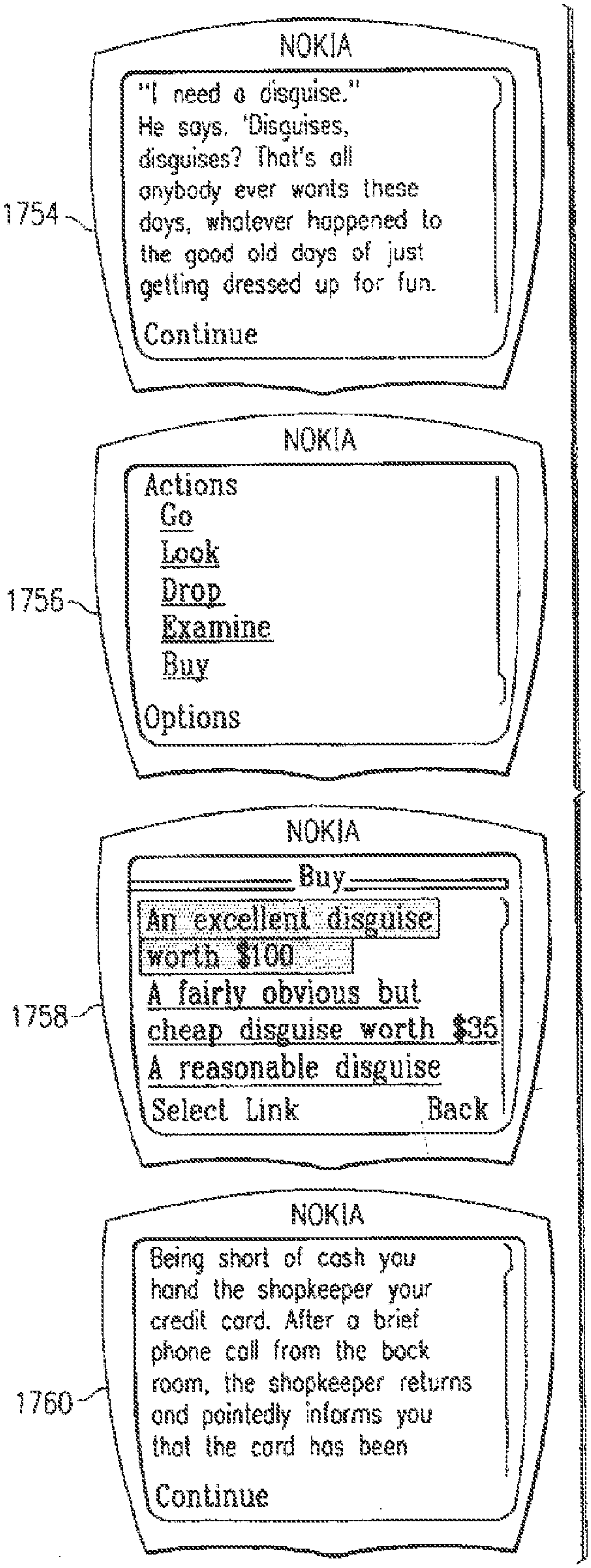
NOKIA

Talk to

The shopkeeper

Select Link Back

FIG. 17G



"I need a disguise."
He says. 'Disguises, disguises? That's all anybody ever wants these days, whatever happened to the good old days of just getting dressed up for fun.

Continue

Actions
- Go
- Look
- Drop
- Examine
- Buy

Options

Buy

An excellent disguise worth $100

A fairly obvious but cheap disguise worth $35

A reasonable disguise

Select Link Back

Being short of cash you hand the shopkeeper your credit card. After a brief phone call from the back room, the shopkeeper returns and pointedly informs you that the card has been

Continue

FIG. 17H

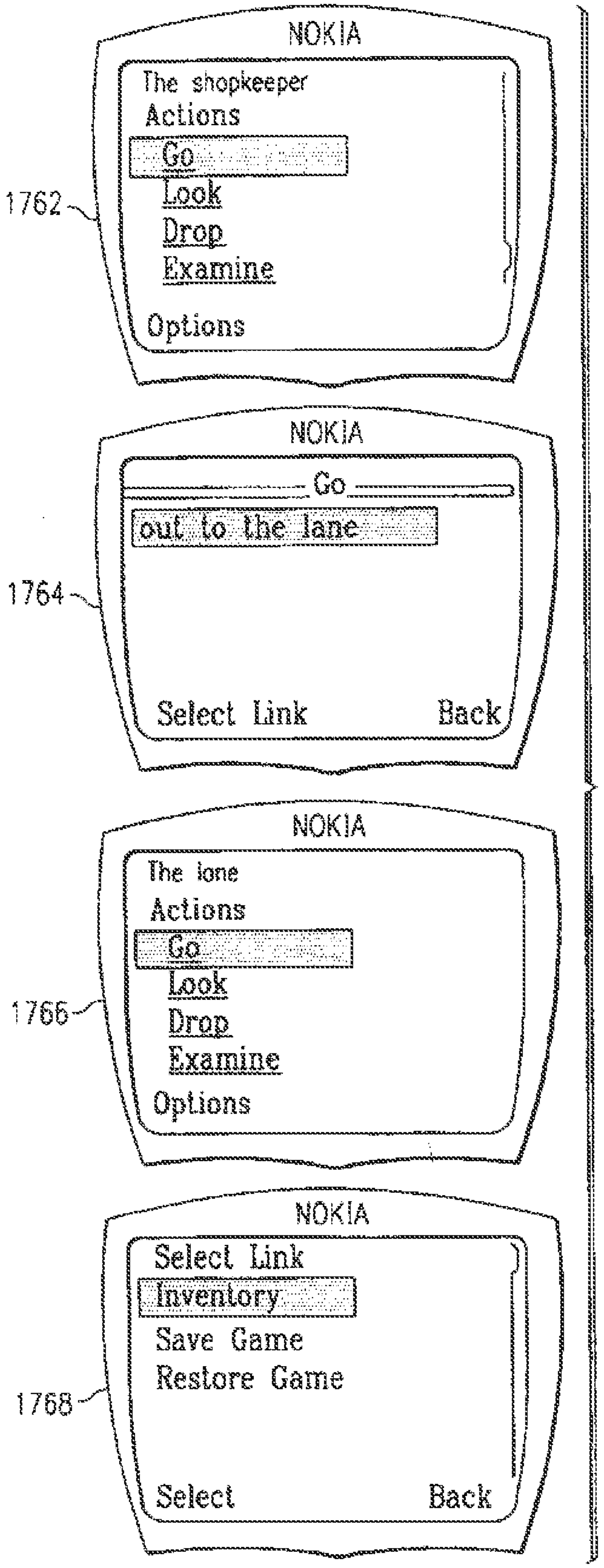
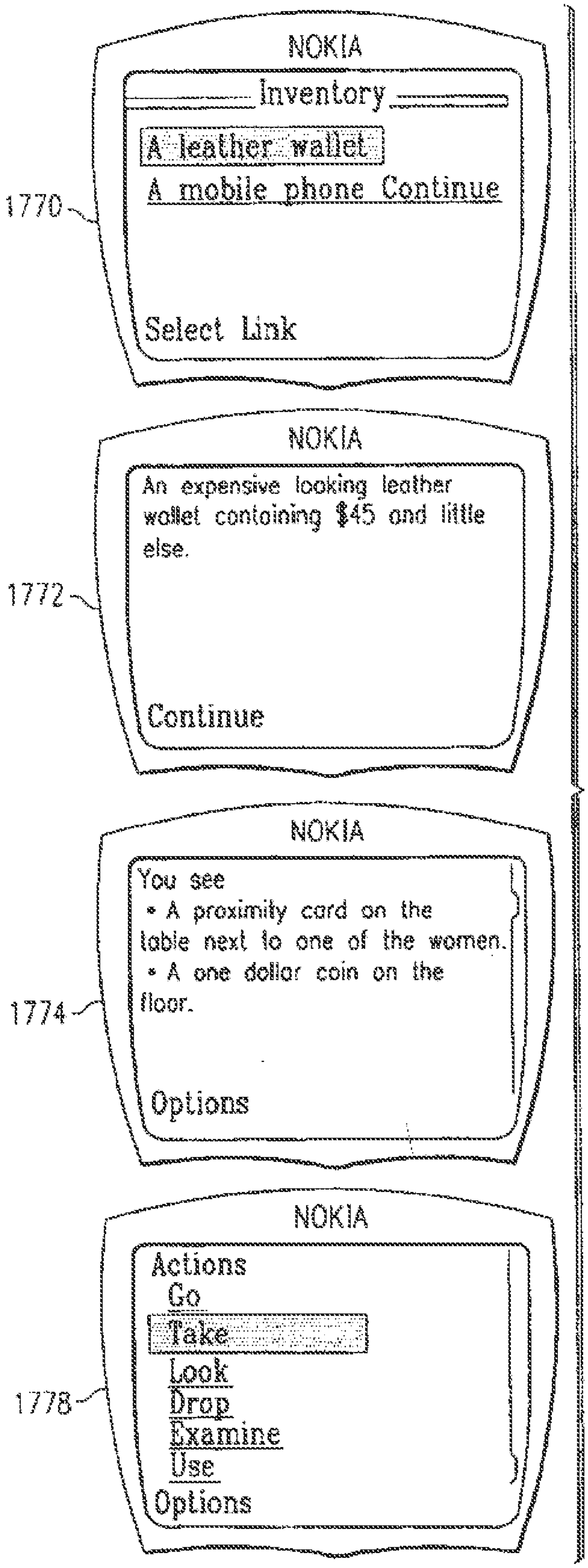

NOKIA
The shopkeeper
Actions
Go
Look
Drop
Examine
Options
1762
NOKIA
Go
out to the lane
Select Link
Back
1764
NOKIA
The lane
Actions
Go
Look
Drop
Examine
Options
1766
NOKIA
Select Link
Inventory
Save Game
Restore Game
Select
Back
1768

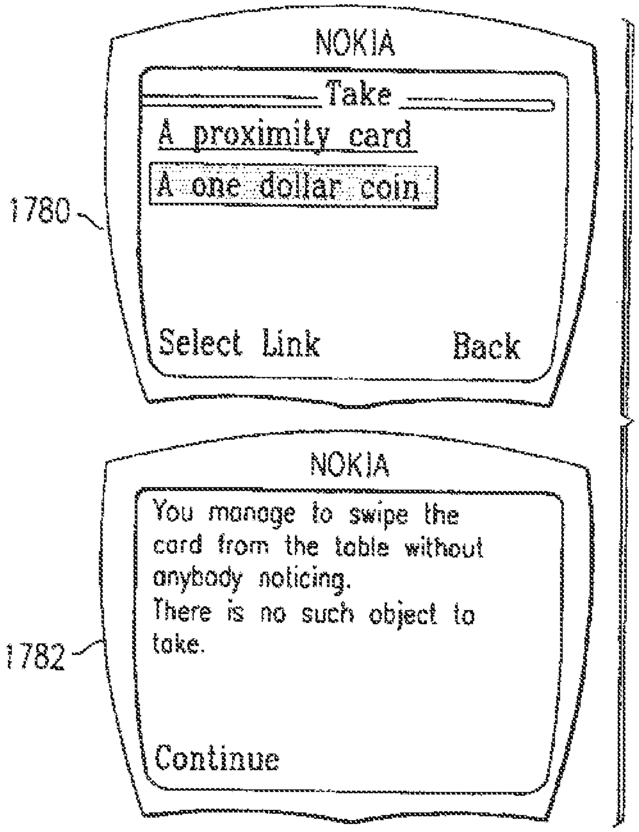
FIG. 17I



An expensive looking leather wallet containing $45 and little else.

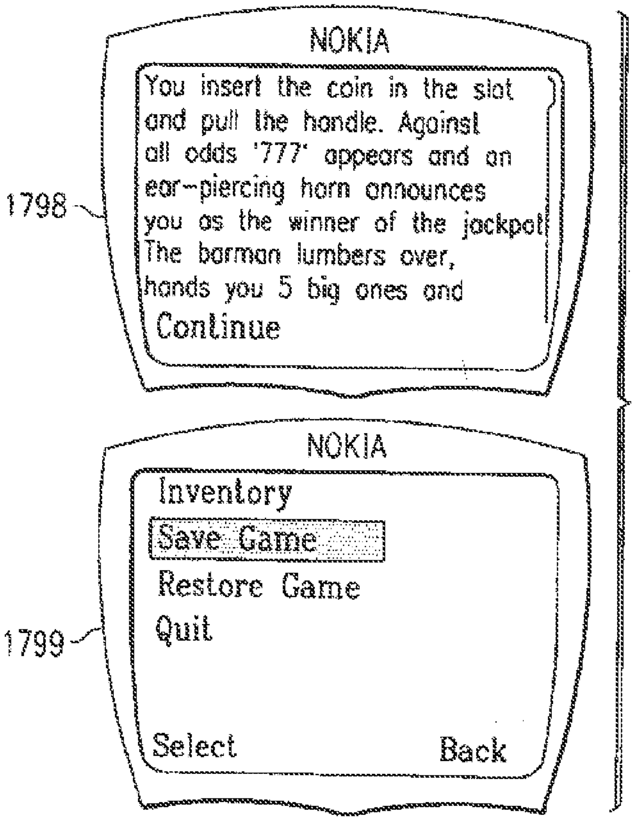
You see
• A proximity card on the table next to one of the women.
• A one dollar coin on the floor.

FIG. 17J



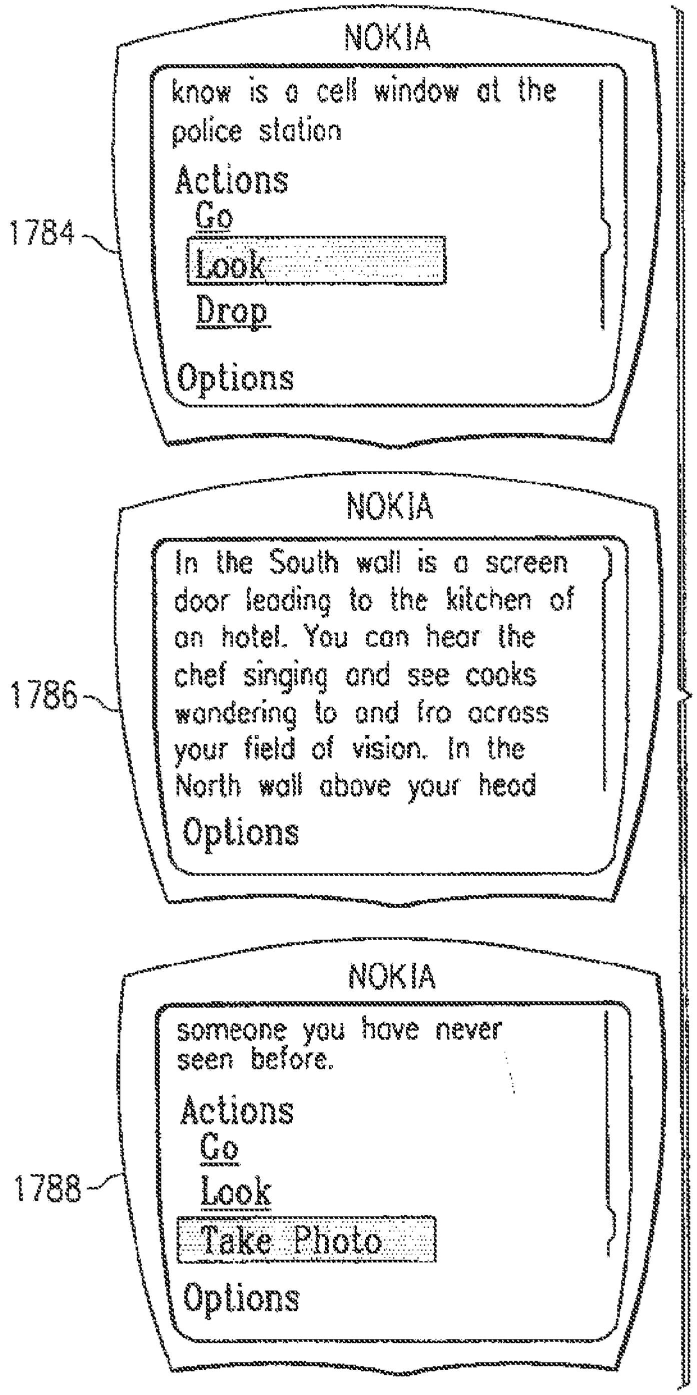
You manage to swipe the card from the table without anybody noticing.
There is no such object to take.

FIG. 17K



You insert the coin in the slot and pull the handle. Against all odds '777' appears and an ear-piercing horn announces you as the winner of the jackpot The barman lumbers over, hands you 5 big ones and

FIG. 17N

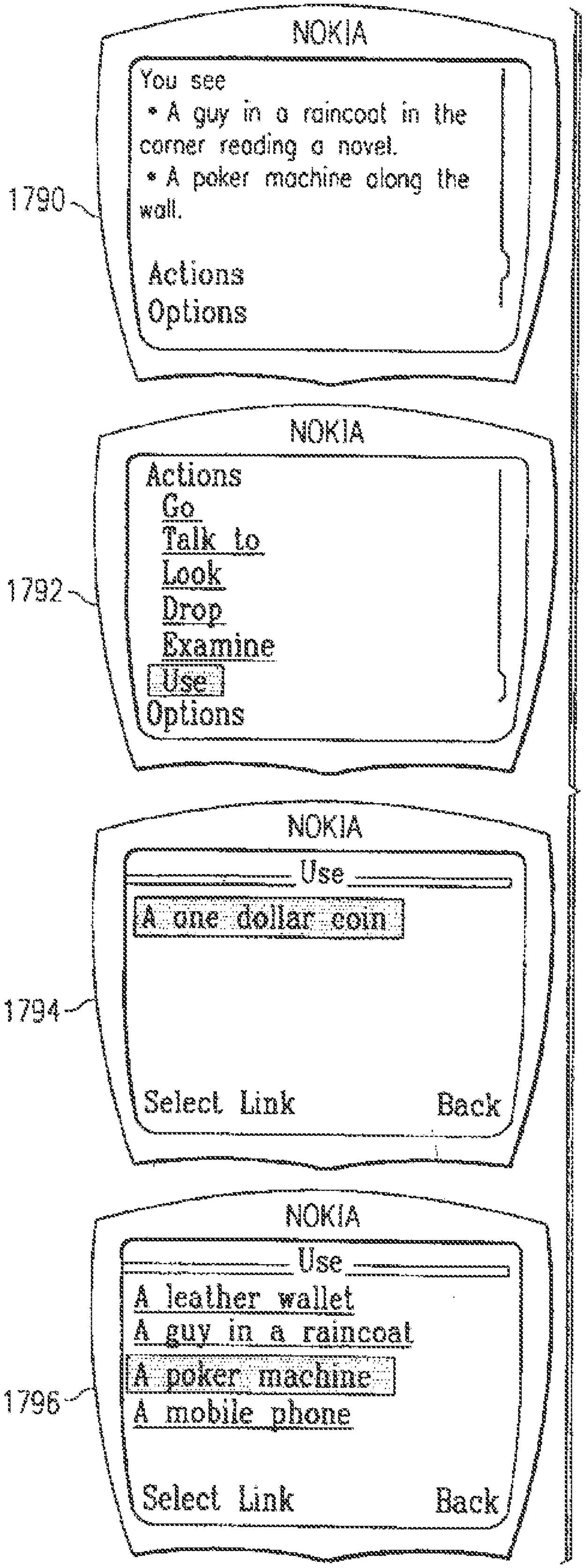


know is a cell window at the police station

In the South wall is a screen door leading to the kitchen of an hotel. You can hear the chef singing and see cooks wandering to and fro across your field of vision. In the North wall above your head

someone you have never seen before.

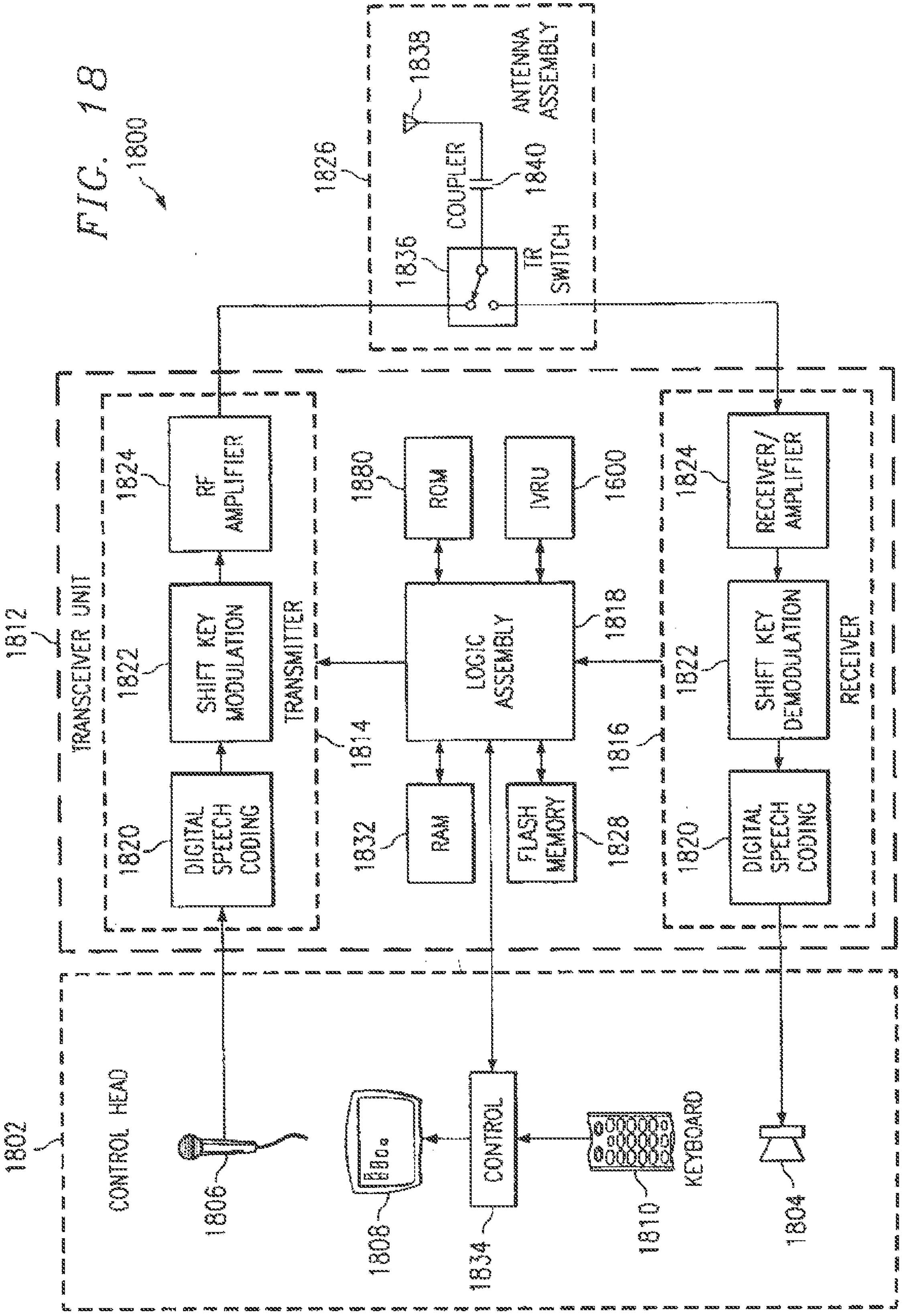
FIG. 17L



You see
- A guy in a raincoat in the corner reading a novel.
- A poker machine along the wall.

FIG. 17M

FIG. 18


1800
1826
1838
ANTENNA ASSEMBLY
COUPLER
1840
1836
TR SWITCH
1812
TRANSCEIVER UNIT
1824
RF AMPLIFIER
1822
SHIFT KEY MODULATION
1820
DIGITAL SPEECH CODING
TRANSMITTER
1814
1880
ROM
IVRU
1600
LOGIC ASSEMBLY
1818
1832
RAM
FLASH MEMORY
1828
1824
RECEIVER/ AMPLIFIER
1822
SHIFT KEY DEMODULATION
RECEIVER
1816
1820
DIGITAL SPEECH CODING
1802
CONTROL HEAD
1806
1808
CONTROL
1834
1810
KEYBOARD
1804

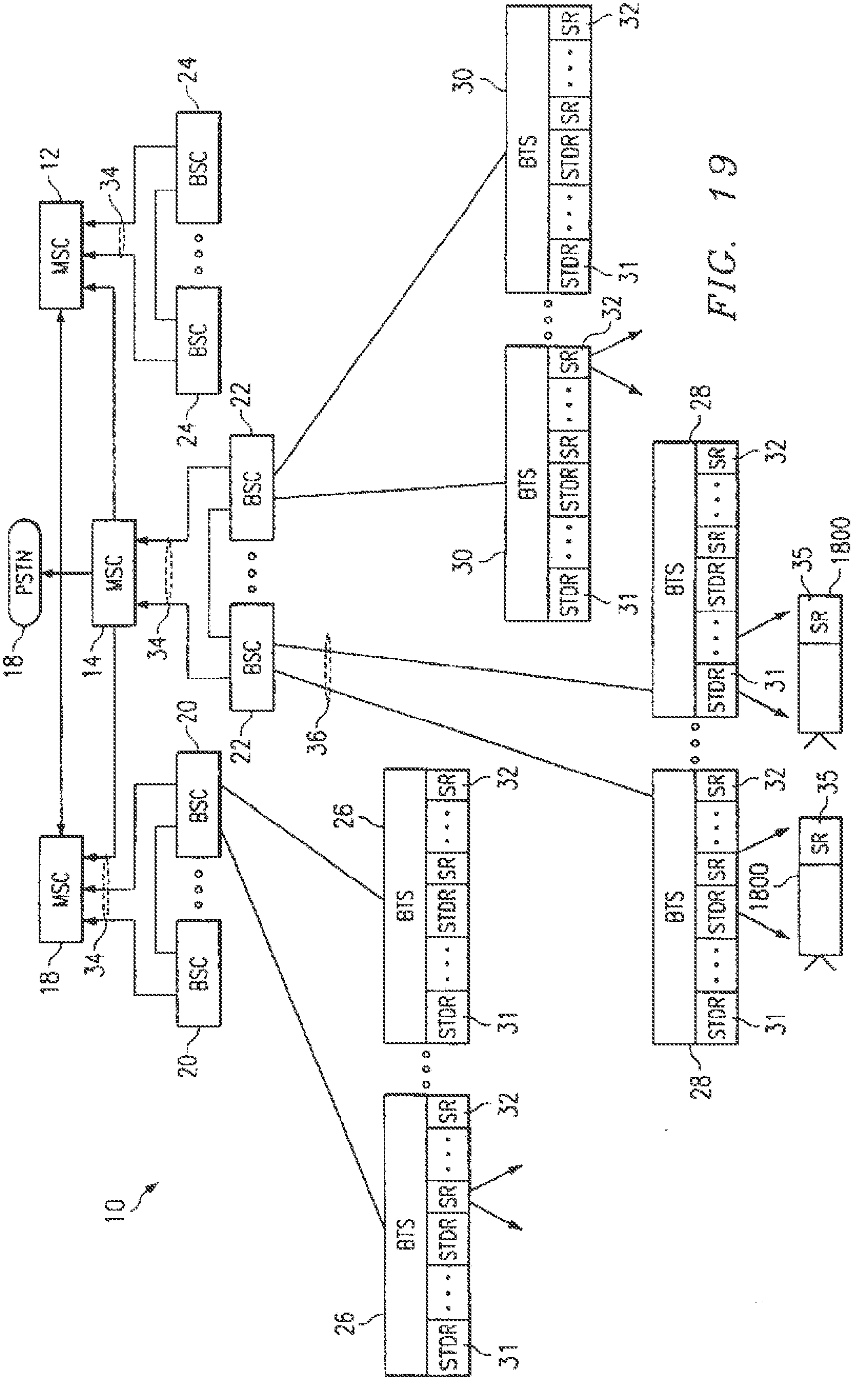

10
12
MSC
14
MSC
18
PSTN
18
MSC
34
34
34
20
BSC
BSC
22
BSC
BSC
24
BSC
BSC
26
BTS
STDR
SR
31
32
28
BTS
STDR
SR
30
BTS
STDR
SR
35
SR
1800
36

FIG. 19

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 66 0160

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 738 583 A (COMAS NELSON R ET AL) 14 April 1998 (1998-04-14) * the whole document *	1,2,5, 12,14, 16, 19-27, 31-35	G06F19/00 H04L29/06 A63F13/12 //G06F161:00
X	US 5 809 415 A (ROSSMANN ALAIN) 15 September 1998 (1998-09-15) * column 3, line 25 - column 6, line 65 * * column 19, line 20 - line 56 * * column 21, line 3 - column 23, line 34 *	1,32	
A	MACEDONIA M R: "A TAXONOMY FOR NETWORKED VIRTUAL ENVIRONMENTS" IEEE MULTIMEDIA,US,IEEE COMPUTER SOCIETY, vol. 4, no. 1, January 1997 (1997-01), pages 48-56, XP000669955 ISSN: 1070-986X * the whole document *	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L
G06F
A63F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 December 2000	Gerling, J.C.J.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 56 0160

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-12-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5738583 A	14-04-1998	NONE	
US 5809415 A	15-09-1998	EP 0779759 A	18-06-1997
		JP 10011383 A	16-01-1998
		US 6119155 A	12-09-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82176 A1

(51) International Patent Classification⁷: G06F 17/60

(21) International Application Number: PCT/US01/12715

(22) International Filing Date: 19 April 2001 (19.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/552,887 20 April 2000 (20.04.2000) US

(71) Applicant: GAMING SYSTEM TECHNOLOGIES, LLC [US/US]; 302 East Carson Avenue, Suite 1102, Las Vegas, NV 89101 (US).

(72) Inventor: KOWALICK, Gregory; 872 Hillbrook Lane, Langhorne, PA 19047 (US).

(74) Agent: GREENE, Gary, A.; Caesar, Rivise, Bernstein, Cohen & Pokotilow, Ltd., 12th Floor, Seven Penn Center, 1635 Market Street, Philadelphia, PA 19103-2212 (US).

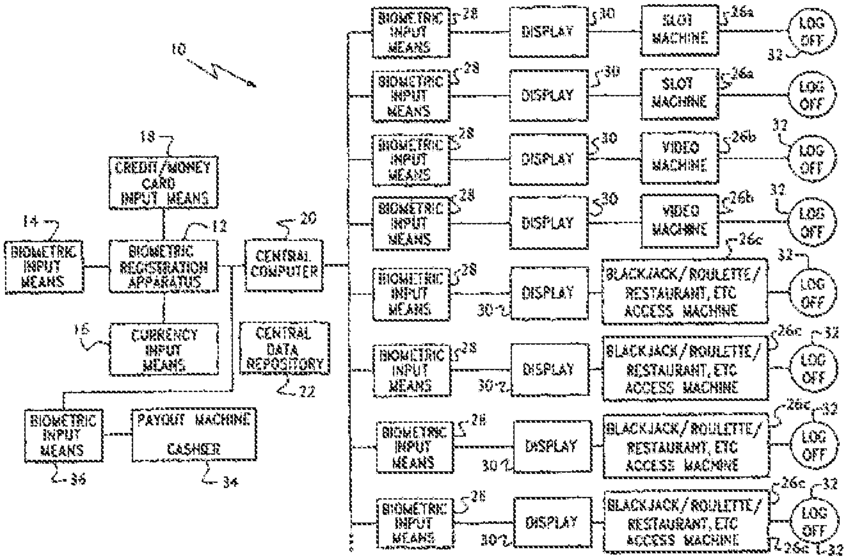
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: BIOMETRIC GAMING ACCESS SYSTEM



(57) Abstract: A method for cashless and tokenless access to casino machines is provided including the steps of providing a biometric registration apparatus connected to a computer having an input for a user to input a biometric sample (14) and a payment input (18). "The player registers including the steps of inputting a biometric sample into the biometric input and inputting money. The money is input into a unique player's account in the central computer (20) associated with the biometric sample of the player. The player is identified at a gaming machine (26) by the entering of a biometric sample and comparing it to the unique biometric data stored in the central computer. The player is then authorized to play and his account is updated to debit or credit the player's wins and losses. The player is then paid any money remaining in his account after the player no longer desires to play by entering a biometric sample to access his account.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82176 A1

(51) International Patent Classification⁷: G06F 17/60

(21) International Application Number: PCT/US01/12715

(22) International Filing Date: 19 April 2001 (19.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/552,887 20 April 2000 (20.04.2000) US

(71) Applicant: GAMING SYSTEM TECHNOLOGIES, LLC [US/US]; 302 East Carson Avenue, Suite 1102, Las Vegas, NV 89101 (US).

(72) Inventor: KOWALICK, Gregory; 872 Hillbrook Lane, Langhorne, PA 19047 (US).

(74) Agent: GREENE, Gary, A.; Caesar, Rivise, Bernstein, Cohen & Pokotilow, Ltd., 12th Floor, Seven Penn Center, 1635 Market Street, Philadelphia, PA 19103-2212 (US).

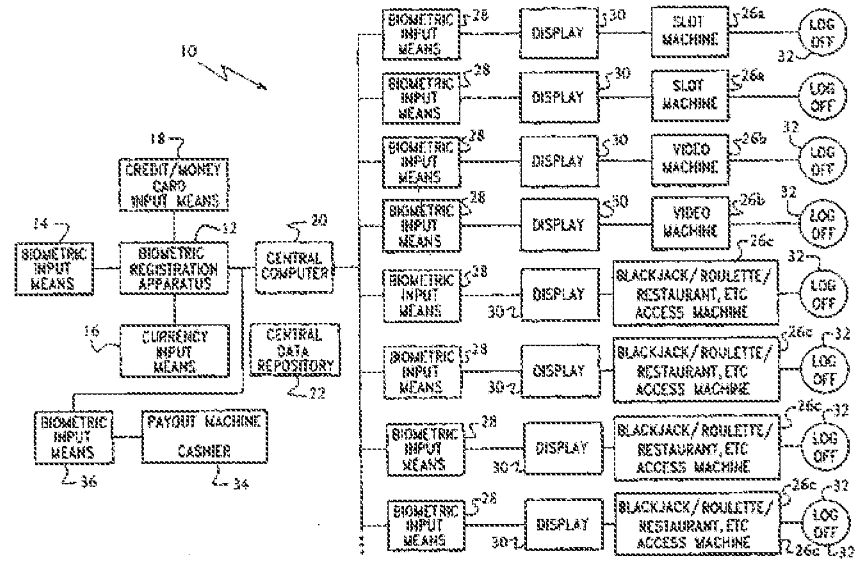
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: BIOMETRIC GAMING ACCESS SYSTEM



(57) Abstract: A method for cashless and tokenless access to casino machines is provided including the steps of providing a biometric registration apparatus connected to a computer having an input for a user to input a biometric sample (14) and a payment input (18). "The player registers including the steps of inputting a biometric sample into the biometric input and inputting money. The money is input into a unique player's account in the central computer (20) associated with the biometric sample of the player. The player is identified at a gaming machine (26) by the entering of a biometric sample and comparing it to the unique biometric data stored in the central computer. The player is then authorized to play and his account is credited or debited based on the player's wins and losses. The player is then paid any money remaining in his account after the player no longer desires to play by entering a biometric sample to access his account.

WO 01/82176 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Biometric Gaming Access System

SPECIFICATION

BACKGROUND OF THE INVENTION

This invention relates generally to casino gaming and, more particularly, to an improved system for operating cashless and tokenless gaming apparatus using an account accessed solely by a biometric sample.

Various means to use biometric samples are known, including use of fingerprints, hand prints, voice prints, retinal images, handwriting samples, and the like. Presently, most biometric data are stored on a token in electronic form, such as on a smart card or the like. Thus, the biometric data for a particular individual can be fraudulently copied and reproduced, for example, if a card is lost or stolen.

A tokenless biometric ATM access system is disclosed in U.S. Patent 5,764,789 wherein a customer registers with a computer system. Here, the customer registers a personal identification number (PIN), one or more biometric samples, and one or more financial accounts. The customer initiates account access at an ATM or other financial device by entering the customer's personal authentication information which includes a PIN and a biometric sample. The personal authentication information is compared with the registration biometric sample to produce a successful or failed identification of the customer. If there is a successful identification of the customer, the customer is allowed to access the account.

This system positively identifies a person's identity to that person's specific account or accounts. In any typical bank or other financial account where a user has access to ATM machines, essential to the transaction is the relating of numerous details concerning the particular person to a particular account where that person is known to the bank or financial institution by address, social security number, birth date, and the like. The present system is not necessarily concerned with a person's details of his identity, such as social security number and the like. The present system is concerned with relating a only a particular biometric sample to a financial account. The person need not be identified further. Thus, effectively, the account is held in the "name" of the biometric sample, rather than in the name of the person. This allows for a certain level of anonymity that numerous gaming patrons deem to be of great importance. Thus, this system may be more similar to a system that uses currency. Of course, on the other hand, if deriserd, the present system allows a gaming organization to keep detailed records of the details of specific gaming patrons and groups of gaming patrons. Obviously, if desired, an alternate embodiment of the present system would give the gaming organization the ability to tie a particular biometric sample to a particular gaming patron and track that patron's activity within the system.

Finally, U.S. Patent No. 6,012,039 (Hoffman et al.) discloses a tokenless biometric electronic rewards system where a recipient registers a biometric sample. The system authorizes reward transactions and the debiting and crediting of reward units from a reward recipient's electronic account, either at the retail point of sale or over the internet. The rewards recipient is not required to directly use any man-made personalized token in order to effect the transaction.

OBJECTS OF THE INVENTION

Accordingly, it is a general object of the present invention to provide a biometric gaming access system.

It is a further object of the present invention to provide a biometric gaming access system that provides for play at casino games without the need to carry currency or tokens during play.

It is still a further object of the present invention to provide a biometric gaming access system that utilizes a central account opened solely with a biometric sample and an amount of money, where a plurality of gaming apparatus may be played utilizing the central account with access obtained by the biometric sample.

It is still a further object of the present invention to provide a biometric gaming access system that utilizes an account accessed by a biometric sample of a fingerprint, hand print, voice print, retinal image, or the like, at a plurality of gaming apparatus.

It is still a further object of the present invention to provide a biometric gaming access system that utilizes an account accessed by a biometric sample and, optionally, a personal identification number (PIN).

It is yet another object of the present invention to provide a biometric gaming access system that utilizes an account accessed by a biometric sample at a plurality of gaming apparatus and gives account information on a display.

It is still another object of the present invention to provide a biometric gaming access system where a player does not have to be concerned with losing cash, a debit or credit card or a cash-out voucher.

It is a further object of this invention to provide a biometric gaming access system where a gaming organization can track players' use of various machines and amounts used by a particular player.

It is a still further object of the present invention to provide a biometric gaming access system that utilizes gaming apparatus that require less labor to maintain due to the apparatus not requiring to dispense cash or tokens.

It is a still further object of the present invention to provide a biometric gaming access system that reduces fraud.

It is a still further object of the present invention to provide a biometric gaming access system that does not require a token to be used that can be lost.

It is still a further object of the present invention to provide a biometric gaming access system that operates in a commercially acceptable time frame, for example, in less than five seconds.

SUMMARY OF THE INVENTION

These and other objects of this invention are achieved by providing a method for cashless and tokenless access to casino machines including the steps of providing a biometric registration apparatus connected to a computer having an input for a user to input a biometric sample and a payment input. The player registers including the steps of inputting a biometric sample into the biometric input and inputting money. The money is input into a unique player's account in the central computer associated with the biometric sample of the player. The player is identified at a gaming machine by the entering of a biometric sample and comparing it to the unique biometric data stored in the central computer. The player is then authorized to play and his account is credited or debited based on the player's wins and losses. The player is then paid any money remaining in his account after the player no longer desires to play by entering a biometric sample to access his account. The account can be kept indefinitely for future play on a gaming machine within the system.

DESCRIPTION OF THE DRAWINGS

Other objects and many attendant features of this invention will become readily appreciated as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. 1 is a schematic diagram of a biometric gaming access system in accordance with one preferred embodiment of the present invention.

FIG. 2 is a simplified front elevation view of a biometric registration apparatus for use with the biometric gaming access system of FIG. 1.

FIG. 3 is a simplified front elevation view of an alternate biometric registration apparatus for use with the biometric gaming access system of FIG. 1.

FIG. 4 is a simplified front view of a slot machine for use with the biometric gaming access system of FIG. 1.

FIG. 5 is a simplified front view of a video gaming machine having a touch screen for use with the biometric gaming access system of FIG. 1.

FIG. 6 is a schematic diagram of a biometric gaming access system in accordance with a second preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to the drawings wherein like reference numbers refer to like parts throughout the several views, there is shown in FIG. 1 a schematic diagram of a biometric gaming access system 10 in accordance with one preferred embodiment of the present invention. As can be seen in FIGS. 1 and 2, a player desiring to access various gaming apparatus, including slot machines, video machines, and the like, first registers at a biometric registration apparatus 12. There, the player provides an appropriate biometric to a biometric input means 14. For example, the biometric input means 14 could be based on one or more fingerprint, hand print, voice print, retinal image, or the like. Once the biometric registration apparatus 12 acknowledges acceptance of the biometric sample, a player then "cashes in" to the biometric registration apparatus 12 by providing a desired amount of currency to a currency input means 16 such as a bill validator as known in the art, or by providing a credit card, debit card, or other money access card to a card input means 18 as are known in the art. If the card input means 18 is used, the player authorizes an appropriate dollar amount, for example 50 or 100 dollars on an input device 13 (see FIG. 2) on the biometric registration apparatus 12. Based on this information, the biometric registration apparatus 12 creates a unique player's account where account information is stored on a central computer 20 connected to the biometric registration apparatus 12. The computer 20 has a central data repository 22 containing unique players' accounts for all players on the system. This computer 20 may be a personal computer, main frame computer, or any other computer that meets the requirements of the present invention. The biometric registration apparatus 12 may optionally provide a paper receipt via a receipt slot 19 and/or provide a display 24 indicating the unique player's account information (see FIG. 2).

FIG. 2 depicts a simplified biometric registration apparatus 12 which includes a biometric input means 14, a currency input means 16 in the form of a bill validator, a card reader 18, a display 24 and keypad 38 on an input device 13, and a receipt slot 19. FIG. 3 depicts a simplified biometric registration apparatus 12' that only has a biometric input means 14', a bill validator 16' and a receipt slot 19'.

It must be noted here that the registration process only requires input of a biometric and input of money in some form. No personal data beyond the biometric is required, thereby providing at least some level of anonymity to the player. However, optionally, additional personal information can be requested or required. A gaming organization may desire to collect information concerning its patrons. Obtaining this information by a biometric as indicated above can be accomplished quickly and nonintrusively.

Once a player has successfully registered onto the system by providing the biometric sample and money, the player then may proceed to any slot machine 26a, video machine 26b, or other access machine 26c in the system and begin play. When the player selects the desired machine that is equipped with the required apparatus as described herein, he provides the appropriate biometric to a biometric input means 28 for which the machine is capable of reading, for example, a fingerprint. See, for example, FIG. 4 which depicts a slot machine 26s, a thumbprint scanner as biometric input means 28s, a display 30s, a logoff button 32s and a receipt slot 19s. Likewise, see, for example, FIG. 5 which depicts a video gaming machine 26v, a thumbprint scanner as biometric input means 28v, a display 30v which is incorporated in the gaming machine's touch screen, a logoff button 32v, and a receipt slot 19v. The desired machine will then communicate back to the central computer 20 to obtain account information based on that biometric sample. Preferably, a display 30 on the machine will then indicate the account balance. Additional information may be provided on the display if that information is available. For example, the display, may indicate "Good Morning Mr. Smith. You have $255.00 in your account." The player then begins play, with his account balance increasing or decreasing according to the players wins and losses.

Once the player decides to cease playing on the particular machine, that player logs off the machine by pressing a logoff means 32 such as a button, or, if the machine has a proximity sensor logoff as described below, the machine would log off automatically when the player leaves. The player could then move to another slot machine 26a, video machine 26b or other access machine 26c on the system, provide the appropriate biometric sample, and again begin play. Once a player is finished all play and desires to "cash out," the player then proceeds to a payout machine or a cashier 34 (or he may cash out a specific machine as described below). There, again, the player provides the appropriate biometric sample to a biometric input means 36, and receives the balance of the money in his unique player's account. Typically, the player would only be required to register once, so long as a balance remains in the player's unique player's account.

Additionally, a biometric registration apparatus 12, including associated biometric input means 14, and card input means 18 and/or currency input means can be incorporated into all or a plurality of gaming machines 26a, 26b, 26c, etc. This could eliminate a need for a separate biometric registration apparatus kiosk. For example a gaming patron could enter a casino, insert money and a thumbprint to a slot machine to create an account. That player could play that machine, then logoff and move to another machine and log on by applying his thumbprint to the new machine. As long as the player's account does not drop to zero, he can continue moving from machine to machine in this manner. Additionally, one or

Ideally, most or all of the major manufacturers of gaming machines would manufacture machines that utilize the present system and all would be connected back to the central computer, within a particular system. A player is able to move from gaming machine to gaming machine by merely providing the appropriate biometric sample, without having to use debit cards or cash-out slips, or the like. When a player moves from one machine to another, his account would automatically be credited or debited through the central computer 20. Therefore, a player can freely move from machine to machine keeping a single account. As indicated above, once a player is finished play on a particular gaming machine, that player would log off the machine to prevent another from playing on his account. Here, numerous means to reduce fraud may be utilized. For example, the system may be set up to allow for only one player to play on a single account such that if that player moves to a second machine without logging off, the first machine would automatically log off. In any event, since the unique player's account may only be accessed by one player, only that player could ultimately collect any account balance since the biometric sample is required to be presented for payment. Another possible way to reduce fraud associated with the present system would be to include a proximity sensor for logging off, as known, for example for plumbing in some public restrooms, that automatically logs a user or player off the machine when that user walks away from that machine.

The system may also be used for other related monetary transactions. For example, a biometric input means with associated access machine might be placed at kiosks in various other locations around a casino or hotel. Such an apparatus might be placed at a restaurant such that a player can deduct a dinner bill from his balance. Likewise, in any other facility within the hotel that requires payment of money, including spas, fitness clubs, cocktail lounges, shops, sports facilities, theaters, and the like, may use the biometric gaming access system 10 of the present invention. Special generic biometric gaming access machines can be provided that allow such transactions or gaming play (for example blackjack or roulette) from a unique user's account. Here, the user would register at the biometric registration apparatus and then register at the generic biometric access machine. The dealer or other person then would credit or debit the account accordingly.

Additionally, the system may be used on a more widespread network. For example, the central computer may extend to other hotels or casinos within a particular area, or even nationally or internationally. The system could likewise extend beyond the gaming industry where the private account and security of the present system is desired, but the privacy associated with this system, which, as indicated above, only requires a biometric to open an account and not necessarily a name, address, social security number, or the like. No further information is required.

Another possible application is for use of the present system by a movie or other type of theater. Here, a player could register in the same manner as described above with respect to gaming. A player would provide the appropriate biometric any time he wished to enter the movie theater. His unique account would be adjusted accordingly. Of course, this application could be applied to substantially any retail establishment.

An obvious benefit to the present system is that players would not be required to carry around large amounts of money or credit/debit cards after the initial buy-in, particularly coins, that might be heavy and burdensome. Gaming facilities around pools or beaches would greatly benefit.

If the gaming organization or other organization using this device desires to use the device to track usage, the gaming organization could provide additional benefits to the player based on that player's known usage. For example, a player might receive bonus play for playing the gaming machines for a particular period of time. Additionally, usage tracking may be used to determine which machines are more popular with certain demographic groups, by requesting that additional identifiers be supplied during the registration process. Promotional activities could also be better targeted based on information obtained.

Another advantage of the present system is that, ultimately, the machines require less labor to service since, if no actual money was inserted or dispensed, there would be fewer moving parts, no coin bins to empty or fill, and the like.

As indicated above, use of the present invention would also substantially decrease fraud since accounts are kept, transactions are recorded, and there are no credit cards, vouchers, or other tokens that are used after registration that may be stolen. It is unlikely that a player would attempt to use another's credit card during the registration process, since a biometric such as a fingerprint must be provided.

The gaming organization would benefit because the amount of play per machine, per hour, will likely increase because the player is buying in only once and does not have to buy in at each machine they play. Additionally, the gaming machines would not have down time caused by the requirement to fill and refill hoppers.

Finally , another unique application of the present invention is that, based on the player tracking information obtained, other unique games may be devised. For example, a feature that may be added to the gaming device is an instant winner game. In this example, the central computer of the present invention may be programmed to randomly select a biometric registered in its system within the last hour, day, week, or the like. When a player registers and moves from machine to machine, if the biometric matches the biometric that the central computer has randomly selected, that player becomes an instant winner of a prize.

Without further elaboration, the foregoing will so fully illustrate our invention that others may, by applying current or future knowledge, readily adopt the same for use under various conditions of service.

CLAIMS

1. A method for cashless and tokenless access to a plurality of casino gaming apparatus, said method comprising the steps of:

(a) providing a biometric registration apparatus having at least one registration biometric input means for a user to input a biometric sample, said biometric registration apparatus having at least one payment input means, said biometric registration apparatus connected to a central computer having a central data repository;

(b) providing the plurality of gaming apparatus, each gaming apparatus connected to said central computer, each gaming apparatus having at least one gaming apparatus biometric input means and a player logoff means;

(c) registering a player comprising the steps of inputting at least one biometric sample of the player into the registration biometric input means, storing unique biometric data created by the biometric input means in the central data repository, inputting into the payment input means an amount of money, and storing the amount of money input in a unique player's account in the central computer associated with the at least one biometric sample of the player;

(d) identifying said player at one of said plurality of gaming apparatus by said player entering a gaming apparatus biometric sample input into said one of said plurality of gaming apparatus biometric input means and comparing it to said unique biometric data stored in said central data repository;

(e) authorizing said player at said one of said plurality of gaming apparatus to play on said one of said plurality of gaming apparatus;

(f) debiting and or crediting said unique player's account based on the player's wins and losses at the gaming apparatus until said player logs off using said player logoff means or until said player's account is exhausted; and

(g) paying said player any money remaining in said player's account after said player no longer desires to play;

whereby a player can move to another of the plurality of gaming apparatus, input a biometric sample into one of the at least one gaming apparatus biometric input means, play the gaming apparatus for a period of time, and log off the gaming apparatus, said unique player's account being credited and debited for wins and losses on the gaming apparatus .

2. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, wherein the step of providing the plurality of gaming apparatus with the player logoff means includes providing a player logoff proximity sensor.

3. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, wherein the step of providing the plurality of gaming apparatus with the player logoff means includes providing a player logoff button.

4. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step of paying said player money remaining in said player's account includes providing a payout machine having a payout biometric input means.

5. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 4, where the step of providing the payout machine includes providing a payout machine that is integral to at least one of said casino gaming apparatus.

6. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the steps including providing the registration biometric input means and the gaming apparatus biometric input means that utilize fingerprints, hand prints, retina scans, or voice prints.

7. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step including providing the payment input means

includes providing a payment input means that accepts credit cards, debit cards, or money access cards.

8. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step including providing the payment input means includes providing a payment input means that accepts currency.

9. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step of providing the plurality of gaming apparatus includes providing slot machines and video gaming machines.

10. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step of providing the plurality of gaming apparatus includes providing generic access machines.

11. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, further including the step of collecting player data related to players' use of said plurality of casino gaming apparatus to the central computer having the central data repository.

12. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 11, where the player data collected includes data concerning type of casino gaming apparatus, quantity of casino gaming apparatus played, time spent on each casino gaming apparatus, and money spent on each casino gaming apparatus.

13. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to Claim 1, including the step of purging the unique biometric data and the unique player's account from the central computer after the step of paying said player any money remaining in said player's account, to provide for privacy of the player.

14. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, including the step of providing a keypad on the biometric registration apparatus for using a PIN and wherein the step of registering a player includes entering a PIN.

15. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, wherein the step of providing the plurality of gaming apparatus includes providing gaming apparatus having a video screen for displaying information related to the player's unique player's account.

16. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 1, where the step of providing a biometric registration apparatus includes providing a biometric registration apparatus connected to an account at a financial institution network.

17. A method for cashless and tokenless access to a financial account, said method comprising the steps of:

(a) providing a biometric registration apparatus having at least one registration biometric input means for a user to input a biometric sample, said biometric registration apparatus having at least one payment input means, said biometric registration apparatus connected to a central computer having a central data repository;

(b) providing a plurality of kiosks, each kiosk connected to said central computer, each kiosk having at least one kiosk biometric input means;

(c) registering a user comprising the steps of inputting at least one biometric sample of the user into the registration biometric input means, storing unique biometric data created by the biometric input means in the central data repository, inputting into the payment input means an amount of money, and storing the amount of money input in a unique user's account in the central computer associated solely with the at least one biometric sample of the user;

(d) identifying said user at one of said plurality of kiosks by said user entering a kiosk biometric sample input into said one of said plurality of kiosk biometric input means and comparing it to said unique biometric data stored in said central data repository;

(e) authorizing said user at said one of said plurality of kiosks to access said unique user's account for a transaction;

(f) debiting and or crediting said unique player's account based on the transaction; and

(g) paying said user any money remaining in said user's account, when said user desires to cancel said unique user's account.

18. A method for cashless and tokenless access to a financial account according to claim 17, where the steps including providing the registration biometric input means and the kiosk biometric input means that utilize fingerprints, hand prints, retina scans, or voice prints.

19. A method for cashless and tokenless access to a financial account according to claim 17, where the step including providing the payment input means includes providing a payment input means that accepts credit cards, debit cards, or money access cards.

20. A method for cashless and tokenless access to a financial account according to claim 17 where the step including providing the payment input means includes providing a payment input means that accepts currency.

21. A method for cashless and tokenless access to a financial account according to Claim 17, including the step of purging the unique biometric data and the unique user's account from the central computer after the step of paying said user any money remaining in said user's account, to provide for privacy of the user.

22. A method for cashless and tokenless access to a financial account according to claim 17, including the step of providing a keypad on the biometric registration apparatus for using a PIN and wherein the step of registering a user includes entering a PIN.

23. A method for cashless and tokenless access to a financial account according to claim 17, wherein the step of providing the plurality of kiosks includes providing kiosks having a video screen for displaying information related to the user's unique user's account.

24. A method for cashless and tokenless access to a plurality of casino gaming apparatus, said method comprising the steps of:

(a) providing the plurality of gaming apparatus, each gaming apparatus connected to a central computer having a central data repository, each gaming apparatus having at least one gaming apparatus biometric input means and a money input means;

(b) allowing a player to play on any of said gaming apparatus by inputting money into said money input means;

(c) after the player plays on a gaming apparatus, registering said player comprising the steps of inputting at least one biometric sample of the player into the gaming apparatus biometric input means, storing unique biometric data created by the biometric input means in the central data repository, crediting to a unique player's account in the central computer an amount of money associated with the at least one biometric sample of the player;

(c) allowing a player to play on another of said gaming apparatus by inputting money into said money input means or by accessing said unique player's account of said player by inputting said biometric sample of said player into the gaming apparatus biometric input means and comparing said biometric sample to said unique biometric data stored in said central data repository;

(e) debiting and or crediting said unique player's account based on the player's wins and losses at said another gaming apparatus until said player logs off by exhausting his account, collecting his winnings, or until said player inputs the biometric sample of said player into said gaming apparatus biometric input means; and

(f) comparing said biometric sample to said biometric data stored in said central data repository and crediting or debiting said unique player's account accordingly;

whereby a player can move to another of the plurality of gaming apparatus, input a biometric sample into one of the at least one gaming apparatus biometric input means, play the gaming apparatus for a period of time, and log off the gaming apparatus, said unique player's account being credited and debited for wins and losses on the gaming apparatus.

25. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the step of paying said player money remaining in said player's account includes providing a payout machine having a payout biometric input means.

26. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 25, where the step of providing the payout machine includes providing a payout machine that is integral to at least one of said casino gaming apparatus.

27. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the steps including providing the gaming apparatus biometric input means that utilizes fingerprints, hand prints, retina scans, or voice prints.

28. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the step including providing the payment input means includes providing a payment input means that accepts credit cards, debit cards, or money access cards.

29. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the step including providing the payment input means includes providing a payment input means that accepts currency.

30. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the step of providing the plurality of gaming apparatus includes providing slot machines and video gaming machines.

31. A method for cashless and tokenless access to a plurality of casino gaming apparatus according to claim 24, where the step of providing the plurality of gaming apparatus includes providing generic access machines.

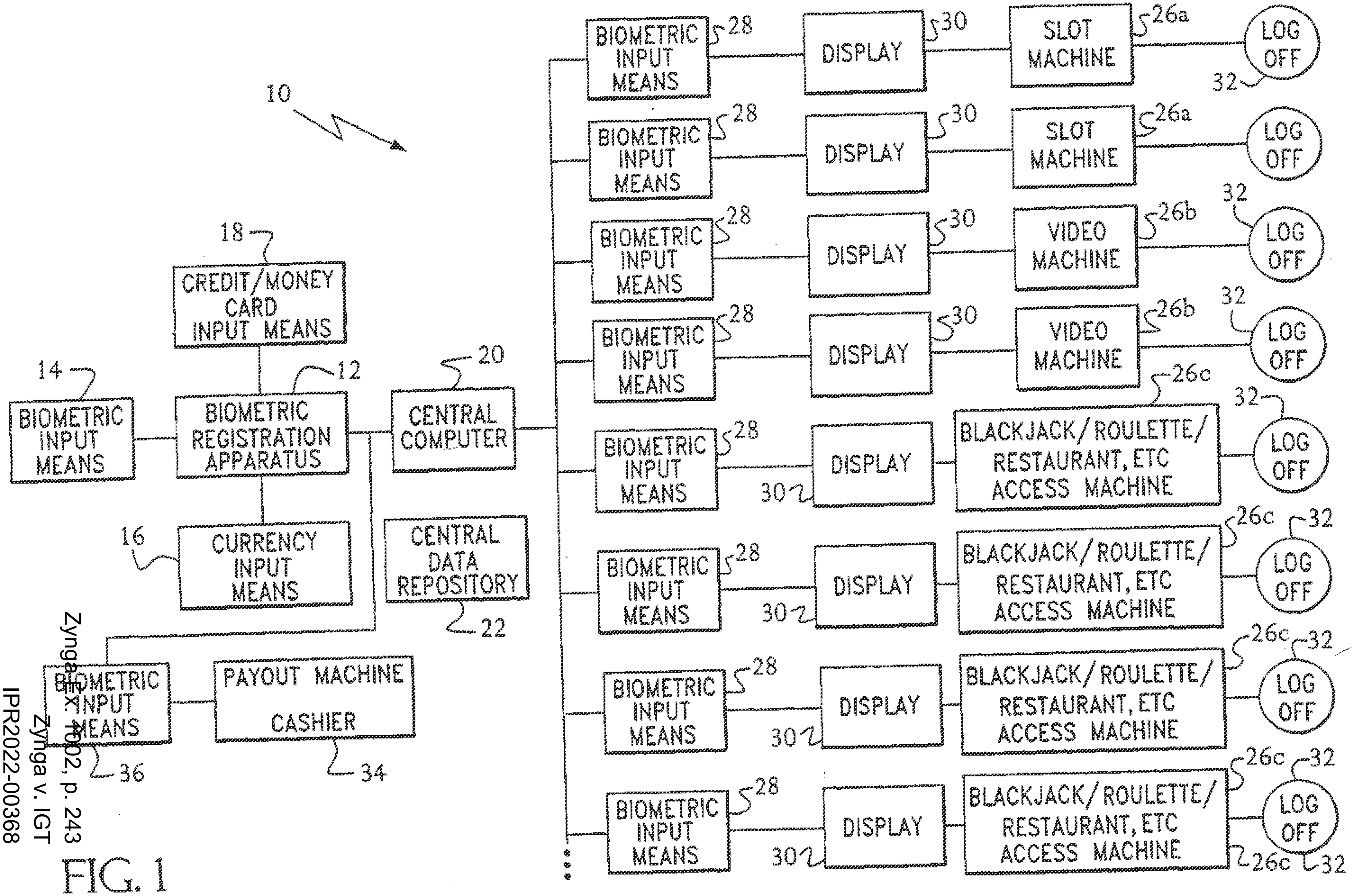

10
18
CREDIT/MONEY CARD INPUT MEANS
14
BIOMETRIC INPUT MEANS
12
BIOMETRIC REGISTRATION APPARATUS
16
CURRENCY INPUT MEANS
20
CENTRAL COMPUTER
CENTRAL DATA REPOSITORY
22
BIOMETRIC INPUT MEANS
36
PAYOUT MACHINE
CASHIER
34
BIOMETRIC INPUT MEANS
28
DISPLAY
30
SLOT MACHINE
26a
LOG OFF
32
VIDEO MACHINE
26b
BLACKJACK/ROULETTE/ RESTAURANT, ETC ACCESS MACHINE
26c

FIG. 1

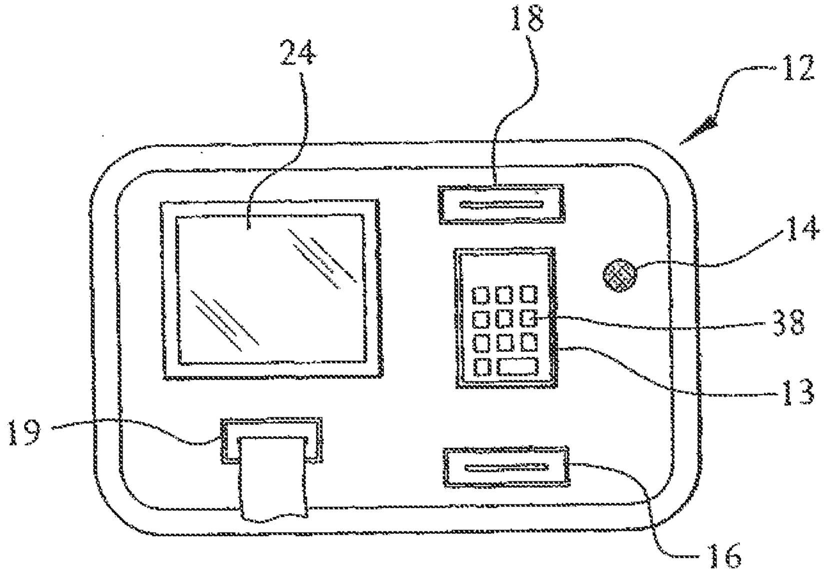


FIG. 2

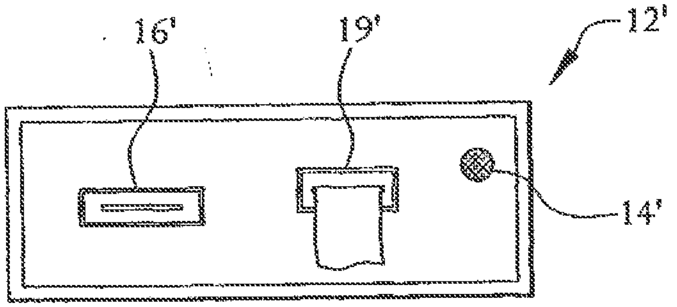


FIG. 3

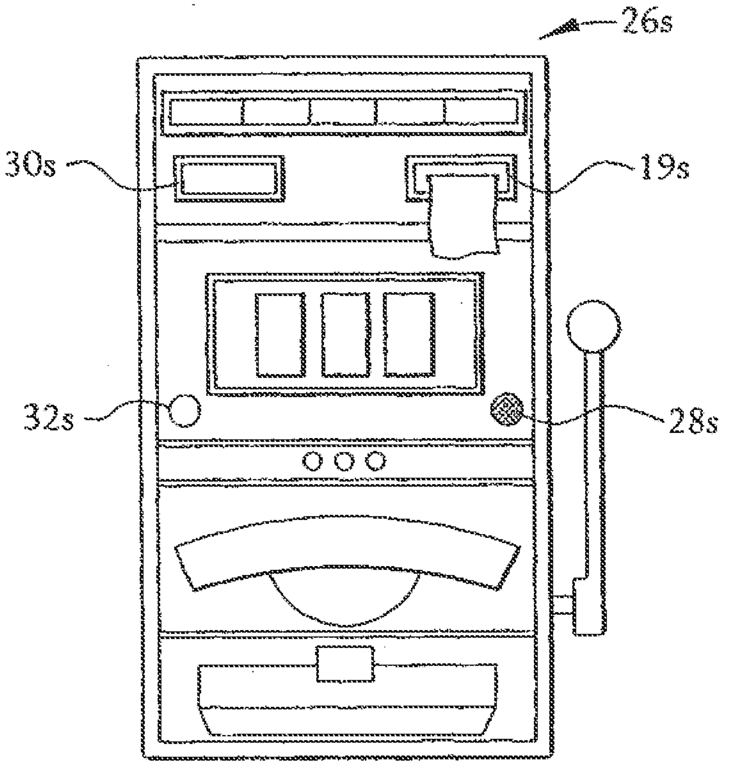


FIG. 4

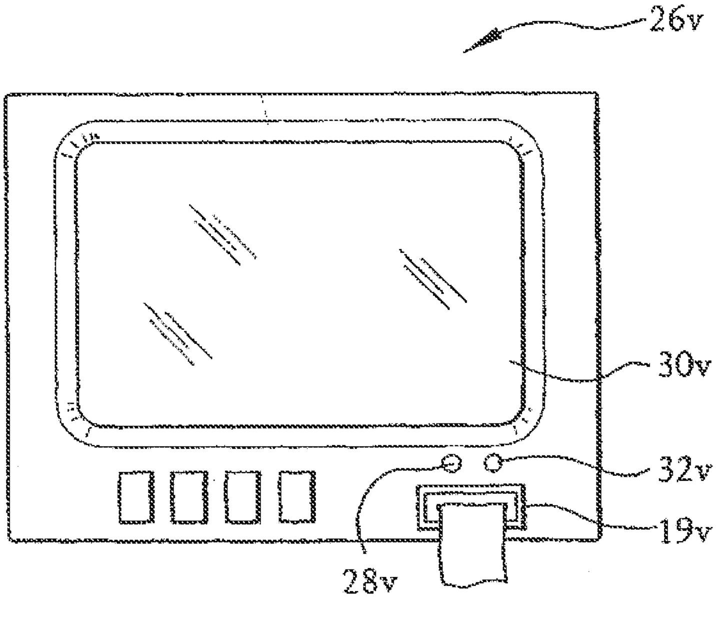


FIG. 5

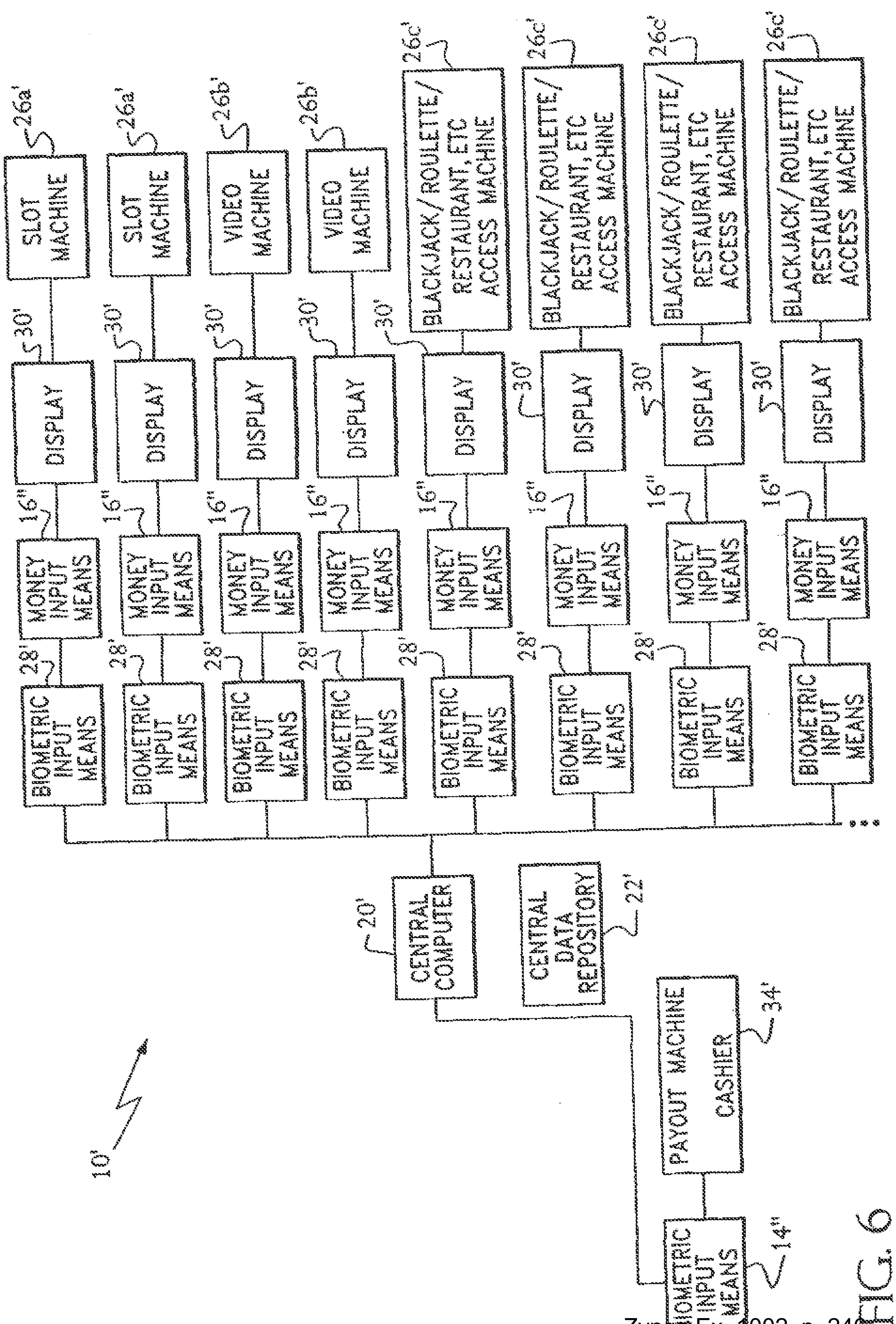

SLOT MACHINE
26a'
SLOT MACHINE
26a'
VIDEO MACHINE
26b'
VIDEO MACHINE
26b'
BLACKJACK/ROULETTE/ RESTAURANT, ETC ACCESS MACHINE
26c'
BLACKJACK/ROULETTE/ RESTAURANT, ETC ACCESS MACHINE
26c'
BLACKJACK/ROULETTE/ RESTAURANT, ETC ACCESS MACHINE
26c'
BLACKJACK/ROULETTE/ RESTAURANT, ETC ACCESS MACHINE
26c'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
DISPLAY
30'
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
MONEY INPUT MEANS
16"
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
BIOMETRIC INPUT MEANS
28'
CENTRAL COMPUTER
20'
CENTRAL DATA REPOSITORY
22'
PAYOUT MACHINE
CASHIER
34'
BIOMETRIC INPUT MEANS
14"
10'

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/12715

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 17/60
US CL. : 705/44,39,38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/44,39,38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,038,334 A (HAMID) 14 March 2000, abstract, fig. 1-3.	1-31
Y,P	US 6,016,476 A (MAES et al) 18 June 2000, abstract, fig. 1,3, col. 2, lines 23-42.	1-18
A	US 6,023,688 A (RAMACHANDRAN et al) 8 Feb 2000, abstract, fig. 1,3; col. 4, lines 60-66.	1-18

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search

21 MAY 2001

Date of mailing of the international search report

14 JUN 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

VINCENT MILLIN

Telephone No. (703) 308-1065

Form PCT/ISA/210 (second sheet) (July 1998)*

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	Thierry Brunet de Courssou
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1	0141892	WO	A2	2001-06-14	Smart Card Integrators, Inc.		□
	2	0141892	WO	A3	2001-06-14	Smart Card Integrators, Inc.		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	Thierry Brunet de Courssou
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CYBS5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Supplemental European Search Report mailed November 28, 2006, in related European Application No. 02784522.	□
	2	Supplemental European Search Report mailed November 16, 2006, in corresponding European Application No. 02780726.	□
	3	Supplemental European Search Report mailed December 4, 2006, in related European Application No. 02789831.	□
	4	European Search Report mailed November 24, 2006, in related European Application No. 02782356.6	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/41892 A2

(51) International Patent Classification⁷: A63F 13/00

(21) International Application Number: PCT/US00/42285

(22) International Filing Date: 28 November 2000 (28.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/456,021 3 December 1999 (03.12.1999) US

(71) Applicant: SMART CARD INTEGRATORS, INC. [US/US]; 1380 W. Washington Boulevard, Los Angeles, CA 90007 (US).

(72) Inventor: CHARRIN, Philippe, A.; 11356 Nebraska Avenue, Los Angeles, CA 90025 (US).

(74) Agents: VANDERLAAN, Christopher, A. et al.; Lyon & Lyon LLP, 633 West Fifth Street, Suite 4700, Los Angeles, CA 90071 (US).

(81) Designated States *(national)*: AU, BR, CA, ZA.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

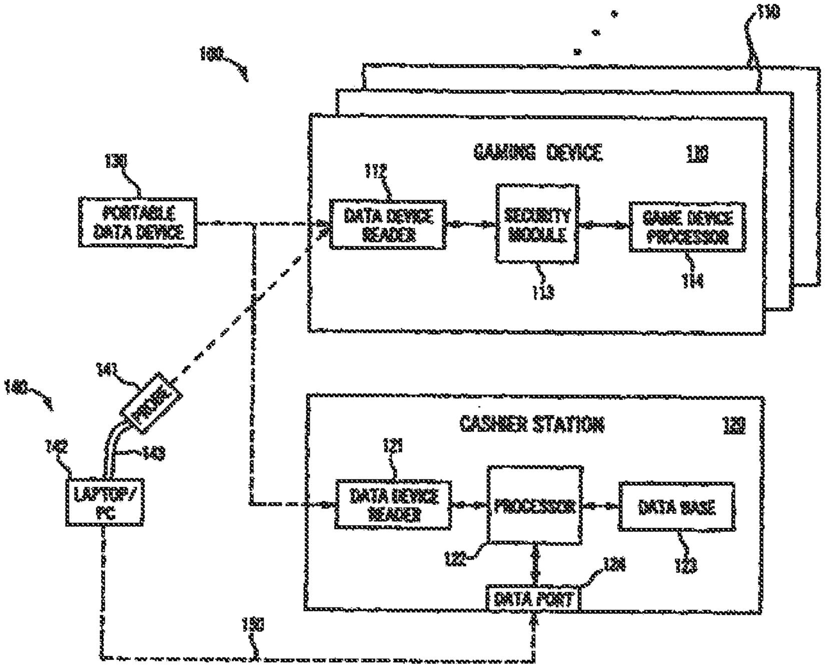
Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/41892 A2

(54) Title: METHOD AND SYSTEM FOR SECURE CASHLESS GAMING



(57) Abstract: A secure cashless gaming system comprises a plurality of gaming devices which may or may not be connected to a central host network. Each gaming device includes an intelligent data device reader which is uniquely associated with a security module interposed between the intelligent data device reader and the gaming device processor. A portable data device bearing credits is used to allow players to play the various gaming devices. When a portable data device is presented to the gaming device, it is authenticated before a gaming session is allowed to begin. The intelligent data device reader in each gaming device monitors gaming transactions and stores the results for later readout in a secure format by a portable data extraction unit, or else for transfer to a central host network. Gaming transaction data may be aggregated by the portable data extraction unit from a number of different gaming devices, and may be transferred to a central accounting and processing system for tracking the number of remaining gaming credits for each portable data unit and/or player. Individual player habits can be monitored and tracked using the aggregated data. The intelligent data device reader may be programmed to automatically transfer gaming credits from a portable data device to the gaming device, and continually refresh the credits each time they drop below a certain minimum level, thus alleviating the need for the player to manually enter an amount of gaming credits to transfer to the gaming device.

SPECIFICATION

TITLE OF THE INVENTION

METHOD AND SYSTEM FOR SECURE CASHLESS GAMING

BACKGROUND OF THE INVENTION

Field of the Invention

The field of the present invention relates to gaming devices and systems and, more particularly, to secure cashless gaming devices and systems utilizing portable data storage devices such as smartcards.

Background

Casinos and gaming establishments have traditionally relied upon coin-operated gaming devices. Such coin-operated gaming devices have a number of drawbacks or limitations. For example, they generally require customers to carry around large numbers of coins, which can be inconvenient or burdensome to customers. Also, the only type of feedback they provide to the machine owner is the raw number of coins played and paid out. Thus, coin-operated gaming devices have no way to track the type of customers using the machines. Such information, if available, could be of significant value to the casinos and gaming establishments.

To increase the convenience to customers, and to make an attempt at tracking game machine use by individual customers, casinos and gaming establishments have for a number of years sought to provide a cashless gaming system, whereby the customers do not have to play the machines using coins and hence need not carry around large quantities of coins. Some proposed systems, for example, allow customers to use gaming establishment credit cards to transfer playing credits to, and retrieve unused credits from, a particular gaming machine. A similar proposed system allows use of a player-carried device such as a magnetic-stripe card to allow customers to use coin-operated game devices by paying a lump sum in lieu of using individual coins. Such a system is described, for example, in U.S. Patent No. 4,575,622.

Yet another proposed approach is described in U.S. Patent No. 5,179,517, which discloses a system in which a credit account for a particular customer is maintained on a portable data carrier commonly known as a "smart card." A smart card is a device generally in the size and shape of a standard credit card, encapsulating solid-state memory, circuitry for allowing the memory to be read from or written to, and, in certain cards, microprocessor circuitry for performing various programmable functions. Smart cards may be equipped with an interface having electrical contacts which make a physical connection with a smart card reader, or else may be equipped with a radio frequency (RF) interface to allow a smart card reader to interact with the smart card electronic circuitry over an RF communication link. A standard (ISO) protocol has been developed within the smart card industry for communicating between smart cards and smart card readers.

Cashless gaming systems are most often deployed in an environment in which the various gaming devices are all connected to and controlled by a central computer, which serves as the host for a local area network, and such systems are referred to as "on-line" systems. While on-line gaming systems have certain advantages such as centralized control and player tracking capability, they can create a "bottleneck" at the central computer when too many transactions need to be processed due, for example, to the number of on-line gaming devices being played simultaneously. On-line gaming systems are also more expensive than so-called "off-line" gaming devices, which are not directly tied to a host computer or a network. One probable reason that most cashless gaming systems have been developed for on-line (rather than off-line) gaming devices is because of the ability of the central computer to account for changes to the player's account and the machine's payment in/payment out during play, by instantly adjusting accounting data relating to the player and/or the gaming device which is being played. Accurate centralized accounting is highly important, because when machines can be played with coins or with credit (via a cashless technique), the number of coins in and out will not necessarily reflect the total intake or payout of a gaming device. Rather, the influx of cashless "credits" in a gaming device would, in the absence of careful monitoring, cause a discrepancy in the accounting for each gaming device. In an on-line gaming system, each bet and each pay-out is typically run through the central computer, which is thereby able to keep a running account of the monetary balance at each gaming device.

On the other hand, such a capability does not exist with off-line gaming devices, since they are not connected to a central computer. Accounting for off-line machines is usually conducted by manually checking various meters at the gaming device. When the number of off-line machines is large, meter checking can be a long and tedious process. It can also be inconvenient to the casinos or gaming establishments, as it requires that the gaming devices be taken off line for a certain period of time during meter checking activity.

While cashless gaming techniques have been proposed for off-line gaming devices, such techniques are inadequate from a security and accounting standpoint. A major potential security problem is the possibility of theft of cashless data unit (e.g., smart card) readers, particularly by employees of the casinos or gaming establishments. In this regard, it may be noted that a high percentage of casino theft is estimated to be caused by internal company employees. With a stolen data unit reader, an individual can illegally add money in the form of credits to one or more cashless data units. The individual could then "cash out" the amount of credit on the cashless data units, without the casino or gaming establishment being aware that the money was illegally added to the cashless data units. The possibility of such covert action puts casinos and gaming establishments at untoward risk of being bilked of large amounts of money. This possibility is generally not present in an on-line system, which requires all transactions to be processed through the central computer.

Another drawback of conventional off-line gaming devices is that they are generally incapable of providing the same level of accounting and targeted player feedback as on-line gaming systems. With conventional techniques, there is no practical and viable way for casinos and gaming establishments issuing portable data units (such as smart cards) to determine their outstanding liability on a given portable data unit. Also, there is no practical and viable way to obtain accurate, timely and comprehensive information as to the playing habits of individual players, which, as noted, could be of significant value to casinos and gaming establishments.

There is a need for a cashless gaming system particularly well suited for off-line gaming devices. There is further a need for a cashless gaming system which provides increased security for off-line gaming devices. There is further a need for such a cashless gaming system which allows rapid and convenient accounting for off-line gaming devices, and which allows information to be gathered concerning the playing habits of individual players. There is also a need for a cashless gaming system that reduces the probability of bottlenecks occurring at the central computer in an on-line gaming system, and further for such a system which can provide an increased level of security for on-line gaming devices.

SUMMARY OF THE INVENTION

The invention provides in one aspect systems, methods and techniques for secure cashless gaming which can be used with off-line or on-line gaming devices. In one or more embodiments, gaming credits are stored on portable data devices such as smart cards, which can be presented to gaming devices in a cashless gaming environment to allow players to use the gaming devices.

In one embodiment, a secure cashless gaming system comprises a plurality of gaming devices which may or may not be connected to a central host network. Each gaming device preferably includes an intelligent data device reader which is uniquely associated with a security module interposed between the intelligent data device reader and the gaming device processor. A portable data device (such as a smart card) bearing credits is used to allow players to play the various gaming devices. When a portable data device is presented to the gaming device, it is authenticated before a gaming session is allowed to begin. The intelligent data device reader in each gaming device monitors gaming transactions and preferably stores the results for later readout in a secure format by a portable data extraction unit, or else for transfer to a central host network. Gaming transaction data may be aggregated by the portable data extraction unit from a number of different gaming devices, and may be transferred to a central accounting and processing system for tracking the number of remaining gaming credits for each portable data unit and/or player. Individual player habits can be monitored and tracked using the aggregated data.

In another embodiment, a gaming device includes an intelligent data device reader which is uniquely associated with a security module interposed between the intelligent data device reader and the gaming device processor. Each time an attempt is made to initiate a gaming session (by, e.g., presenting a portable data device such as a smart card), and periodically thereafter, if desired, an authentication process is performed to ensure that the correct intelligent data device reader and the correct security module are present. If one or the other is missing, then the player will be unable to utilize the gaming device, and the portable data device will not be updated.

The intelligent data device reader may, in certain embodiments, be programmed to automatically transfer gaming credits from a portable data device inserted in the intelligent data device reader to the gaming device. Each time the number of credits falls below a predetermined minimum level, the intelligent data device reader may be programmed to transfer a given number of additional gaming credits to the gaming device, thus alleviating the need for the player to manually enter an amount of gaming credits to transfer to the gaming device.

Further embodiments, variations and enhancements of the invention are also described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a secure cashless gaming system in accordance with a preferred embodiment as described herein.

Fig. 2 is a block diagram of an intelligent data device reader as may be used in the secure cashless gaming system shown in Fig. 1.

Fig. 3 is a block diagram of a security module as may be used in the secure cashless gaming system shown in Fig. 1.

Fig. 4 is a process flow chart of a cross-authentication procedure as may be carried out between an intelligent data device reader and a security module of the secure cashless gaming system shown in Fig. 1.

Fig. 5 is a conceptual diagram illustrating the different interfaces among some of the primary components for one embodiment in accordance with the secure cashless gaming system shown in Fig. 1.

Fig. 6 is a diagram of a data extraction device such as may be used in the secure cashless gaming system shown in Fig. 1.

Fig. 7 is a diagram of a portion of a transaction list file format.

Figs. 8A – 8E are diagrams illustrating the format of records which may be included in the transaction list file transmitted from a data device reader to a data extraction device.

Fig. 9 is a block diagram illustrating processing of transaction data extracted from a data device reader.

Fig. 10 is a diagram of a secure cashless gaming system illustrating interactions between players and the various components of the gaming system.

Fig. 11 is a diagram of a gaming device system wherein on-line gaming devices having intelligent data device readers are connected to a centralized network

Fig. 12 is a diagram illustrating one manner of connecting a gaming device to a centralized network in accordance with one embodiment as disclosed herein.

Fig. 13 is a diagram illustrating another manner of connecting a gaming device to a centralized network, in accordance with another embodiment as disclosed herein.

Fig. 14 is a block diagram of a preferred security and authentication module usable in various embodiments of an intelligent data device reader.

Fig. 15 is a diagram of a portable data device, illustrating the information storage format for the portable data device.

Fig. 16 is a flow chart diagram illustrating from a global perspective the operation of a gaming system in accordance with a preferred embodiment as described herein.

Fig. 17 is a conceptual diagram illustrating the different interfaces among some of the primary components for an alternative embodiment in accordance with the secure cashless gaming system shown in Fig. 1.

Figs. 18 - 21 are additional flow chart diagrams illustrating the operation of a gaming system in accordance with an embodiment as described herein.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 is a block diagram of a secure cashless gaming system 100 in accordance with a preferred embodiment as described herein. As illustrated in Fig. 1, the secure cashless gaming system 100 comprises one or more gaming devices 110, a cashier station 120 and a data extraction device 140 which collectively provide for secure cashless gaming activity by an arbitrary number of players on various gaming devices 110, the ability to securely and accurately monitor the gaming activity at each of the gaming devices, and the ability, if desired, to track individual player gaming habits. In the typical environment which is contemplated, a large number of gaming devices 110 (in the order of tens or hundreds) may be included in the cashless gaming system 100, but the principles and concepts described herein do not depend upon any particular number of gaming devices 110 being utilized in the cashless gaming system 100.

As further illustrated in Fig. 1, each gaming device 110 preferably comprises an intelligent data device reader 112, a security module 113 connected to the intelligent data device reader 112, and a game device processor 114 connected to the security module 113. The cashier station 120 preferably comprises a data device reader 121, a cashier station processor 122 connected to the data device reader 121, and a database 123 accessible to the cashier station processor 122. The cashier station 120 also may comprise a data port 124 for receiving data from the data extraction device 140, or alternatively may comprise a disk drive (not shown) or other media reading device for receiving information from the data extraction device 140 via a portable storage medium (e.g., disk).

In an exemplary embodiment, the gaming devices 110 are off-line machines, in that they need not be connected to a central computer for handling each wagering transaction. However, it will be apparent that various concepts and principles of the secure cashless gaming system 100 illustrated in Fig. 1 would be applicable to gaming devices in an on-line gaming environment as well, and thus, in certain alternative embodiments, the gaming devices 110 may be on-line machines.

As will be described in further detail herein, a player utilizes a portable data device 130 to obtain gaming credit, and to expend the credit in the various gaming devices 110, while the system operator uses the data extraction device 140 to extract data from the gaming devices 110 concerning player wagers, winnings and other information about gaming sessions. In a preferred embodiment, the portable data device 130 comprises a smart card, which, as previously noted in the Background section herein, is a device generally in the size and shape of a standard credit card, encapsulating solid-state memory, circuitry for allowing the memory to be read from or written to, and, in a preferred embodiment as described herein, microprocessor circuitry for performing various programmable functions. As also noted previously, smart cards may be equipped with an interface having electrical contacts which make a physical connection with a smart card reader, or else, alternatively, may be equipped with a radio frequency (RF) interface to allow a smart card reader to interact with the smart card electronic circuitry over an RF communication link. Techniques for manufacturing smart cards, and for communicating between a smart card and a smart card reader via either physical contacts or an RF communication link, are well known and conventional.

Alternatively, rather than a smart card, the portable data device 130 may comprise another type of data storage and retrieval unit. An embodiment in which the portable data device 130 comprises a smart card is preferred, however, because of the ability, with on-board microprocessor circuitry, to imbue the smart card with intelligence, thereby facilitating some of the security and other features described elsewhere herein. Accordingly, the portable data device 130 may occasionally be assumed herein to be a smart card, and the data device readers 112 and 121 would in such a case be assumed to be smart card readers, as further described herein. Alternative data storage and retrieval units used instead of smart cards preferably have built-in intelligence in the form of programmable microprocessor circuitry or the equivalent, to carry out the security and other features described elsewhere herein.

Prior to using a gaming device, the player first obtains gaming credit on the portable data device (e.g., smart card) 130 by providing the portable data device 130 to the cashier station 120. Typically, this might be done by the player handing the portable data device 130 to a cashier (an employee of the casino or gaming establishment), who would be responsible for inserting the portable data device 130 in the data device reader 121 (which, if the portable data device 130 is a smart card, would take the form of a smart card reader). The cashier would then issue gaming credit to the portable data device 130, and collect an appropriate cash or payment from the player. In a typical embodiment of the cashier station 120, the cashier is presented with a screen interface (not shown), and can select among a number of options, one of which is adding gaming credit to the current portable data device 130. The cashier station 120 is preferably configured with a keyboard, keypad or other data input device (not shown), so as to allow the cashier to select the desired amount of gaming credit to add to the portable data device 130. When the player is finished gaming and wants to redeem (i.e., "cash out"), the data device reader 121 may read the amount of credit left on the portable data device 130, and display the amount of credit left on the screen for the cashier to read. The cashier may then select an option of deleting the remaining gaming credit on the portable data device 130, and may disburse cash or other form of payment to the player. In some embodiments, the portable data device 130 may have a programmed "retain value" which cannot be used for gaming, but is redeemable at the cashier station 120 to encourage the player to return the portable data device 130 when all of the available credit has been exhausted.

In addition to storing gaming credit, each portable data device 130 also preferably includes a player identification code, which allows the card to be correlated to a particular individual or entity. The player identification code is used for accounting purposes when information about particular gaming sessions is extracted from the gaming devices 110.

Fig. 15 is a diagram of a portable data device as may be used in the system shown in Fig. 1 or the various other embodiments herein, illustrating the information storage format for the portable data device. As shown in Fig. 15, a portable data device 1500 (which may, for example, comprise a smart card) comprises an identify file 1505 which stores identification and other information concerning the player and issuing gaming establishment, a keys file 1510 containing the secret keys for performing authentication checks, a transaction log file 1515 for storing data from the last gaming transactions (e.g., last 40 transactions), and a session log file 1520 storing data from the last gaming sessions (e.g., last 40 sessions).

Once gaming credit has been placed on a portable data device 130, the player may take the portable data device 130 to any of the gaming devices 110 and utilize them in a manner generally similar to coin-operated gaming devices, but only requiring a single simple act on the part of the player to obtain gaming credit on the gaming device 110. The player inserts the portable data device 130 into the intelligent data device reader 112, which communicates with the portable data device 130 over a communication link, such as is conventionally done with smart cards and smart card readers. According to well known communication protocols used with smart cards and smart card readers, data may be transmitted from the portable data device 130 to the data device reader 112 over the communication link (either with physical electrical contacts or an RF connection), and may likewise be transmitted from the data device reader 112 to the portable data device 130 over the communication link.

When the player inserts the portable data device 130 into the intelligent data device reader 112, the gaming device 110 validates the portable data device using a security module 113. If the portable data device 130 comprises a smart card, then the intelligent data device reader 112 preferably takes the form of an "intelligent" smart card reader, as further described herein. In a preferred embodiment, details of which are provided later herein, the intelligent data device reader 112 and security module 113 perform a cross-authentication check at the start of each new gaming session, and periodically during each gaming session. In such an embodiment, a gaming session is not enabled unless the cross-authentication check is passed without error.

In a preferred embodiment, the intelligent data device reader 112 and the security module 113 are uniquely associated with one another, such that the intelligent data device reader 112 will only operate with the security module 113 uniquely associated with it, and the security module 113 will only allow authentication of the intelligent data device reader 112 uniquely associated with it. Thus, an intelligent data device reader 112 which has been removed from its gaming device 110 will not be operable because its attempt to cross-authenticate with the associated security module 113 will result in a failure. Similarly, an intelligent data device reader 112 that is removed from one gaming device 110 and inserted in a different gaming device 110 will not be operable, because its attempt to cross-authenticate with the proper security module 113 will lead to an error. The security module 113 is preferably fastened securely to the gaming device 110 so that its removal is made as difficult as possible. For example, the security module 113 may take the form of an integrated circuit (i.e., chip) on a small printed circuit board, attached to the interior housing of the gaming device 110 by cabling passing through the printed circuit board, or by any other suitable means. Alternatively, the security module 113 may be integrated with the same electronic circuitry as the game device processor 114. In such a case, the random number generator used by the gaming device may also be incorporated within the security module 113, to prevent gaming from occurring without proper authentication. Placing the random number generator within the security module 113 also provides the capability of generating an electronic signature that allows verification of the authenticity of a jackpot (whether the gaming device 110 is in cash mode or cashless mode).

In addition to performing a cross-authentication check, the gaming device 110 also runs a validation test to ensure that the inserted portable data device 130 has been issued by an authorized casino or gaming establishment.

If the cross-authentication check passes, and if the portable data device 130 is determined to be valid, the gaming session is allowed to take place. The intelligent data device reader 112 reads the gaming credit on the card, and transfers part of the gaming credit to the game device processor 114. The security module 113 acts as a pass-through channel, allowing the intelligent data device reader 112 and the game device processor 114 to communicate freely, so long as the periodic cross-authentication checks are passed without error. The intelligent data device reader 112 stores gaming session information, such as the amount of gaming credit transferred in for the particular session, the amount played for the session, the amount won for the session, and the amount paid out for the session. The intelligent data device reader 112 stores the player identification code along with the gaming session information. A preferred set of information stored by the intelligent data device reader 112 is described hereafter in relation to Figs. 8A - 8E.

Each player can, using a single portable data device 130, play as many of the gaming devices 110 as desired, so long as the portable data device 130 has gaming credit available. Likewise, each gaming device 110 is capable of accepting portable data devices 130 from as many players as desire to play the gaming device 110. For each player, the gaming device 110 stores information pertaining to the player's gaming session.

At periodic intervals, which may be once each day or once every set number of days (primarily dependent upon the level of usage of the gaming devices 110), the gaming session information stored in the intelligent data device readers 112 of the various gaming devices 110 is extracted and delivered to a central accounting and processing system (an example of which is shown in Fig. 9 and discussed later herein). In a preferred embodiment, a data extraction device 140 is utilized to collect the gaming session information stored in the intelligent data device readers 112 of the various gaming devices 110. The data extraction device 140 preferably comprises a probe 141 connected to a portable high-volume memory storage device 142, which may simply be a laptop, personal computer, or a custom piece of equipment. The probe 141 is constructed in the size and shape of a smart card, and is configured with a smart card interface, including circuitry for communicating over the communication link between the probe 141 and the intelligent data device reader 112. When the probe 141 is inserted into the intelligent data device reader 112, the same type of validation and cross-authentication checks as described with reference to the portable data device 130 may, if desired, be carried out to ensure that the probe 141 is associated with an authorized data extraction device 140, and to ensure that the data device reader 112 is associated with the proper security module 113.

Once the validation and cross-authentication checks, if any, are carried out, a user of the data extraction device 140 may, using predefined buttons, a keypad, or user interface of any sort, instruct the intelligent data device reader 112 to transfer the collected gaming session data to the data extraction device 140. In response to such an instruction, the intelligent data device reader 112 downloads its collected gaming session information, and possibly other information (such as the number of incidents or mishaps), across the communication link to the data extraction device 140, via the probe 141. The type of data that may be transferred is described in more detail later herein with reference to Figs. 7 and 8A – 8E. Among other things, the data extraction device 140 obtains gaming session information for each player that has played the gaming device 110 since the last time the data was extracted from the gaming device.

The operator of the casino or gaming establishment proceeds in a similar manner with the relevant gaming devices 110, collecting gaming session information en masse from all of the gaming devices 110 which are a part of the secure cashless gaming system 100. After gaming session data is read out from a particular gaming device 110, the gaming session memory for the intelligent data device reader 112 may be cleared, or, alternatively, the gaming session memory may be re-circulated, with new gaming session information as it comes in overwriting the oldest gaming session information. In the latter case, should the extracted gaming session information be lost for whatever reason, it can be reconstructed by re-reading the data preserved in the gaming session memory of the intelligent data device reader 112.

Once the aggregate gaming session information has been obtained from the various gaming devices 110, the data extraction device 140 may be connected to a central accounting and processing database (e.g., database 123), through, for example, a physical cable connection to a data port 124 located at the cashier station 120 or elsewhere at the host system. Alternatively, the gaming session data may be transposed from the data extraction device 140 to a portable, permanent storage medium (such as a floppy disk), and then transferred to the central accounting and processing system through a reader (e.g., disk drive) of the permanent storage medium. In such a manner, the aggregate gaming session data is provided to the central accounting and processing system.

Once the aggregate gaming session data is provided to the central accounting and processing system, data for individual players and individual portable data devices (e.g., smart cards) are accumulated and processed. The current amount remaining on each of the portable data devices 130 can be determined, as of the date and time of the last extraction of gaming session data by the data extraction unit 140. Also, reconciliation for each of the gaming devices 110 can be accomplished. If desired, various data concerning individual player gaming habits can be collected and processed, for use by the casino or gaming establishment to track individual play and to allow the casino or gaming establishment to improve its targeted marketing efforts to the type of players it seeks to attract.

Fig. 2 is a block diagram of one embodiment of an intelligent data device reader 200 as may be used in the secure cashless gaming system shown in Fig. 1 (for example, as intelligent data device reader 112). The intelligent data device reader 200 is particularly geared for use in reading smart cards, but can be adapted with different interfaces to other types of portable data devices as well. As illustrated in Fig. 2, the intelligent data device reader 200 comprises a smart card reader 201 and a expansion module 250 which allows various interface functionality. The smart card reader 201 comprises a smart card interface 211, which is capable of reading information from and transmitting information to smart cards inserted therein over a standard smart card communication link. The smart card interface 211 is connected to a microprocessor 212, which in turn is connected to a memory 214 (divided into data memory 215 and program memory 216), a serial interface (such as an RS-232 interface) 213, and a security and authentication module (SAM) 210 and associated interface. The memory 214 preferably comprises a combination of random-access memory (RAM) and electrically erasable programmable read-only memory (EEPROM), and programming code (or part of the total programming code) may be downloaded to the memory 214 in order to program the intelligent data device card reader 200. The expansion module 250 is connected to the smart card reader 201, and comprises a liquid crystal display (LCD) interface 251, a keypad interface 252, additional (external) program and data memory 253, a real time clock 254, and a universal external device switch 255.

In operation, data received from a smart card via the smart card interface 211 may be stored in local memory 214, or else may be communicated across the serial interface 213 to the security module 113 and/or the gaming device processor 114 (see Fig. 1). Similarly, data received over the serial interface 213 may be stored by microprocessor 212 in the local memory 214, or else may be communicated via the smart card interface 211 to an inserted smart card. Gaming session data 215 may be stored in the data memory 215, and/or in the external program and data memory 253, and may be read out to a data extraction device 140 (see Fig. 1) via the smart card interface 211 when the microprocessor 212 receives the appropriate commands.

The intelligent data device reader 200 may keep track of date and time information relating to gaming session data, and may use the real time clock 254 in expansion module 250 for obtaining accurate date and time information. The microprocessor 212 of the smart card reader 201 may be programmed to display pertinent information on the LCD interface 251, such as gaming credits currently remaining on the inserted smart card, the player's name, or any other desired information. The intelligent data device reader 200 may read a language field from the portable data device 130 in order to learn the preferred language of the player, and select the language of the information displayed on the LCD interface 251 accordingly. The keypad interface 252 of the expansion module 250 provides the ability for the player to manually select an amount to wager, to enter a personal identification number (PIN) to utilize the portable data device 130 (in a manner similar to a bank or credit card), or to otherwise communicate with the gaming device 110. It can also be used by gaming establishment personnel for maintenance, such as entering test data. The universal external device switch 255 of the expansion module 250 may comprise an electrical switch which can be used to allow the microprocessor 212 of the smart card reader 201 to activate an audible buzzer, beeper, LED, light, or the like.

A block diagram of a preferred security and authentication module (SAM) 1400 usable in various embodiments of the intelligent data device reader 200 is shown in Fig. 14. The security and authentication module 1400 may physically comprise a smart card core (i.e., smart card electronics) 1450, and is preferably constructed to be a completely integral component encased in a secure housing (like an integrated chip), so that its internal connections are not externally accessible. As illustrated in Fig. 14, the security and authentication module 1400 comprises external contacts 1415 which are connected to a processor 1410 via an interface manager 1412 (preferably configured so as to be compatible with ISO 7816 interface standards). The processor 1410 is connected to a memory 1420, which is divided into data memory 1423 and program memory 1424. The processor is also preferably connected to a electrically erasable programmable read-only memory (EEPROM) 1421, or other form of non-volatile, erasable memory, for storing programming code or data that may need to be kept even if power is removed from the gaming device.

The EEPROM 1421 within the SAM 1020 may be used to store various cashless meters (in the form of program variables). Once stored, the cashless meters cannot be changed or cleared without proper access to the security and authentication module 1400 (generally requiring a master card giving the holder such privileges), even if power is removed from the gaming device. The cashless meters may be maintained by the SAM 1400 in addition to the cash meters which are typically maintained by the game device itself, and the provision of separate cashless and cash meter allows easier and more convenient accounting for the gaming device after the meters are read out. Preferably, both the cashless meters and cash meters may be read out using the portable data extraction device 140, which is described elsewhere in more detail herein.

As explained in connection with the secure cashless gaming system 100 of Fig. 1, the intelligent data device reader 200 may interface with a security module (such as security module 113 shown in Fig. 1), a preferred embodiment of which is illustrated in Fig. 3. As shown in Fig. 3, a security module 300 comprises a first interface 313 (such as an RS-232 serial communication port), which is connected to the intelligent data device reader 200 (or 112), a microprocessor 310, a memory 314 (which is divided into data memory 320 and program memory 321), and a second communication interface 312 (such as an RS-232 serial communication port), which is connected to the game device processor. Two communication port managers 311, 315 (each of which may take the form of a universal asynchronous transceiver/receiver (UART)) are resident with the microprocessor 310, for handling communications over the communication interfaces 312 and 313, respectively. Alternatively, the communication port managers (e.g., UARTs) 311, 315 may be located off-chip from the microprocessor 310.

In a preferred embodiment, the microprocessor 310 of the security module 300 is programmed to, among other things, perform one side of the cross-authentication check when a gaming session starts, and periodically thereafter. Programming instructions for its part of the cross-authentication check are stored in program memory 321. Likewise, programming instructions for the counterpart of the cross-authentication check conducted by the intelligent data device reader 200 are stored in the program memory 216 of the smart card reader 201.

Fig. 16 is a flow chart diagram illustrating the operation of a gaming system in accordance with a preferred embodiment as described herein. The flow chart diagram of Fig. 16 will be described in relation to the gaming system 110 illustrated in Fig. 1 and the preferred intelligent data device reader 200 illustrated in Fig. 2, but many of its principles may be applied to other embodiments, including on-line embodiments, as well. Further, for purposes of illustration, the portable data device 130 will be assumed to be a card (e.g., smart card), although other types of portable data devices could also be used.

As illustrated in Fig. 16, in a first step 1601 of the operation of the gaming system, a card is inserted into the intelligent data device reader 112. In a preferred embodiment of the gaming system, the card may be one of several types. The card may be, for example, a user card, a master card, or an operator card. In a next step 1602, the intelligent data device reader 112 identifies the type of card. This identification process may be accomplished by reading the response from the data device interface (e.g., smart card reader 211 shown in Fig. 2); for example, the "answer to reset" or "ATR" returned by a smart card reader. Besides being a user, master or operator card, the input could also be a probe 141 from a data extraction unit 140, in which case gaming session data may be read out, with or without authentication as described elsewhere herein.

If the input is identified as a master card, then the process moves to step 1610, wherein the card is cross-authenticated with the intelligent data device reader 112 and, more specifically, with the security and authentication module (SAM) 210 (shown in Fig. 2). For the cross-authentication referred to in step 1610, the microprocessor 212 of the smart card reader 201 acts as an intermediary between the processor located on the master card and the processor (such as processor 1410 shown in Fig. 14) located on the SAM 210. A first common key is used for this cross-authentication check, which may be carried out, for example, in accordance with the same general techniques described hereinafter with respect to Fig. 4. If the cross-authentication check fails, then, moving to step 1612, the process is aborted and the card is expelled. The cross-authentication check may be done multiple times (twice, in the example shown) to increase security.

If the cross-authentication check succeeds, the process then moves to step 1613, wherein the master card checks whether the gaming device 110 has been initialized and, specifically, whether the intelligent data device reader 112 has been initially configured. If not, then an initial configuration is run in step 1616, whereby the intelligent data device reader 112 is "matched" to the security module 113 by downloading the unique security module identifier to the SAM 200, which may be done using the portable data extractor 140 in its programming capacity. Once the SAM 200 has been loaded with the unique security module identifier, the SAM 200 and security module 113 jointly build a second common key for subsequent use in later authentication checks, and the intelligent data device reader 112 thereby becomes uniquely associated with the particular security module 113 for the gaming device 110. If the intelligent data device reader 112 has not been initially configured, then there is no way for a player with a user card to attempt to cross-authenticate with the security module 113, and no way for the player to utilize the gaming device 110.

Once the intelligent data device reader 112 has been initially configured and associated with the security module 113, the SAM 200 may be enabled using the master card. The SAM 200 preferably is programmed so that it needs to be re-enabled by the master card whenever the gaming device 110 is reset or power is removed from the gaming device 110.

If the inserted card is an operator card, then the process moves to step 1630, wherein the card and SAM 200 carry out a cross-authentication as described above for the master card. . Alternatively, one-way authentication of the operator card (but not the SAM 200) may be performed. If the cross-authentication or one-way authentication check not successful, the process aborts and the card is expelled. Otherwise, the intelligent data device reader 112 may perform a second cross-authentication, this time with the security module 113 itself (although this step 1632 may be skipped, if desired, since the operator card generally does not attempt to communicate with the game device processor). In particular, the second cross-authentication, if done, may be carried out between the SAM 200 and the security module 113, using the second common key that is stored in the SAM 200 and in the security module 113 (and developed during initial configuration). The cross-authentication check may be carried out according to the process shown in Fig. 4 and described later herein. If not successful, the process aborts. Otherwise, the intelligent data device reader 112 displays gaming session data from the last several sessions. In one embodiment, for example, the intelligent data device reader 112 displays the total gaming session results from the last five sessions, as well as the most recent results from the last several gaming transactions associated with the most recent gaming session. The operator card can thereby be used by gaming establishment personnel on the floor to check wins, losses, jackpots and the like that have recently occurred at a machine. The gaming session data may be automatically scrolled through by the intelligent data device reader 112, or else, if a keypad or keyboard is provided, the operator may select which gaming session information to display. In addition to its other functions, the master card may also be provided with the same privileges as an operator card.

If the card inserted is a user card, then the process moves to step 1650, wherein cross-authentication between the card and the SAM 200 is carried out in a manner similar to that described for the master card. If not successful, the process aborts.

Otherwise, the intelligent data device reader 112 queries the game device processor 114 to see whether any credits (i.e., coins or other cash input) remains on the game device 110. If so, then a message to that effect is displayed in step 1653, and the process aborts with the user card being expelled. Otherwise, the intelligent data device reader 112 instructs the game device processor 114 to enter a cashless mode, and refuse to accept cash until the end of the gaming session. Transferring between cash and cashless mode in gaming devices is conventionally done in on-line gaming devices, and is well known in the art. Once cashless mode is entered, in step 1655 a second cross-authentication is carried out, this time between the intelligent data device reader 112 and the security module 113. More particularly, the cross-authentication is carried out between the SAM 200 and the security module 113 using the second common key stored in the SAM 200 and the security module 113. The cross-authentication check may be carried out according to the process shown in Fig. 4 and described later herein. If the cross-authentication check fails, then the process aborts. Otherwise, in step 1657, a gaming session is allowed to begin.

Figs. 18 – 21 are additional flow chart diagrams illustrating the operation of a gaming system in accordance with a preferred embodiment as described herein, providing some additional details and some variation over the flow chart diagram of Fig. 16. Fig. 18 illustrates a top-level flow chart, wherein, similar to the flow chart diagram of Fig. 16, a master card is required to be inserted and authenticated, and association of the security module 113 accomplished. After association of the security module 113 and intelligent data device reader 112 is accomplished, the intelligent data device reader 112 awaits insertion of a portable data extraction unit 140, a user card, or an operator or master card.

Fig. 19 illustrates a preferred process flow in the case that the probe 141 of the data extraction unit 140 is inserted into the intelligent data device reader 112. According to the process flow shown in Fig. 19, various options are provided to the operator, including the setting of parameters and uploading of various data, as described later herein. Fig. 20 illustrates a preferred process flow in the case that a master card is re-inserted or an operator card is inserted into the intelligent data device reader 112. As shown in Fig. 20, various authentication checks are performed prior to allowing application of the operator card or master card functionality. Fig. 21 illustrates a preferred process flow in the case that a user card is inserted into the intelligent data device reader 112. Again, various authentication checks are performed prior to allowing user card functionality to be applied.

Fig. 4 is a process flow chart of a preferred cross-authentication procedure as may be carried out between the intelligent data device reader (e.g., intelligent data device reader 200 shown in Fig. 2) and the security module (e.g., security module 300 shown in Fig. 3), or between the intelligent data device reader and portable data device (e.g., portable data device 1500 shown in Fig. 15). As illustrated in Fig. 4, in a first step 401, a random number R1 is generated by the intelligent data device reader 200. In a next step 402, the random number R1 is enciphered by the intelligent data device reader 200 using a common key (which may be stored in SAM interface 210), yielding enciphered random number R1'. Concurrently, in step 420, a random number R2 is generated by the security module 300, and in a following step 421, the random number R2 is enciphered by the security module 300 using the same common key, yielding enciphered random number R2'. The enciphered random numbers R1', R2' are then exchanged by the intelligent data device reader 200 and the security module 300. In step 403, the intelligent data device reader 200 deciphers enciphered random number R2' using the common key, thus obtaining the original random number R2, and generates a session key S from R1 and R2 in step 404. Likewise, in step 422, the security module 300 deciphers enciphered random number R1' using the common key, thus obtaining the original random number R1, and generates the same session key S from R1 and R2 in step 423, using the same algorithm to do so as the intelligent data device reader 200.

In step 405, after the session key S has been generated, random number R2 is enciphered by the intelligent data device reader 200 using the session key S, yielding an enciphered resultant A2'. Similarly, in step 424, random number R1 is enciphered by the security module 300 using the session key S, yielding an enciphered resultant A1'. The enciphered resultants A1' and A2' are exchanged by the intelligent data device reader 200 and the security module 300. In step 406, the intelligent data device reader

200 deciphers enciphered resultant A1' received from the security module 300, while in step 425 the security module 300 deciphers enciphered resultant A2' received from the intelligent data device reader 200. In step 407, the intelligent data device reader 200 compares the deciphered resultant R1 against its originally generated random number R1. If a match is found, then, in step 408, the gaming session is enabled, while if no match is found an error condition is returned in step 409. Similarly, in step 426, the security module 300 compares the deciphered resultant R2 against its originally generated random number R2. If a match is found, then, in step 427, the gaming session is enabled, while if no match is found an error condition is returned in step 428. The results of each part of the cross-authentication check may be shared between the intelligent data device reader 200 and the security module 300.

If either part of the cross-authentication check fails, then the security module 300 will not open up the communication pathway to the gaming device processor 114 (see Fig. 1), and the player will essentially be locked out from utilizing the gaming device 110. Similarly, if either part of the cross-authentication check fails, then the intelligent data device reader 200 is programmed to prevent communication with the gaming device processor 114 and to shut down its further communication with the portable data device 130. Thus, even if the security module 300 were physically bypassed (for example, by wires) after a gaming session had started, the periodic cross-check would determine that the security module 300 was no longer present, and the intelligent data device reader 200 would not allow the gaming session to continue.

Fig. 5 is a conceptual diagram illustrating the different interfaces among some of the primary components in a preferred secure cashless gaming system. As shown in Fig. 5, a smart card 501 is configured to communicate according to a standard (e.g., ISO) card interface protocol 502. An intelligent data device reader 505 is configured to communicate with the smart card 501 using the same standard (e.g., ISO) card interface protocol 507. The intelligent data device reader 505 is also configured to communicate with a security module 510 using a standard gaming device interface protocol 508, such as SAS or SDS, for example, both of which are conventional and well known in the field of gaming devices. The security module 510 is configured so as to allow pass-through communication (i.e., transparency), once the cross-authentication and validation checks have cleared. The intelligent data reader 505 thereby communicates with the gaming device processor 515, which is also configured to communicate using a standard gaming device interface protocol 518 (the same gaming device interface protocol 508 as used by the intelligent data device reader 505), such as SAS or SDS.

The interfaces illustrated in Fig. 5 may be utilized in the cashless gaming device system 100 shown in Fig. 1, or in connection with the specific intelligent data device reader 200 or security module 300 illustrated in Figs. 2 and 3, respectively.

Fig. 17 is a conceptual diagram illustrating the different interfaces of some of the primary components of the secure cashless gaming system shown in Fig. 1, in accordance with an alternative embodiment as described herein. As illustrated in Fig. 17, similar to the embodiment shown in Fig. 5, a smart card 1701 is configured to communicate according to a standard (e.g., ISO) card interface protocol 1702. An intelligent data device reader 1705 is configured to communicate with the smart card 1701 using the same standard (e.g., ISO) card interface protocol 1707. The intelligent data device reader 1705 is also configured to communicate with a security module 1710 using a special protocol, designated as a security module (SM)/Reader interface protocol 1711 in Fig. 17. A security module 1710 also is configured to communicate with the intelligent data reader 1705 using the SM/Reader protocol 1712. The security module 1710 translates between the SM/Reader protocol 1712 and a standard gaming device interface protocol 1708, such as SAS or SDS. The security module 1710 is configured so as to communicate with the gaming device processor 1715, which is also configured to use the standard gaming device interface protocol 1718 (i.e., the same gaming device interface protocol 1708 as used by the security module 1710), such as SAS or SDS.

The SM/Reader interface protocol 1711, 1712 preferably supports at least of subset of commands and capabilities as provided by the standard gaming device interface protocol 1708 and 1718, but need not provide all of the capabilities thereof, particularly if the gaming device is used off-line. The SM/Reader interface protocol 1711, 1712 may, for example, support commands or capabilities for crediting the gaming device, debiting the gaming device, checking the denomination of the gaming device, checking the gaming device identification number, checking the currency of the gaming device, checking the amount of credit left on the gaming device, and receiving gaming device activity (such as, for example, how much the player is betting, result of gaming transaction (winner, loser, jackpot, etc.), or error conditions at the gaming device).

An advantage of the protocol structure illustrated in the embodiment of Fig. 17 is that the same intelligent data device reader 1705 could be used without modification along with gaming devices using any standard gaming device interface protocol that is supported by the security module 1710. For the protocol structure illustrated in Fig. 5, by contrast, it may be necessary to download the specific standard gaming device interface protocol 508 to the intelligent data device reader 505 prior to operation, unless the memory space of the intelligent data device reader 505 is sufficient to contain the various standard gaming device interface protocols from which the desired one may be selected. By moving the responsibility for interfacing with the standard gaming device interface protocol to the security module 1710, as illustrated in Fig. 17, the memory requirements for the intelligent data device reader 1705 may be alleviated somewhat.

As with the embodiment shown in Fig. 5, the interfaces illustrated in Fig. 17 may be utilized in the cashless gaming device system 100 shown in Fig. 1, or in connection with the specific intelligent data device reader 200 or security module 300 illustrated in Figs. 2 and 3, respectively.

When the cross-authentication and validation checks first pass, and a gaming session is enabled, the intelligent data device reader 112 may be programmed with additional capability to start off a gaming session without extra effort by the player. Specifically, the intelligent data device reader 112 may be programmed to remove gaming credits from the credit amount stored in the portable data device 130, and to transfer those credits to the gaming device processor 114 to allow play to begin. The number of credits to be so transferred may be programmably set. The intelligent data device reader 112 uses an link layer protocol (such as a smart card protocol) for reading and adjusting the credits on the portable data device 130, then uses the gaming device protocol (such as SAS or SDS) to transfer the credits over to the gaming device processor 114. The monetary value and/or number of credits transferred (and hence available) may be displayed to the player on an LCD display, along with other information, as desired, such as the players name or pseudonym. The portable data device 130 may have a player language data field, which may be read by the intelligent data device reader 112, which can adjust the language of any special messages accordingly.

The intelligent data device reader 112 may further be programmed such that each time the number of available credits drops below a predefined level, the intelligent data device reader 112 transfers additional gaming credits from the current credit amount on the portable data device 130 to the gaming device processor 114. The intelligent data device reader 112 is aware of the number of current credits, as well as the outcome of the most recent gaming transaction, because the gaming device processor 114 is typically programmed to make such information available according to standard gaming device protocols (such as SAS or SDS). The level at which the intelligent data device reader 112 re-credits the gaming device 110, and the amount of credits transferred in a re-credit transaction, may both be programmably set. By automatically re-crediting the machine each time the number of credits drops below the predefined minimum, the player does not need access to a keypad or other similar means for transferring credits, and is not burdened with the inconvenience of constantly refreshing the amount of credits at the machine.

At the end of a gaming session, or periodically during the gaming session as gaming credits are transferred to the gaming device 110, the intelligent data reader 112 transmits back to the smart card (or other portable data device 130) update information which alters the amount of gaming credit remaining on the portable data device 130. When the player leaves the gaming device, the new gaming credit amount will reside on the portable data device 130. Preferably, the portable data device 130 stores a predefined number of previous gaming transactions (i.e., wagers), such as 10 or 20 previous gaming transactions. Generally, memory space on devices such as smart cards is very limited, which prevents storage of large amounts of information. Storage of a limited number of gaming transactions may prove beneficial in certain circumstances. For example, should the player contest a pay-out on a recent wager, the portable data device 130 could be read (at the cashier station 120) to determine what transpired at the gaming device 110.

Fig. 6 is a diagram of a preferred data extraction device 600 such as may be used in the secure cashless gaming system shown in Fig. 1 (for example, as data extraction device 140 shown in Fig. 1). As illustrated in Fig. 6, the data extraction device 600 includes a probe 630 connected to a portable high-volume data retention unit 610 via a cable 640. The probe 630 consists of an interface 631 which is compatible with the interface utilized by the intelligent data device reader 112 (see Fig. 1). Signals received by the interface 631 from the intelligent data device reader 112 are amplified by a voltage converter interface 632, so as to make them of the appropriate voltage level for a serial (e.g., RS-232) interface 635. Typically, signals output by the interface 631 are 5-volt signals, while an RS-232 interface operates with 12-volt signals. The amplified signals are transmitted by the serial interface 635 over the cable 640 to another serial (e.g., RS-232) interface 614, which is part of the portable high-volume data retention unit 610. The portable high-volume data retention unit 610 also comprises a processor 611 and a memory 612 for receiving and storing information received by the probe 630 from the intelligent data device reader 112. Memory 612 is preferably of sufficient capacity so as to allow storage of gaming session information from a large number of gaming devices 110. Alternatively, gaming session information may periodically be written to floppy disks or other intermediate storage devices, when the memory 612 gets full.

In operation, the operator inserts the probe 630 into the intelligent data device reader 112, generally in the same manner as a player would insert a portable data device 130. For example, if the portable data device 130 is a smart card, and the intelligent data device reader 112 includes a smart card interface, then the operator would insert the probe 630 in the slot of the smart card interface intended to receive smart cards. The operator then triggers the extraction of data from the gaming device 110, by manually pressing a button, or entering a code on a keypad, or otherwise generating a manual input. Alternatively, the presence of the probe 630 may be automatically detected by the intelligent data device reader 112, which then proceeds to transmit accumulated gaming session information to the data extraction device 600 via the communication link established by the probe 630. The intelligent data device reader 112 may store, for example, hundreds or thousands of the last gaming sessions played at the machine. In a presently preferred embodiment, the intelligent data device reader 112 stores the last 3000 gaming sessions played at the machine.

Figs. 7 and 8A – 8E are diagrams illustrating various formats in which data is transferred from the intelligent data device reader 112 to the data extraction device 600, and stored therein. In a preferred embodiment, the gaming session information is made secure and tamper-resistant by providing a special integrity code (referred to as a "MAC") for each gaming session record, and then again by providing a separate MAC for all of the gaming sessions transmitted with the file as a group, so as to prevent the erasure of an entire gaming session. Fig. 7 is a diagram of a portion of a transaction list file format illustrating the use of MACs to preserve data integrity. As shown in Fig. 7, a transaction list file 700 comprises a header record 701, one or more gaming session records 702a-702n, each of which has its own individual MAC 703a-703n, respectively, and a group MAC 705.

Figs. 8A – 8E are diagrams illustrating the format of records which may be included in the transaction list file transmitted from a data device reader to a data extraction device. Figs. 8A and 8B show a header records 800 and 820 for transactions and meter readings, respectively. Fig. 8C shows a gaming session record 840. Fig. 8D shows a header record 860 for recorded incidents during previous gaming sessions, and Fig. 8E shows an incident file record 880.

Header record 800 shown in Fig. 8A may include, for example, a record number identifier field 801, a machine identifier field 802, a data device reader identifier field 803, a denomination field 804, a total money in field 805, a total money out field 806, a total money played 807 field, a total money won field 808, a start date field 809, a start time field 810, a last time field 812, a number of sessions field 813, and a total field 814.

Header record 820 shown in Fig. 8B may include, for example, a record identifier field 821, a cumulative money in field 822, cumulative money out field 823, cumulative money played field 824, a cumulative money won field 825, and a total field 826.

Gaming session record 840 shown in Fig. 8C may include, for example, a record identifier field 841, a session number field 842, a portable data device (e.g., smart card) identifier field 843, a transaction type field 844, a session money in field 845, a session money out field 846, a session money played field 847, a session money won field 848, a player identifier field 849, an offset data field 850, a start time field 851, a duration field 852, and total field 853.

Header record 860 shown in Fig. 8D may include, for example, a record identifier field 861, a machine identifier field 862, a data device reader identifier field 863, a number of incidents field 864, and a total field 865. Incident file record 880 shown in Fig. 8E may include, for example, a record identifier field 881, a incident type code field 882, a date of incident field 883, a time of incident field 884, a program status field 885, and a data message field 886.

The data extraction device 600 may, in a preferred embodiment, provide the operator with a choice of various commands. Examples of commands include: (1) read transaction list (i.e., gaming session information); (2) read incident list; (3) read parameters; (4) load new parameters; (5) erase transaction list (from memory of the intelligent data device reader 112); and (6) erase transaction list (from memory of the intelligent data device reader 112). The parameters which may be read with command (3) may include, for example, display messages, machine denomination ($1, $5, etc.), initial credit transfer amount, level at which to re-credit, and how much to re-credit. By using command (4), the parameters (including the machine denomination and display messages) may be re-programmed using the data extraction device 600.

Once the aggregate gaming session data has been downloaded from all of the gaming devices to the data extraction unit 600, the gaming session data is transferred to a central accounting and processing system. The gaming session data may be transferred via a physical cable connection through a data port 615 of the data extraction device 600 (using a physical cable 655 with a port connector 650 and a cable wire 651), or else may be written to one or more floppy disks or other storage media and read by computer equipment associated with the central accounting and processing system.

Further details concerning the entry of data into the central accounting and processing system are provided with reference to Fig. 9, which is a block diagram illustrating processing of transaction data extracted from a data device reader. As illustrated in Fig. 9, gaming device data (including transaction list data and incident data) is received from the data extraction device 140 (or 600) over an interface 901 (such as a parallel port connection, for example, or via a disk or other storage medium). The transaction data is validated by validation function routine 915 by checking the MAC for each gaming session and checking the group MAC for all of the gaming sessions (see, e.g., Fig. 7). The running totals for each portable data device 130 are then updated by an update function routine 917. The transaction data is stored in a transaction database 925, and the incident data is stored in an incident database 926. A database interface 910 may format the data and otherwise facilitate storage in the transaction database 925 or incident database 926. Via a user interface 941 (such as at a cashier station 120), an authorized employee or agent of the casino or gaming establishment may view the transaction or incident data by issuing a query to the database 925 or 926, respectively. A batch process 930 may be run on the information stored in the transaction database 925, to allow profiling or information gathering concerning particular players. Tracking of any of the types or fields of data obtained from the portable data devices 130 or the portable data extraction unit 140 may be done by the gaming establishment in a batch mode. The results of such tracking may provide a basis for the gaming establishment to issue coupons, gaming credits, or other perquisites to customers to encourage their continued business.

Fig. 10 is a diagram of one embodiment of a secure cashless gaming system 1001, illustrating from a graphical perspective, examples of interactions between players and the various components of the gaming system 1001. As illustrated in Fig. 10, players can obtain variable amount portable data devices (such as smart cards) from a cashier station, and utilize them in various gaming devices as may be provided by the gaming establishment. Information stored in the intelligent data device readers (designated as "internal reader" of the "game" in Fig. 10) may be read out using a portable data extractor, such as a laptop or other computerized device connected to a probe.

Fig. 11 is a diagram of a cashless gaming system 1100 using on-line gaming devices 1110 having intelligent data device readers connected to a network host 1151 in a centralized network configuration. In the embodiment illustrated in Fig. 11, a network host 1151 communicates with the various on-line gaming devices 1110 over a network communication bus 1150. Each gaming device 1110, similar to those shown in Fig. 1, comprises an intelligent data device reader 1112, a game device processor 1114, and a security module 1113 interposed between the intelligent data device reader 1112 and game device processor. The data device reader 1112 accepts and reads portable data devices 1113, in a manner similar to that described for Fig. 1. The intelligent data device reader 1112 also stores gaming session data as previously explained herein.

Rather than using a portable data extractor to obtain the gaming session data stored in the intelligent data device reader 1112, the gaming session data is transferred to the network host 1151 during convenient periods of time, depending on the traffic at the network host 1151. In most, if not all, conventional on-line gaming systems, the gaming devices transmit gaming information to a network host for each gaming transaction. The network host thus can get overwhelmed when the attached gaming devices are very busy, and bottlenecks or slow response of the network host can occur. In the embodiment illustrated in Fig. 11, on the other hand, the intelligent data device reader 1112 alleviates the processing burden on the network host 1151 by temporarily storing gaming session information that may accrue over hours or even days, until the network host 1151 requests it. With such a configuration, the network host 1151 need only perform a fraction of the processing of conventional on-line gaming systems.

As further illustrated in Fig. 11, the network host 1150 may be connected to a cashier station 1120, which is generally of the same character as that described with respect to Fig. 1. Players can receive portable data devices 1130 from the cashier station 1120, or else can redeem remaining credits on portable data devices 1130 after they have been used, by taking them to the cashier station 1120.

The content and format of the gaming session (and related) data stored by the intelligent data device reader 1112 may take the format, for example, which is shown in Figs. 8A - 8E. Transferring information in such a format would generally require an adaptation to a standard network communication protocol format, such as SAS or SDS.

There are a variety of ways in which the intelligent data device reader 1112 may be connected to the network communication bus 1150 for communication with to the network host 1151. Two examples of such connection are shown in Figs. 12 and 13, respectively. In the first example, shown in Fig. 12, a gaming device 1210 includes the game device processor 1214 connected to both a network communication port 1238 and a local communication port 1237. The game device processor 1214 selects between the local communication port 1237 and the network communication port 1238 as circumstances dictate. The local communication port 1237 is connected to a local area network including a local network bus 1261. The local network includes a security module 1213, and may optionally include a keyboard 1235, a display 1236, or any other additional component desired. The security module 1213 is connected to an intelligent data device reader 1212. The security module 1213 and intelligent data device reader 1212 are in most respects analogous to the security module 113 and intelligent data device reader 112 depicted in Fig. 1. However, rather than extracting data from the intelligent data device reader 1212 using a portable data extractor (as in a preferred embodiment in accordance with Fig. 1), instead the gaming session data is transmitted over the network communication bus 1250 to the network host 1251. The transfer of the gaming session data can be initiated by either the intelligent data device reader 1212, the game device processor 1214, or the network host 1251. The game device processor 1214 acts as the intermediary between the intelligent data device reader 1212 and the network host 1251. The intelligent data device reader 1212 transfers gaming session data to the game device processor 1214 via the local communication port 1237, and the game device processor 1214 then forwards the gaming session data to the network host 1251 via the network communication port 1238. The gaming session data need not necessarily be formatted with MACs, depending upon the level of security of the lines connecting the network host 1251 to the gaming device 1210.

Fig. 13 is a diagram illustrating another manner of connecting a gaming device to a network host. As illustrated in Fig. 13, a gaming device 1310 includes a game device processor 1314, and intelligent data device reader 1312, and a security module 1313 interposed between the game device processor 1314 and the intelligent data device reader 1312. The security module 1313 internally has a "T" data path configuration, such that data may be routed over a first data path 1324 between the intelligent data device reader 1312 and the game device processor 1314, or else over a second data path 1323 between the game device processor 1314 and the network host 1351. In operation, when the gaming device 1310 is in a cash mode, the security module 1313 allows the game device processor 1314 to communicate freely with the network host 1351. However, when a portable data device is inserted in the intelligent data device reader 1312, and when the gaming device 1310 enters a cashless mode after the portable data device and intelligent data device reader 1312 are authenticated, the security module 1313 temporarily shuts down data path 1323 between the game device processor 1314 and the network host 1351, until the gaming session is complete. The embodiment shown in Fig. 13 thereby allows gaming devices having only a single communication port to have a cash or cashless capability, and still be connected to a centralized network host 1351 for on-line control.

In a number of embodiments that have been discussed above and/or illustrated in the drawings, specific types of interfaces (such as RS-232) have been enumerated. It should be understood that no limitation is intended by the specific type of interface that has been included as part of the various embodiments, and those skilled in the art will recognize that various alternative serial or parallel interfaces may be used, depending upon such things as cost, available space, preferred protocol, and other design considerations which are routinely addressed by engineers.

While preferred embodiments of the invention have been described herein, many variations are possible which remain within the concept and scope of the invention. Such variations would become clear to one of ordinary skill in the art after inspection of the specification and the drawings. The invention therefore is not to be restricted except within the spirit and scope of any appended claims.

CLAIMS

What is claimed is:

1. A gaming device for use in a cashless gaming system, comprising:

a data device reader adapted to receive and read portable data devices;

a game device processor; and

a security module interposed between said data device reader and said game device processor, said security module preventing communication between said data device reader and said game device processor unless said data device reader is authenticated by said security module upon one of said portable data devices being received by said data device reader.

2. The gaming device of claim 1, wherein said portable data devices comprise smart cards, and wherein said data device reader comprises a smart card reader.

3. An intelligent data reader for use in a gaming device, comprising:

a data device interface adapted to receive and read portable data devices, each of said portable data devices associated with a player;

a gaming device interface for connection to the gaming device;

a memory; and

a processor connected to said memory, said data device interface and said gaming device interface, said processor configured to communicate with the gaming device over said gaming device interface and to store session gaming data for each player in said memory.

4. The intelligent data reader of claim 3, wherein each portable data device stores a credit amount allowing the player associated with the portable data device to utilize the gaming device.

5. The intelligent data reader of claim 4, wherein a portion of said credit amount is automatically conveyed by said intelligent data device reader to the gaming device upon presentation of said portable data device to said data device interface.

6. A security module for use in a gaming device, comprising:

a data device reader interface for connection to a data device reader;

a gaming device interface for connection to a game device processor; and

a processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated.

7. The security module of claim 6, wherein said processor allows communications to pass through unimpeded between said data device reader and said game device processor after authentication of said data device reader.

8. The security module of claim 6, wherein said processor is configured to perform periodic authentication of said data device reader after said data device reader is first authenticated, and to prevent communication between said data device reader and said game device processor if said data device reader fails said periodic authentication.

9. The security module of claim 6, wherein said data device reader is first authenticated when said processor generates a first random number, enciphers said first random number using a common key to generate a first enciphered random number, sends said first enciphered random number to said data device reader over said data device reader interface, receives a second enciphered random number from said data

device reader' over said data device reader interface, deciphers said second enciphered random number using said common key to generate a second random number, generates a session key from said first random number and said second random number, receives a third enciphered number from said data device reader over said data device reader interface, deciphers said third enciphered number using said session key to generate an authentication test value, and verifies that said authentication test value matches said second random number.

10. A secure, cashless gaming system, comprising:

a plurality of gaming devices, each of said gaming devices comprising

a security module;

a gaming device processor; and

an intelligent data device reader adapted to receive and read portable data devices, said intelligent data device reader storing data for individual gaming sessions in a local memory;

a portable data extractor adapted to be received by said intelligent data device reader, said portable data extractor comprising memory for storing said data for individual gaming sessions from said plurality of gaming devices.

11. The intelligent data reader of claim 3, wherein said processor is configured to store session gaming data for each player in said memory.

12. The intelligent data reader of claim 3, wherein said processor switches the gaming device from the cash mode of operation to the cashless mode of operation by sending a command across the gaming device interface in response to reading a portable data device at said data device interface.

13. The intelligent data reader of claim 12, wherein switching of the gaming device from the cash mode of operation to the cashless mode of operation is inhibited if credit is still remaining on said gaming device.

14. The intelligent data reader of claim 12, wherein switching of the gaming device from the cash mode of operation to the cashless mode of operation is inhibited if said portable data device does not pass an authentication check.

15. The intelligent data reader of claim 14, further comprising an internal security access module, wherein said authentication check includes a first cross-authentication check between said portable data device and said internal security access module, and a second cross-authentication check between said internal security access module of the intelligent data reader and an external security module interposed between said gaming device interface and the gaming device.

16. The intelligent data reader of claim 12, wherein said processor switches the gaming device from the cashless mode of operation back to the cash mode of operation by sending a command across the gaming device interface in response to termination of a gaming session.

17. The intelligent data reader of claim 16, further comprising cashless meters for storing session gaming data, including credit information relating to said portable data devices.

18. The intelligent data reader of claim 17, wherein credit information is transmitted from said cashless gaming meters over the data device interface to the portable data device upon termination of a gaming session.

19. The intelligent data reader of claim 16, wherein the commands sent from said processor to said gaming device to switch said gaming device to the cashless mode of operation or the cash mode of operation are transmitted using a standard gaming device communication protocol.

20. The intelligent data reader of claim 19, wherein said standard gaming device communication protocol is either SDS or SAS.

21. A data reader, comprising:

a data device interface adapted to receive and read portable data devices, each of said portable data devices storing credit information;

an external device interface for connection to an external device having a cash input mechanism;

a memory, said memory including cashless meters for storing credit information relating to said portable data devices; and

a processor connected to said memory, said data device interface and said external device interface, said processor configured to communicate with the external device over said external device interface and to switch said external device between a cash mode of operation and a cashless mode of operation.

22. The data reader of claim 21, wherein said external device comprises an electronic gaming machine, and wherein said external device interface comprises a gaming machine interface.

23. The data reader of claim 22, wherein each portable data device stores a credit amount allowing a player associated with the portable data device to utilize the gaming device.

24. The data reader of claim 23, wherein a portion of said credit amount is automatically conveyed to the gaming device over the gaming device interface upon presentation of said portable data device to said data device interface.

25. The data reader of claim 23, wherein said processor is configured to store session gaming data for each player in said memory.

26. The data reader of claim 22, wherein credit information is transmitted from said cashless gaming meters over the data device interface to the portable data device upon termination of a gaming session.

27. The data reader of claim 22, wherein the commands sent from said processor to the gaming device to switch the gaming device to the cashless mode of operation or the cash mode of operation are transmitted using a standard gaming device communication protocol.

28. The data reader of claim 27, wherein said standard gaming device communication protocol is either SDS or SAS.

29. The data reader of claim 21, wherein said processor switches the external device from the cash mode of operation to the cashless mode of operation by sending a command across the external device interface in response to reading a portable data device at said data device interface.

30. The data reader of claim 29, wherein switching of the external device from the cash mode of operation to the cashless mode of operation is inhibited if credit is still remaining on said external device.

31. The data reader of claim 12, wherein switching of the external device from the cash mode of operation to the cashless mode of operation is inhibited if said portable data device does not pass an authentication check.

32. The data reader of claim 31, further comprising an internal security access module, wherein said authentication check includes a first cross-authentication check between said portable data device and said internal security access module, and a second cross-authentication check between said internal security access module of the data reader and an external security module interposed between said external device interface and the external device.

33. The data reader of claim 32, wherein said external security module allows communications to pass through unimpeded between said data device reader and said external device after the cross-authentication check between said internal security access module with said external security module.

34. The data reader of claim 33, wherein said external security module is configured to perform periodic authentication of said data device reader after said cross-authentication check between said internal security access module with said external security module, and to prevent communication between said data device reader and said external device if said periodic authentication fails.

35. The data reader of claim 32, wherein said second cross-authentication check is carried out when said internal security access module generates a first random number, enciphers said first random number using a common key to generate a first enciphered random number, sends said first enciphered random number to said external security module over said external device interface, receives a second enciphered random number from said external security module over said gaming device interface, deciphers said second enciphered random number using said common key to generate a second random number, generates a session key from said first random number and said second random number, receives a third enciphered number from said external security module over said data device reader interface, deciphers said third enciphered number using said session key to generate an authentication test value, and verifies that said authentication test value matches said second random number.

36. A method of controlling operation of a gaming device, said gaming device comprising a cash input mechanism, the method comprising the steps of:

reading portable data devices at a portable data device interface of an intelligent data reader, said portable data device storing credit information; and transmitting commands from said intelligent data reader to the gaming device over a gaming device interface, to switch the gaming device between a cash mode of operation and a cashless mode of operation.

37. The method of claim 36, wherein the step of transmitting commands from said intelligent data reader to the gaming device over the gaming device interface comprises the steps of transmitting a first command to switch the gaming device to the cashless mode of operation when a portable data device is initially read at said portable data device interface, and transmitting a second command to switch the gaming device to the cash mode of operation when a gaming session initiated using the portable data device has terminated.

38. The method of claim 36, wherein said portable data device are smart cards.

39. The method of claim 36, further comprising the step of cross-authenticating each portable data device with an internal security access module upon initially reading the portable data device.

40 The method of claim 39, further comprising the step of cross-authenticating the internal security access module with an external security module interposed between said gaming device interface and the gaming device, upon initially reading the portable data device.

41. The method of claim 36, further comprising the step of automatically transferring, without manual intervention, a fixed amount of credit from a portable data device to the gaming device whenever an amount of credit remaining at the gaming device drops below a predetermined threshold amount.

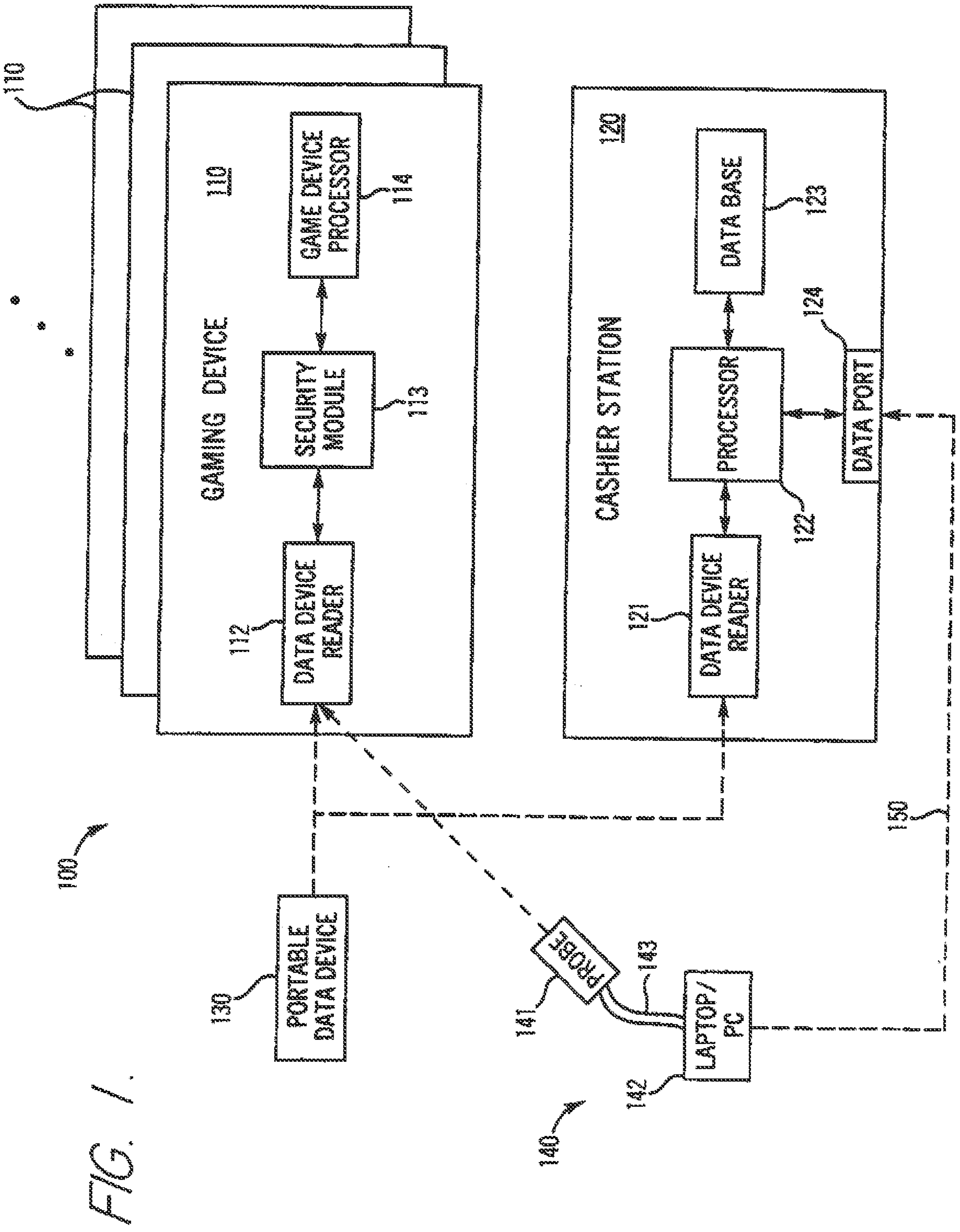

100
110
GAMING DEVICE
110
GAME DEVICE PROCESSOR
114
SECURITY MODULE
113
DATA DEVICE READER
112
CASHER STATION
120
DATA BASE
123
PROCESSOR
122
DATA PORT
124
DATA DEVICE READER
121
PORTABLE DATA DEVICE
130
PROBE
141
143
LAPTOP/ PC
142
140
150

FIG. 1.

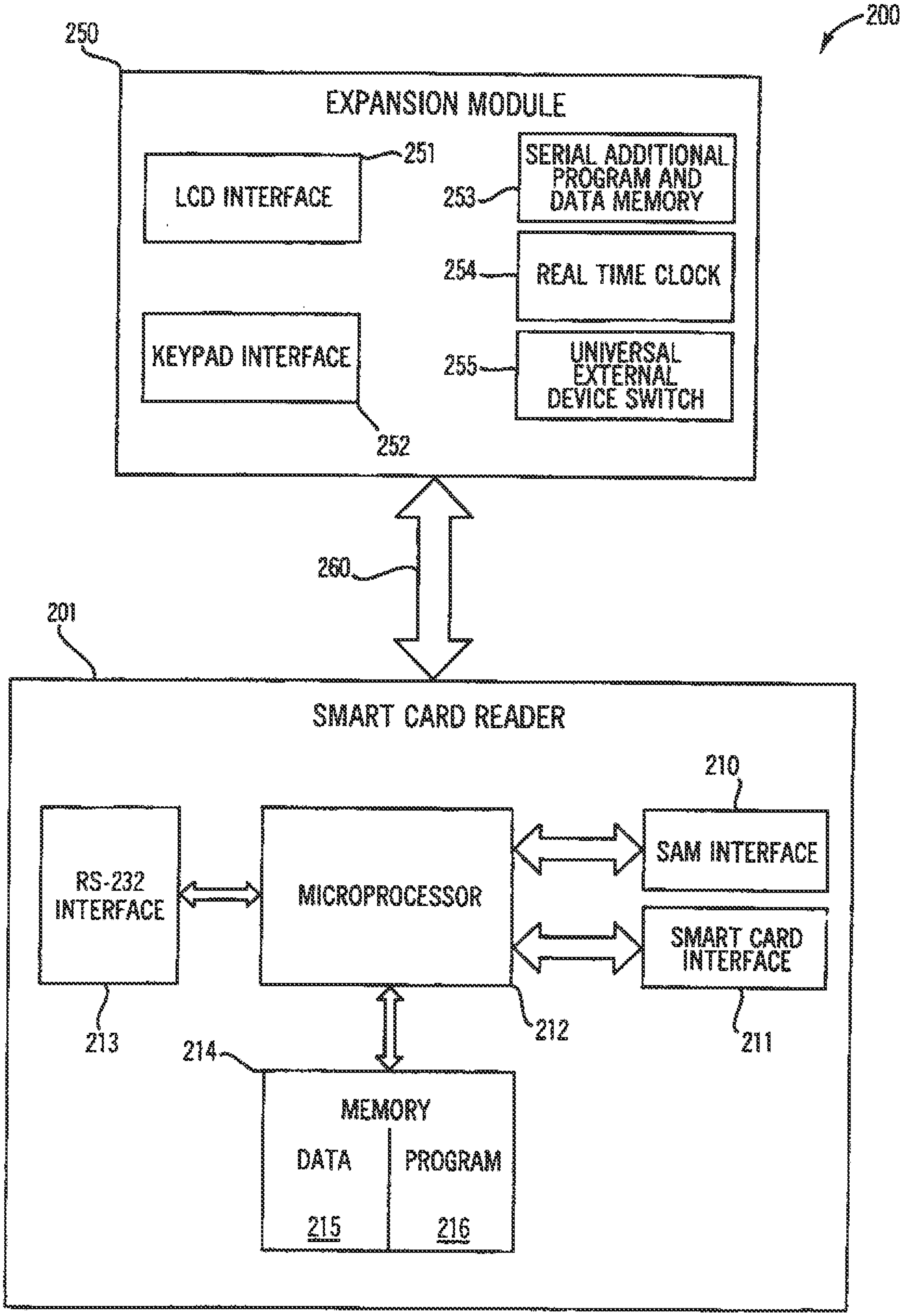

200
250
EXPANSION MODULE
LCD INTERFACE
251
253
SERIAL ADDITIONAL PROGRAM AND DATA MEMORY
254
REAL TIME CLOCK
KEYPAD INTERFACE
255
UNIVERSAL EXTERNAL DEVICE SWITCH
252
260
201
SMART CARD READER
210
RS-232 INTERFACE
MICROPROCESSOR
SAM INTERFACE
SMART CARD INTERFACE
213
212
211
214
MEMORY
DATA
PROGRAM
215
216

FIG. 2.

FIG. 3.

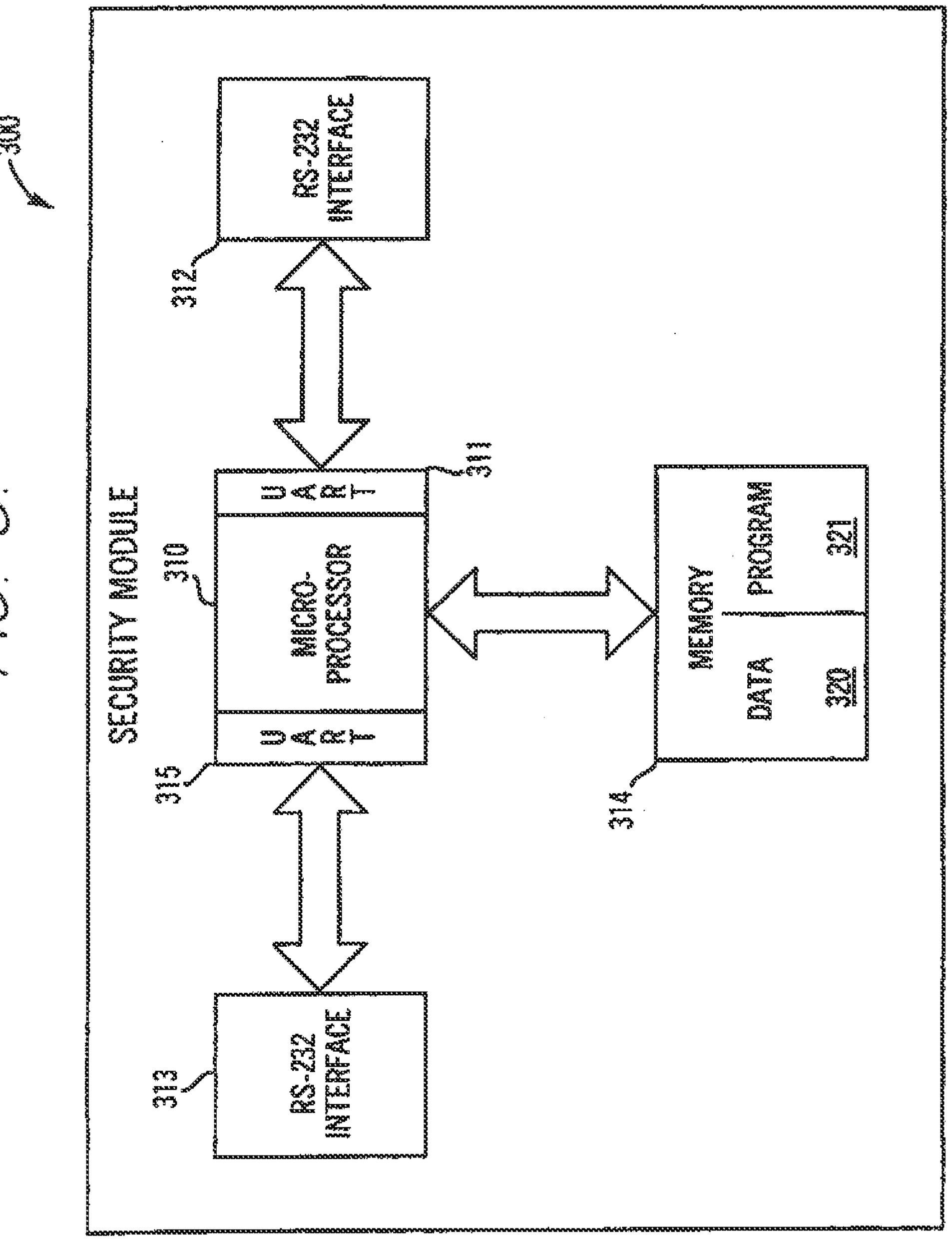
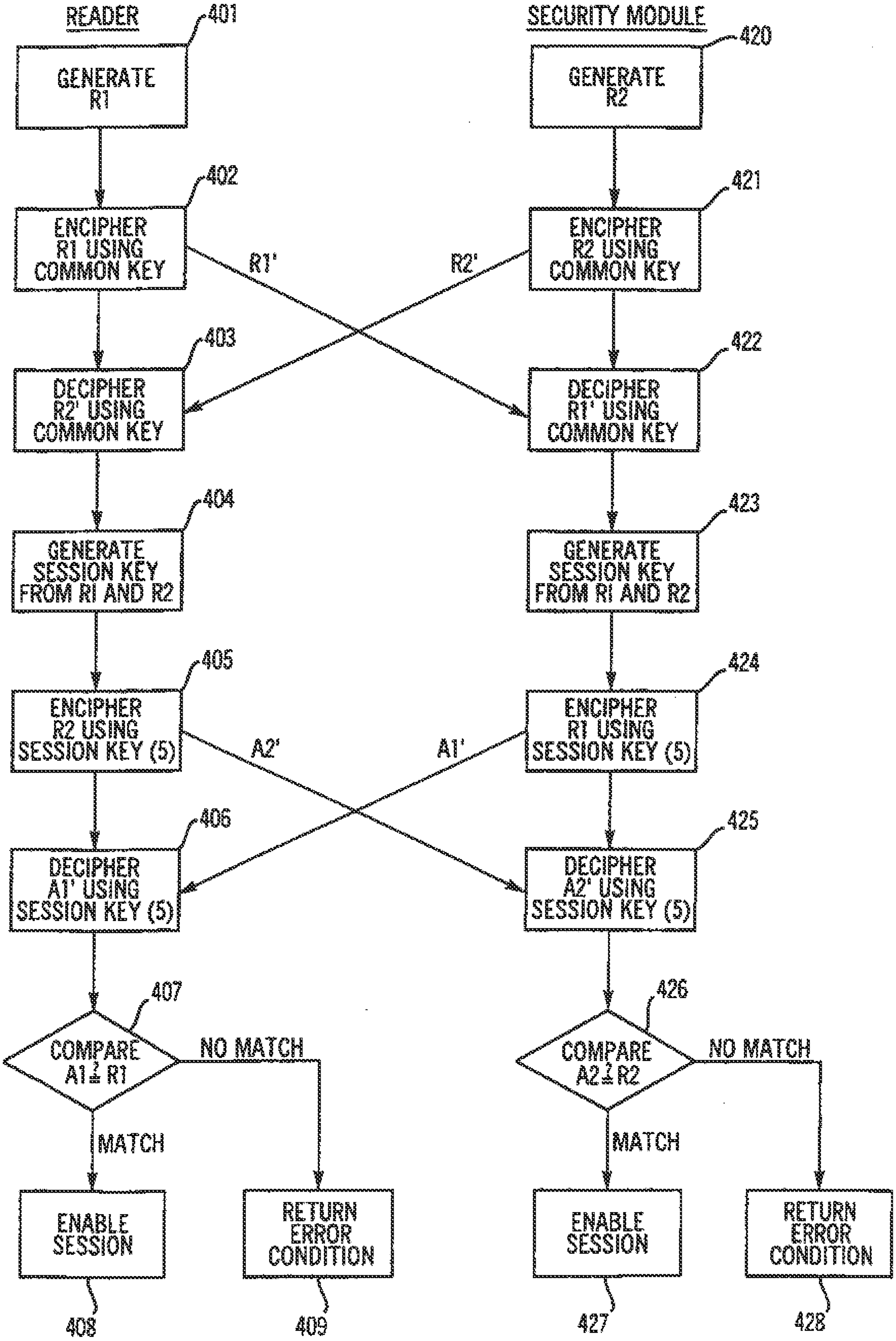

300
SECURITY MODULE
RS-232 INTERFACE
312
UART
311
MICRO-PROCESSOR
310
UART
315
RS-232 INTERFACE
313
MEMORY
DATA
320
PROGRAM
321
314

FIG. 4.


READER
401
GENERATE R1
402
ENCIPHER R1 USING COMMON KEY
R1'
403
DECIPHER R2' USING COMMON KEY
404
GENERATE SESSION KEY FROM RI AND R2
405
ENCIPHER R2 USING SESSION KEY (5)
A2'
406
DECIPHER A1' USING SESSION KEY (5)
407
COMPARE A1 ?= R1
NO MATCH
MATCH
ENABLE SESSION
408
RETURN ERROR CONDITION
409
SECURITY MODULE
420
GENERATE R2
421
ENCIPHER R2 USING COMMON KEY
R2'
422
DECIPHER R1' USING COMMON KEY
423
GENERATE SESSION KEY FROM RI AND R2
424
ENCIPHER R1 USING SESSION KEY (5)
A1'
425
DECIPHER A2' USING SESSION KEY (5)
426
COMPARE A2 ?= R2
NO MATCH
MATCH
ENABLE SESSION
427
RETURN ERROR CONDITION
428

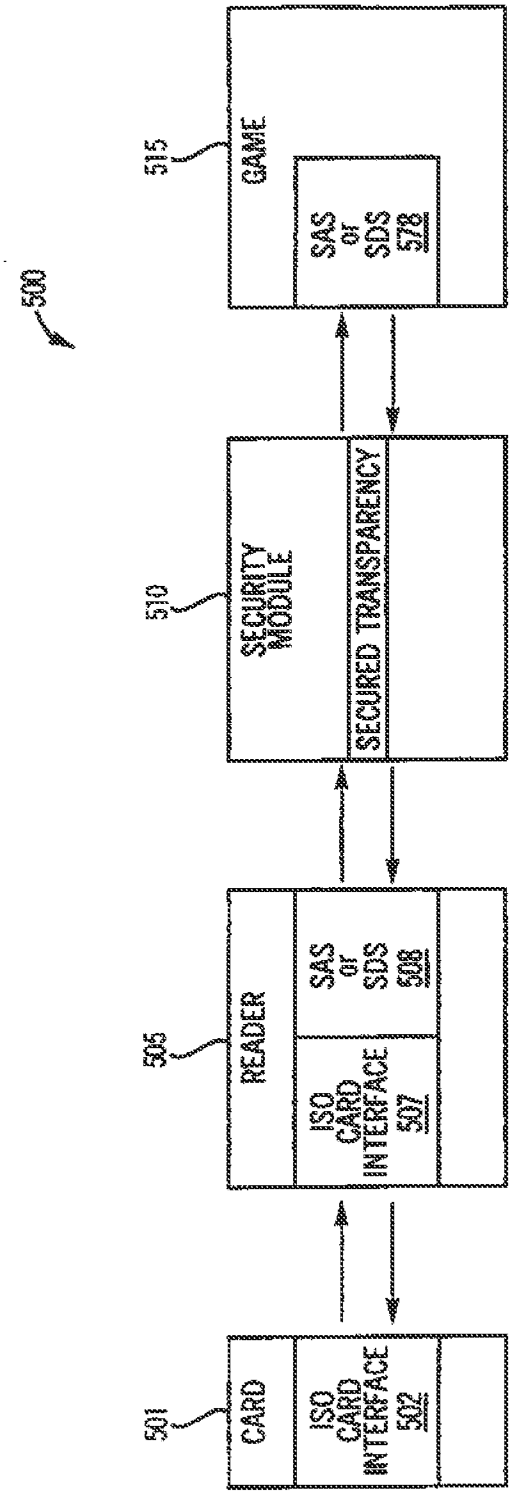

500
501
CARD
ISO CARD INTERFACE 502
505
READER
ISO CARD INTERFACE 507
SAS or SDS 508
510
SECURITY MODULE
SECURED TRANSPARENCY
515
GAME
SAS or SDS 578

FIG. 5.

FIG. 6.

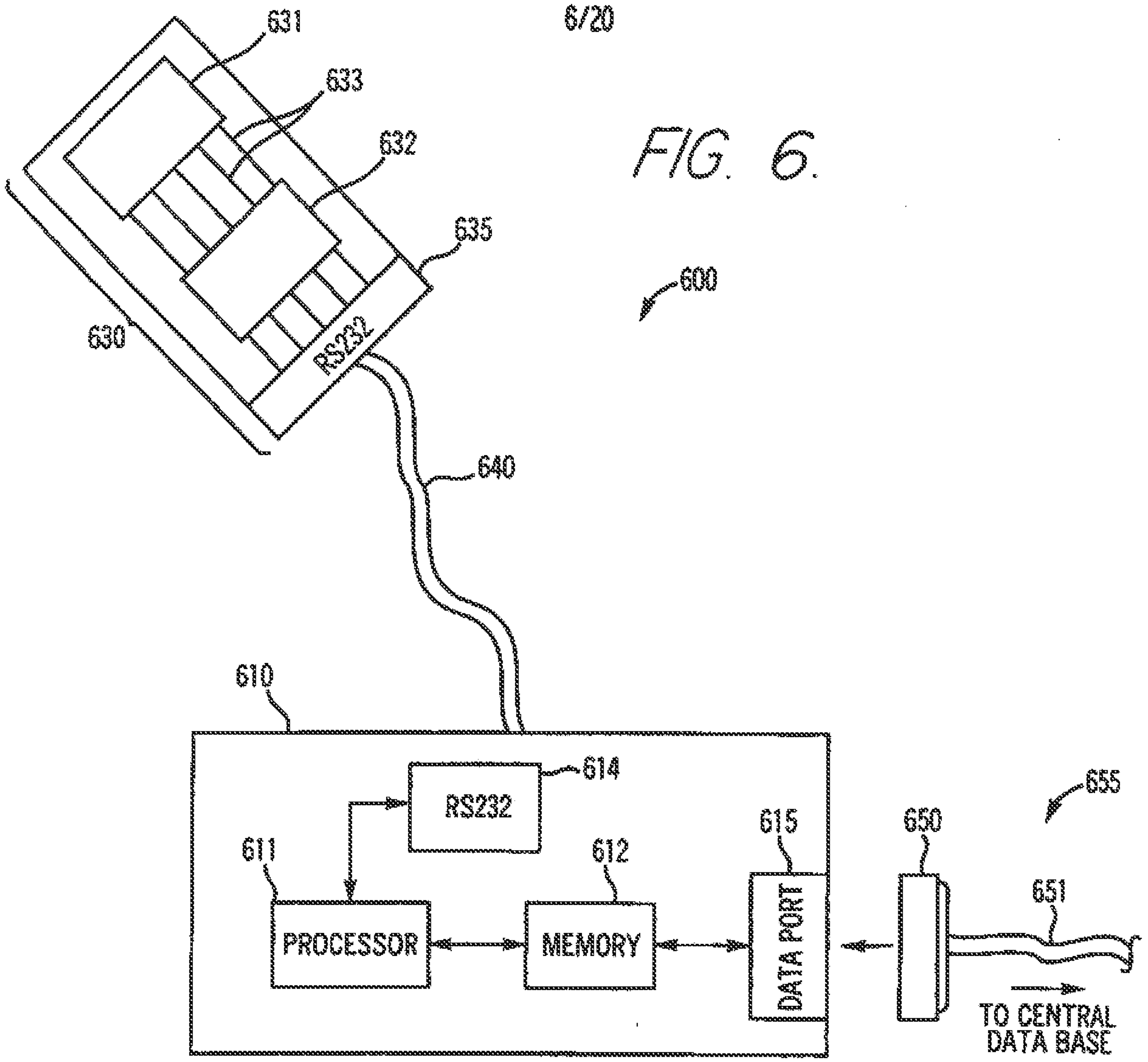
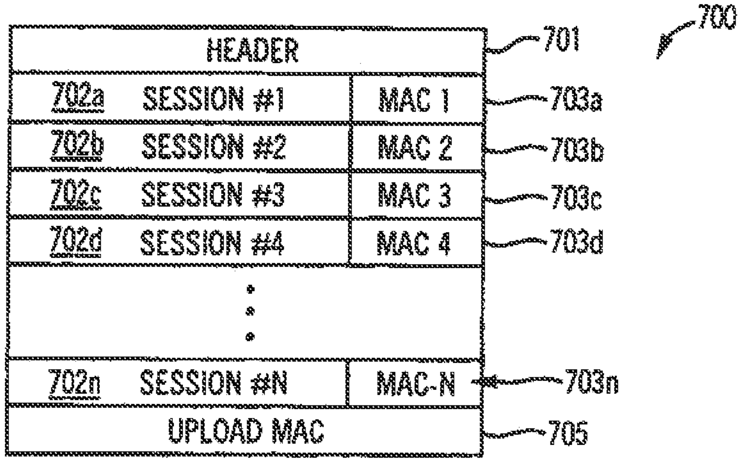


FIG. 7.



TRANSACTION LIST RECORD FORMAT

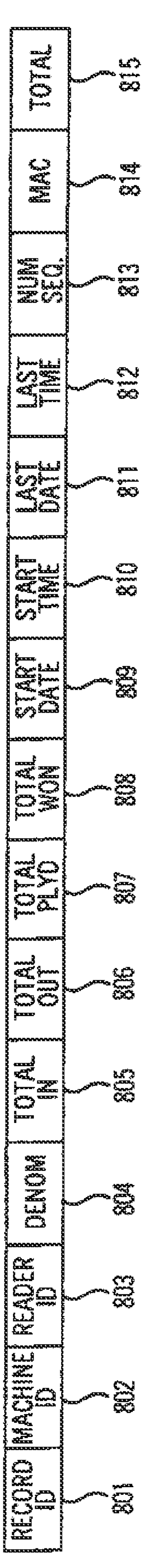


FIG. 8A.

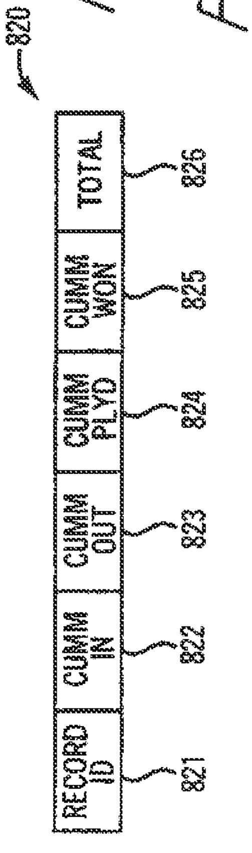


FIG. 8B.

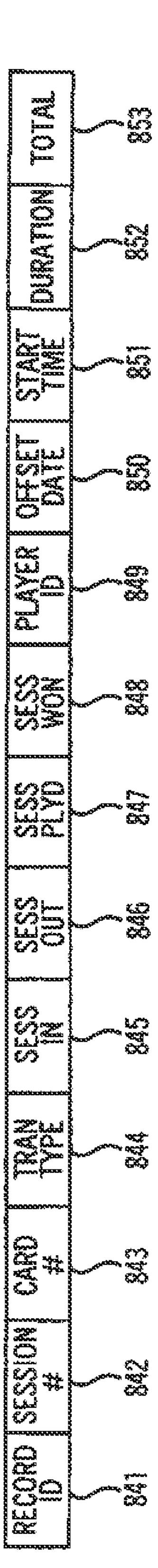


FIG. 8C.

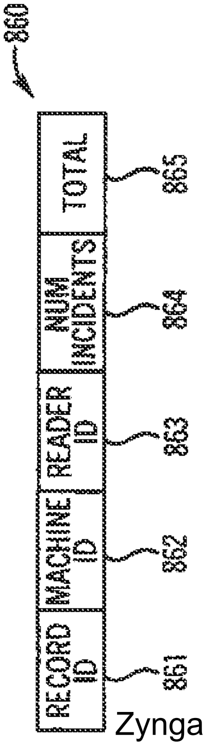


FIG. 8D.

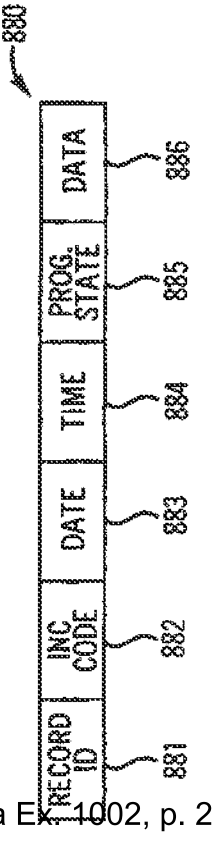


FIG. 8E.

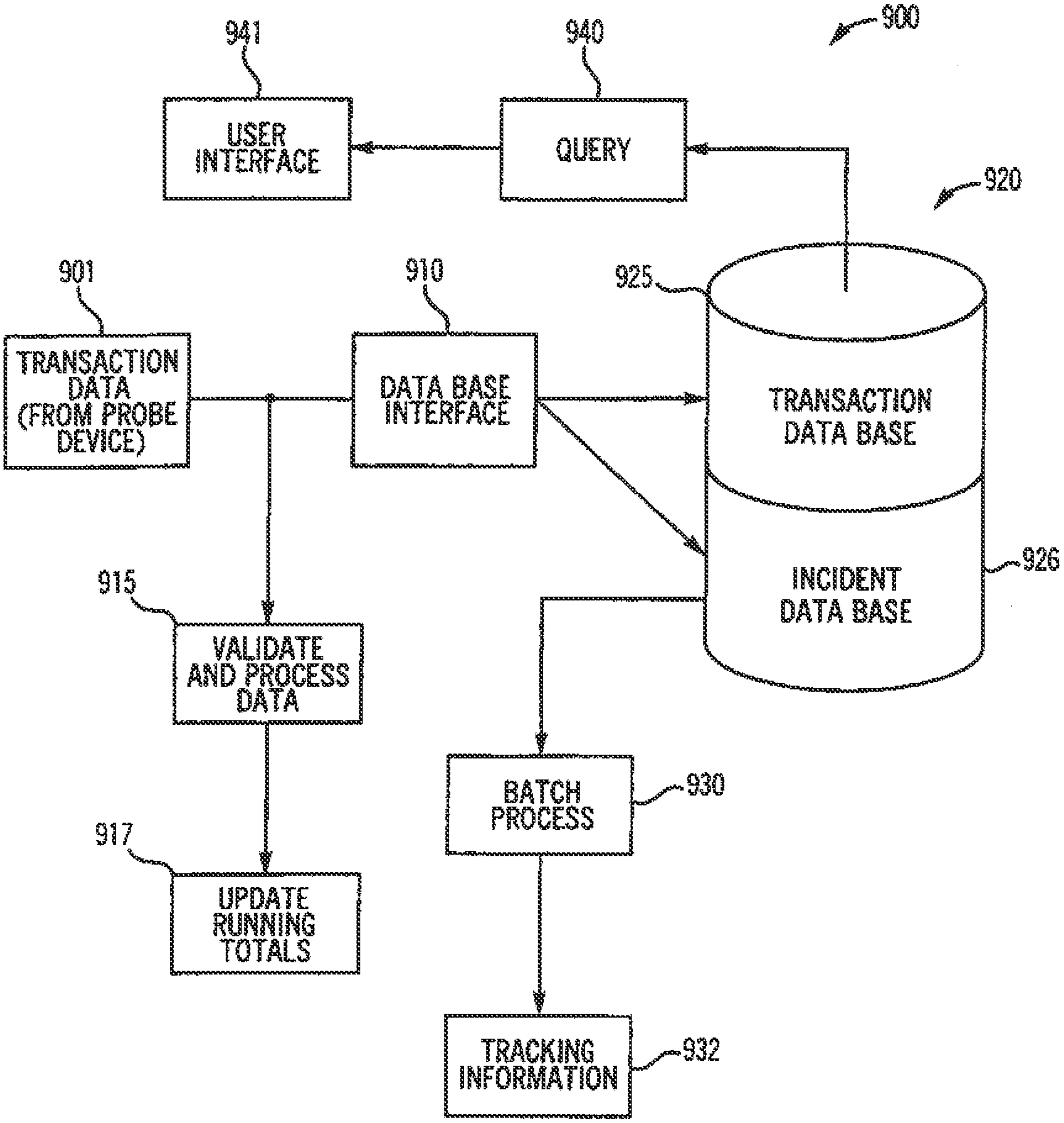

900
941
USER INTERFACE
940
QUERY
920
901
TRANSACTION DATA (FROM PROBE DEVICE)
910
DATA BASE INTERFACE
925
TRANSACTION DATA BASE
INCIDENT DATA BASE
926
915
VALIDATE AND PROCESS DATA
917
UPDATE RUNNING TOTALS
BATCH PROCESS
930
TRACKING INFORMATION
932

FIG. 9.

9/20

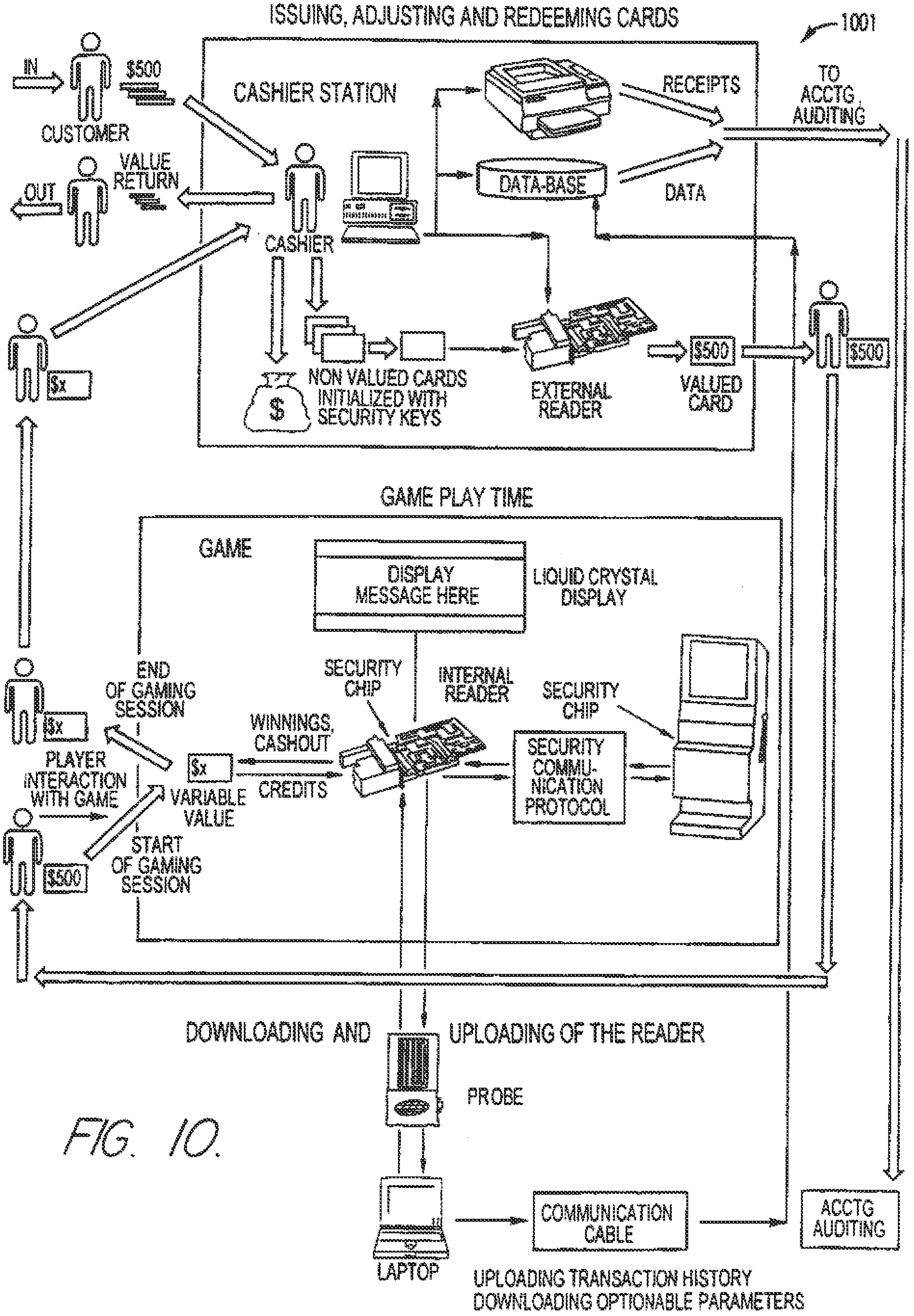

ISSUING, ADJUSTING AND REDEEMING CARDS
1001
IN
$500
CUSTOMER
CASHIER STATION
RECEIPTS
TO ACCTG. AUDITING
VALUE RETURN
OUT
DATA-BASE
DATA
CASHIER
NON VALUED CARDS INITIALIZED WITH SECURITY KEYS
$
EXTERNAL READER
$500
VALUED CARD
$500
$x
GAME PLAY TIME
GAME
DISPLAY MESSAGE HERE
LIQUID CRYSTAL DISPLAY
SECURITY CHIP
INTERNAL READER
SECURITY CHIP
END OF GAMING SESSION
$x
WINNINGS, CASHOUT
SECURITY COMMU-NICATION PROTOCOL
PLAYER INTERACTION WITH GAME
$x
VARIABLE VALUE
CREDITS
START OF GAMING SESSION
$500
DOWNLOADING AND UPLOADING OF THE READER
PROBE
LAPTOP
COMMUNICATION CABLE
ACCTG AUDITING
UPLOADING TRANSACTION HISTORY
DOWNLOADING OPTIONABLE PARAMETERS

FIG. 10.

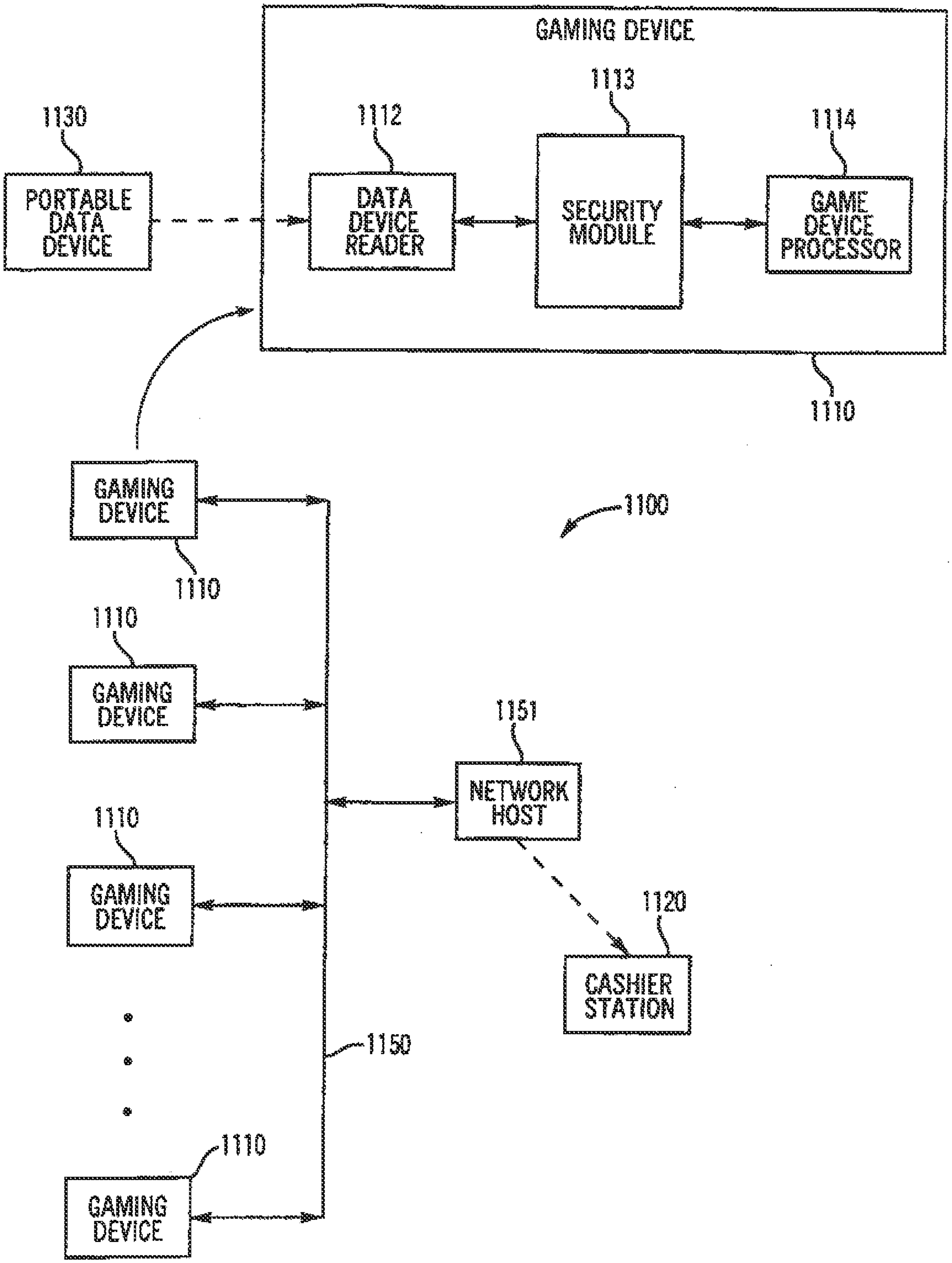

GAMING DEVICE
1130
PORTABLE DATA DEVICE
1112
DATA DEVICE READER
1113
SECURITY MODULE
1114
GAME DEVICE PROCESSOR
1110
GAMING DEVICE
1110
1100
1110
GAMING DEVICE
1110
GAMING DEVICE
1151
NETWORK HOST
1120
CASHIER STATION
1150
1110
GAMING DEVICE

FIG. 11.

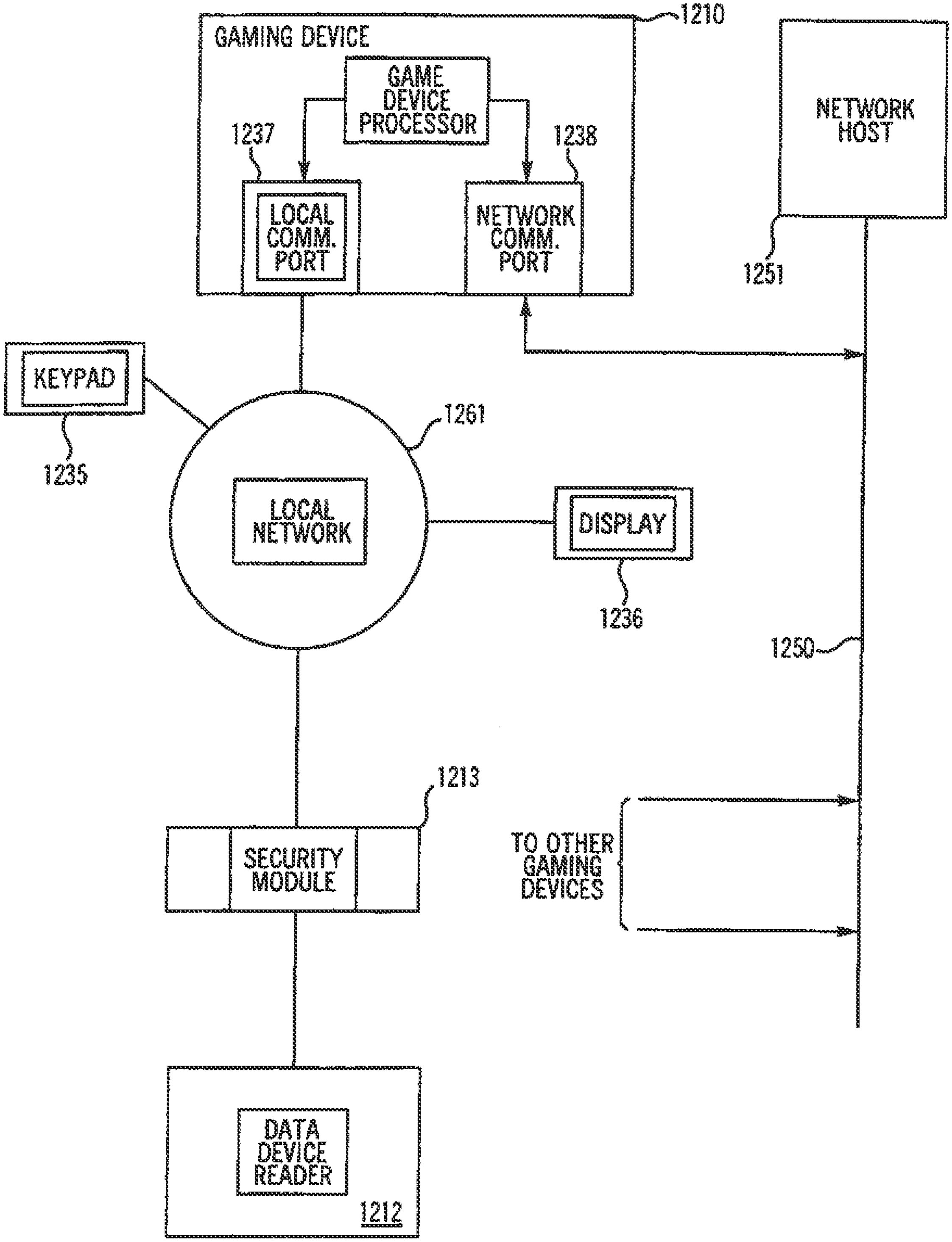

GAMING DEVICE
1210
GAME DEVICE PROCESSOR
1237
1238
LOCAL COMM. PORT
NETWORK COMM. PORT
NETWORK HOST
1251
KEYPAD
1235
1261
LOCAL NETWORK
DISPLAY
1236
1250
1213
SECURITY MODULE
TO OTHER GAMING DEVICES
DATA DEVICE READER
1212

FIG. 12.

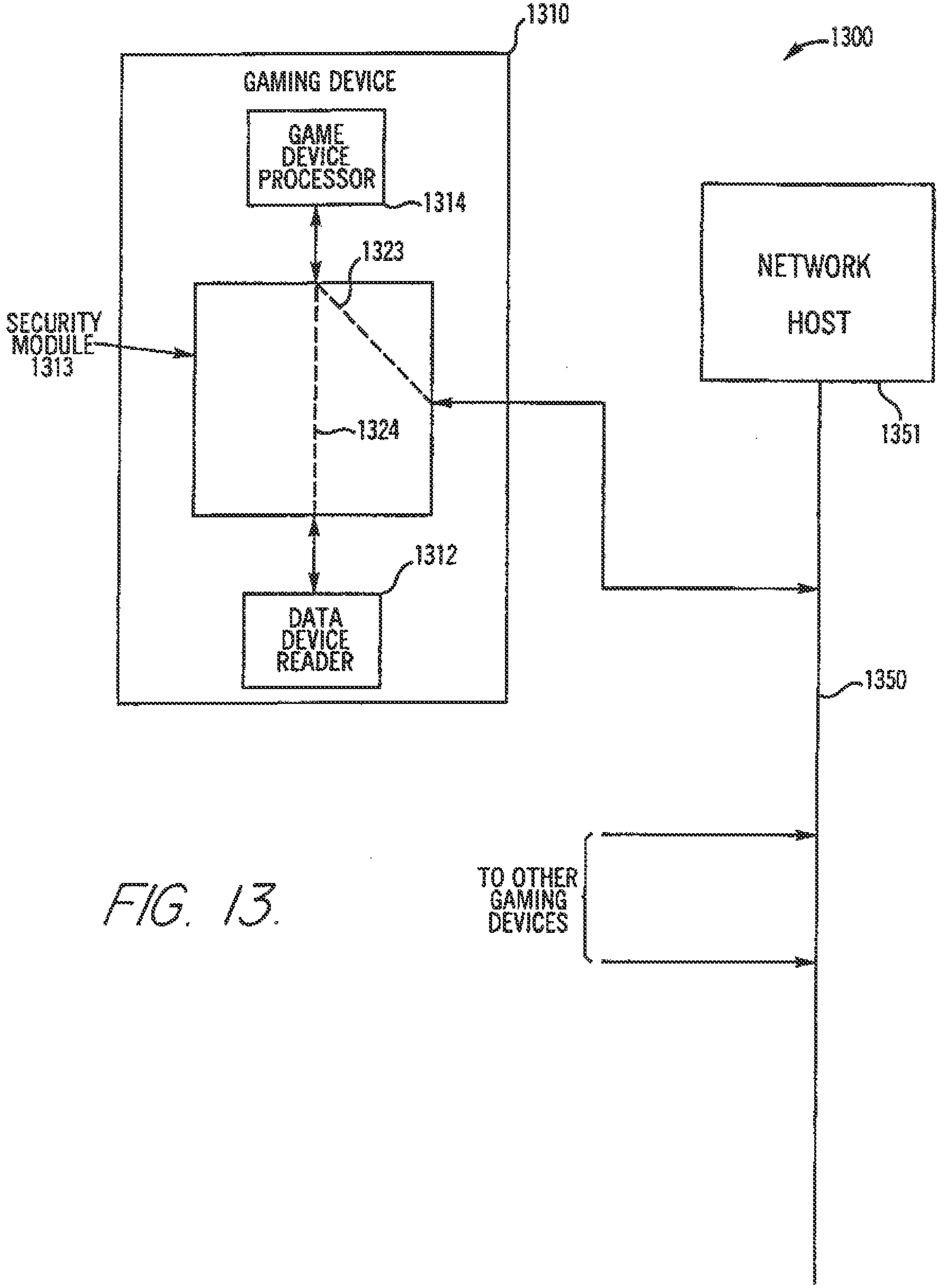

1310
1300
GAMING DEVICE
GAME DEVICE PROCESSOR
1314
1323
SECURITY MODULE 1313
1324
1312
DATA DEVICE READER
NETWORK HOST
1351
1350
TO OTHER GAMING DEVICES

FIG. 13.

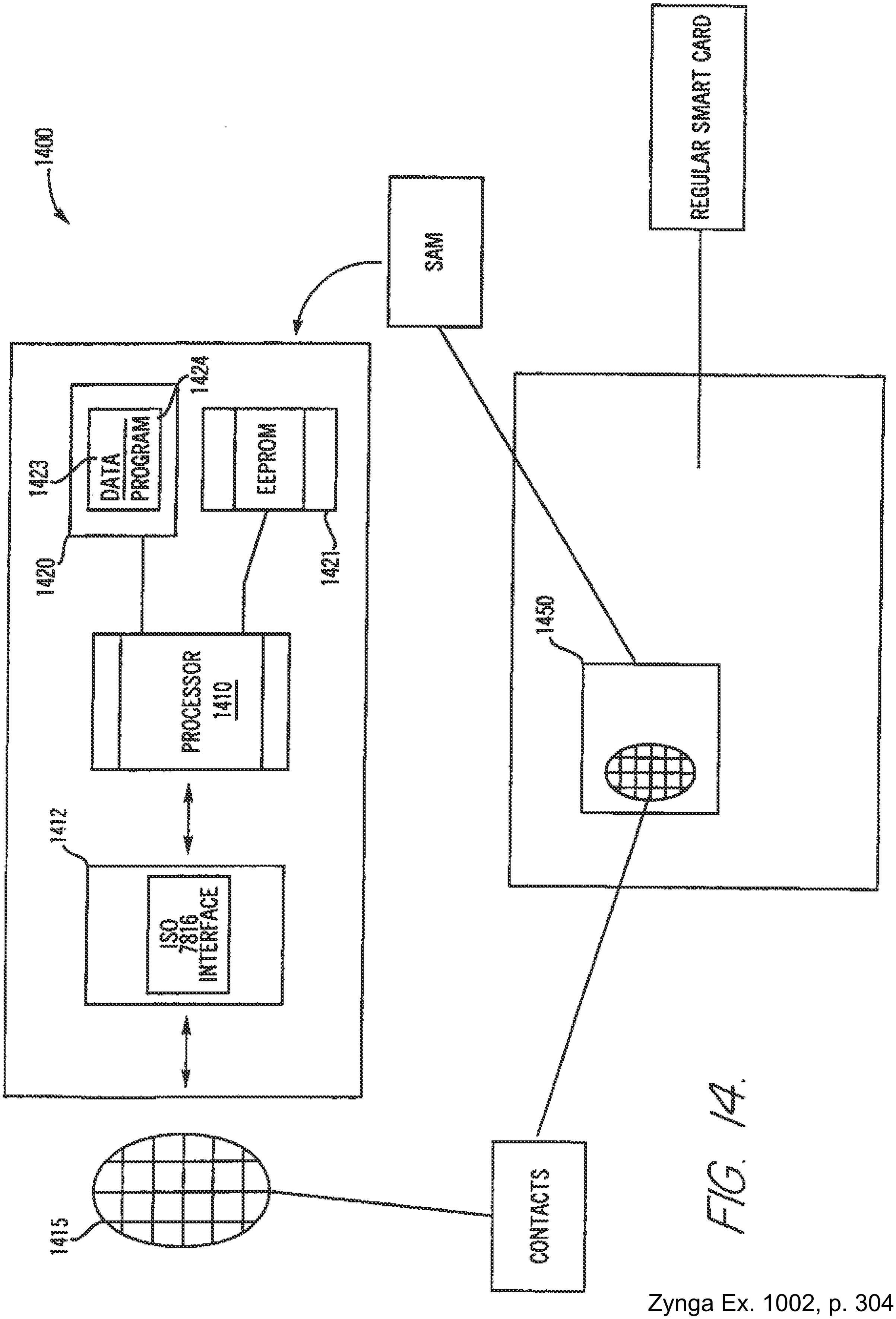
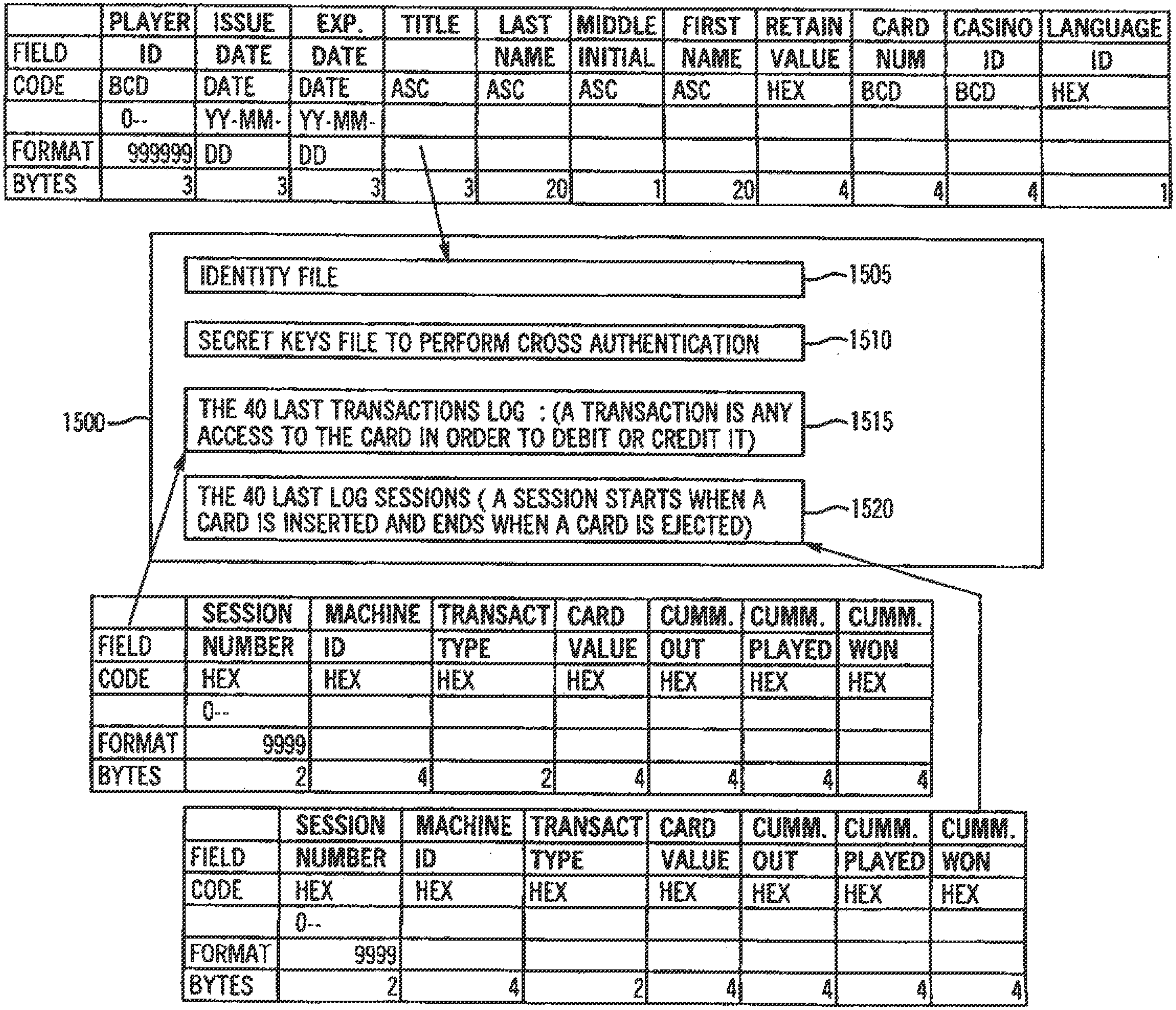

1400
SAM
REGULAR SMART CARD
1424
1423
DATA
PROGRAM
EEPROM
1420
1421
PROCESSOR
1410
1412
ISO
7816
INTERFACE
1450
1415
CONTACTS

FIG. 14.

USER CARD MAPPING



	PLAYER	ISSUE	EXP.	TITLE	LAST	MIDDLE	FIRST	RETAIN	CARD	CASINO	LANGUAGE
FIELD	ID	DATE	DATE		NAME	INITIAL	NAME	VALUE	NUM	ID	ID
CODE	BCD	DATE	DATE	ASC	ASC	ASC	ASC	HEX	BCD	BCD	HEX
	0--	YY-MM-	YY-MM-								
FORMAT	999999	DD	DD								
BYTES	3	3	3	3	20	1	20	4	4	4	1

IDENTITY FILE

SECRET KEYS FILE TO PERFORM CROSS AUTHENTICATION

THE 40 LAST TRANSACTIONS LOG : (A TRANSACTION IS ANY ACCESS TO THE CARD IN ORDER TO DEBIT OR CREDIT IT)

THE 40 LAST LOG SESSIONS (A SESSION STARTS WHEN A CARD IS INSERTED AND ENDS WHEN A CARD IS EJECTED)

	SESSION	MACHINE	TRANSACT	CARD	CUMM.	CUMM.	CUMM.
FIELD	NUMBER	ID	TYPE	VALUE	OUT	PLAYED	WON
CODE	HEX	HEX	HEX	HEX	HEX	HEX	HEX
	0--						
FORMAT	9999						
BYTES	2	4	2	4	4	4	4

	SESSION	MACHINE	TRANSACT	CARD	CUMM.	CUMM.	CUMM.
FIELD	NUMBER	ID	TYPE	VALUE	OUT	PLAYED	WON
CODE	HEX	HEX	HEX	HEX	HEX	HEX	HEX
	0--						
FORMAT	9999						
BYTES	2	4	2	4	4	4	4

FIG. 15.

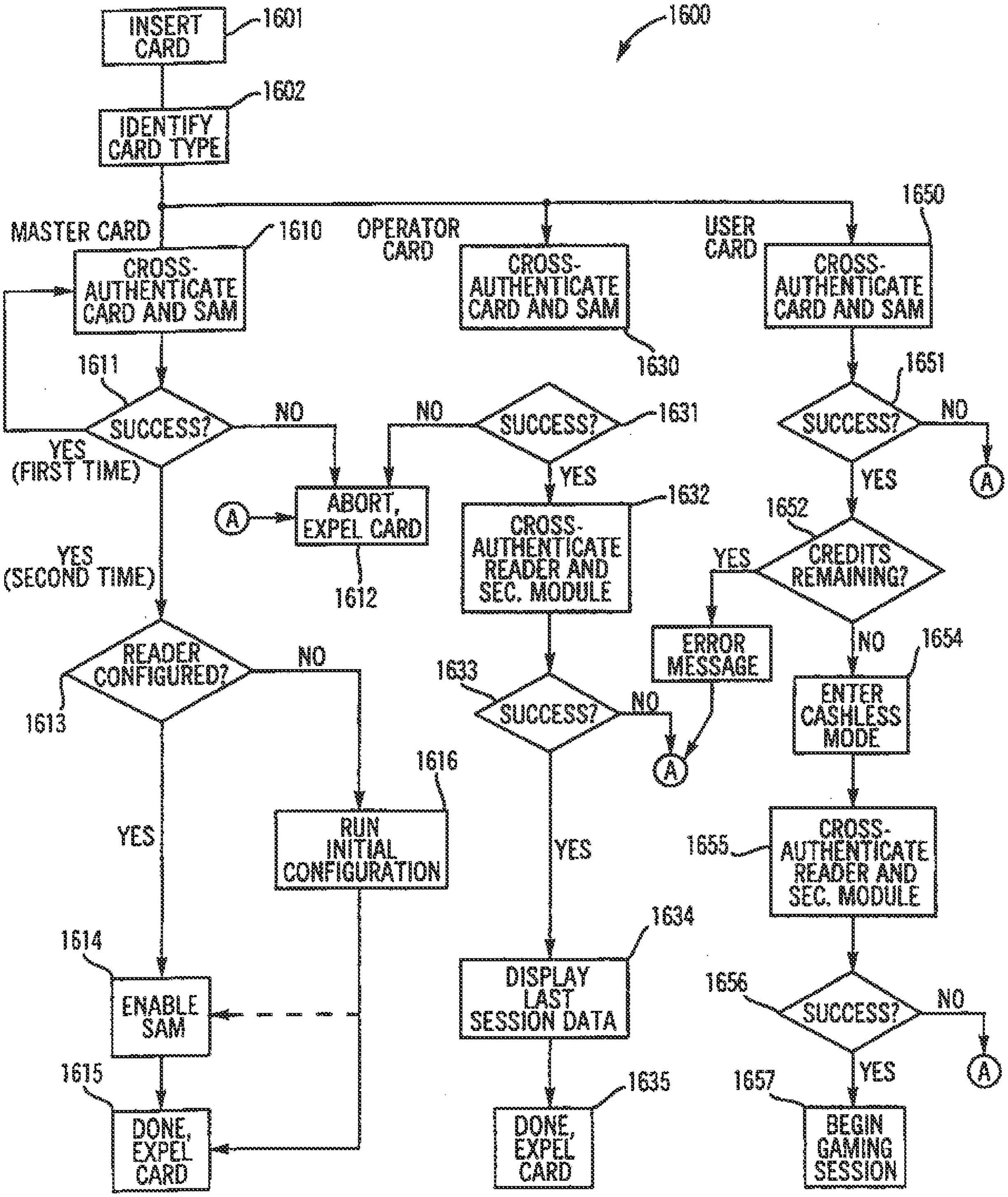

1600
INSERT CARD
1601
IDENTIFY CARD TYPE
1602
MASTER CARD
OPERATOR CARD
USER CARD
1650
CROSS-AUTHENTICATE CARD AND SAM
1610
CROSS-AUTHENTICATE CARD AND SAM
1630
CROSS-AUTHENTICATE CARD AND SAM
1611
SUCCESS?
NO
YES (FIRST TIME)
YES (SECOND TIME)
NO
SUCCESS?
1631
YES
1651
SUCCESS?
NO
YES
A
A
ABORT, EXPEL CARD
1612
CROSS-AUTHENTICATE READER AND SEC. MODULE
1632
1652
YES
CREDITS REMAINING?
NO
ERROR MESSAGE
1654
ENTER CASHLESS MODE
READER CONFIGURED?
NO
1613
1633
SUCCESS?
NO
A
YES
1616
RUN INITIAL CONFIGURATION
YES
1655
CROSS-AUTHENTICATE READER AND SEC. MODULE
1634
DISPLAY LAST SESSION DATA
1614
ENABLE SAM
1656
SUCCESS?
NO
YES
A
1615
DONE, EXPEL CARD
1635
DONE, EXPEL CARD
1657
BEGIN GAMING SESSION

FIG. 16.

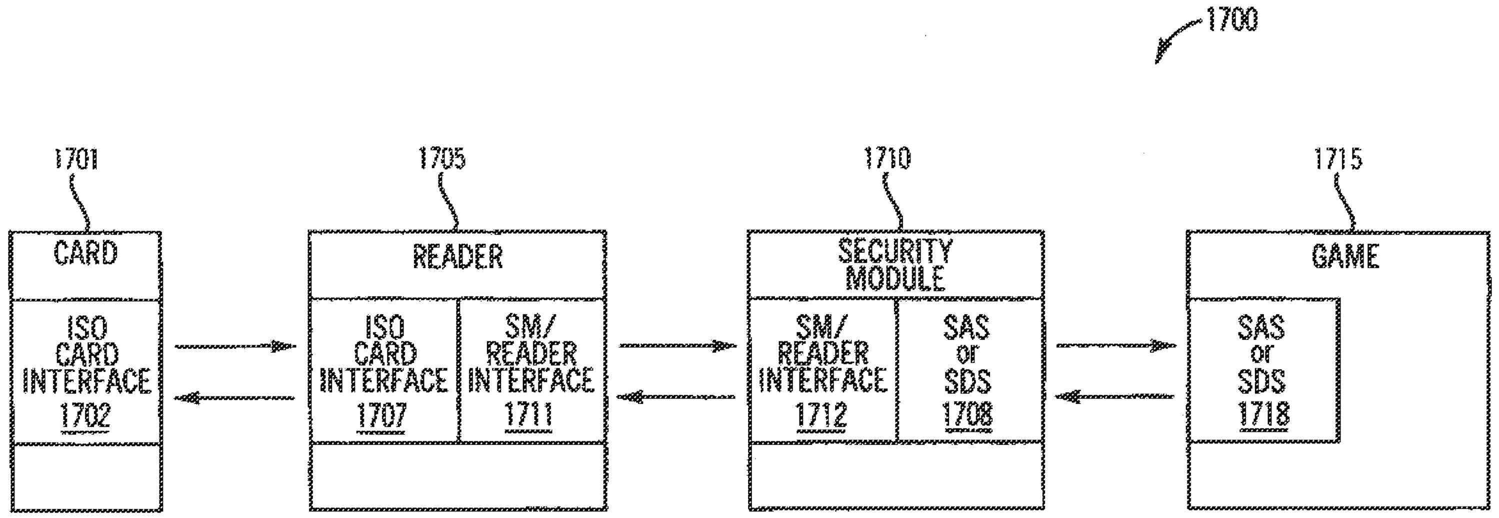

1700
1701
CARD
ISO CARD INTERFACE 1702
1705
READER
ISO CARD INTERFACE 1707
SM/ READER INTERFACE 1711
1710
SECURITY MODULE
SM/ READER INTERFACE 1712
SAS or SDS 1708
1715
GAME
SAS or SDS 1718

FIG. 17.

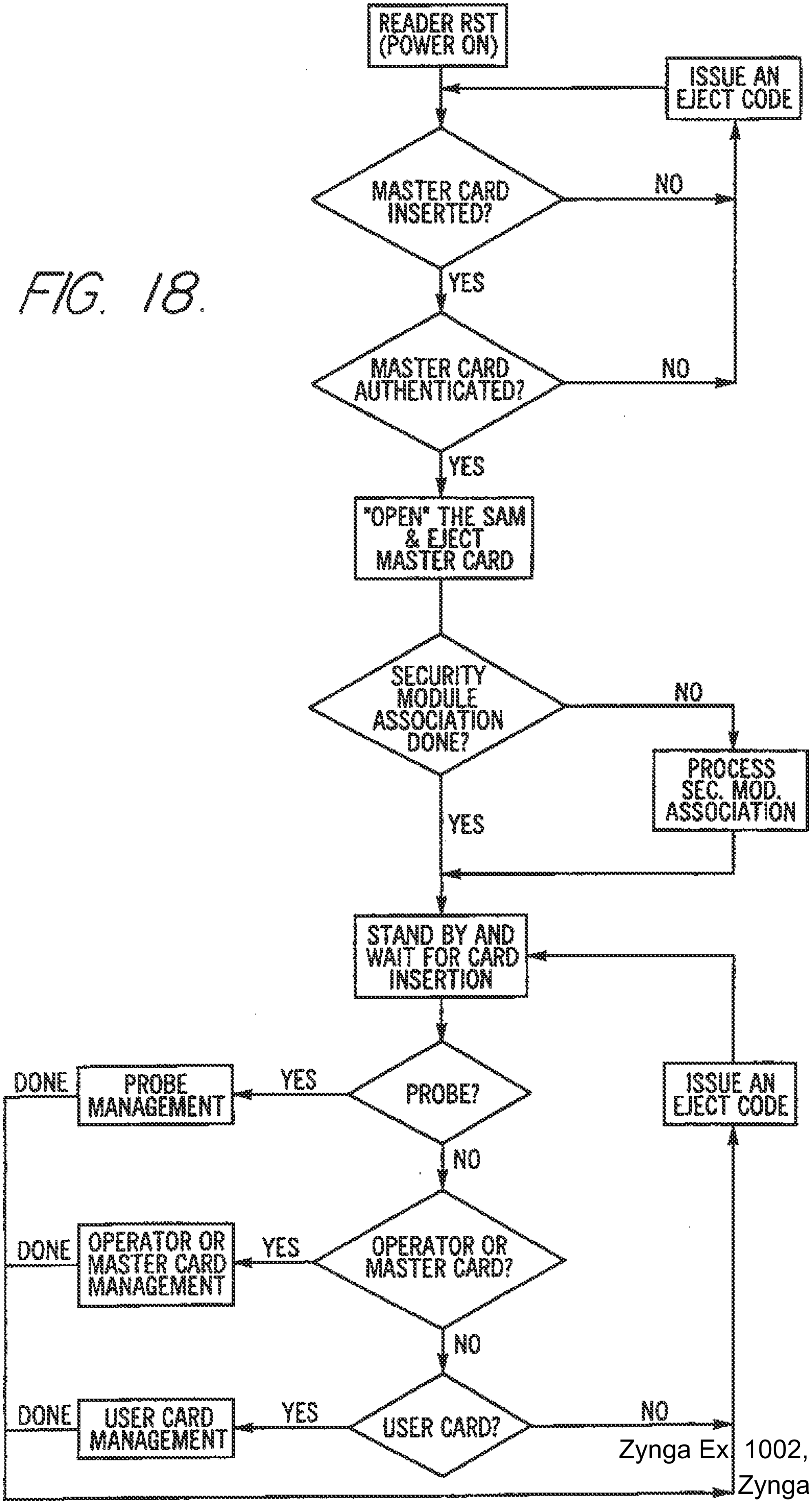

READER RST (POWER ON)
ISSUE AN EJECT CODE
MASTER CARD INSERTED?
NO
YES
MASTER CARD AUTHENTICATED?
NO
YES
"OPEN" THE SAM & EJECT MASTER CARD
SECURITY MODULE ASSOCIATION DONE?
NO
PROCESS SEC. MOD. ASSOCIATION
YES
STAND BY AND WAIT FOR CARD INSERTION
DONE
PROBE MANAGEMENT
YES
PROBE?
ISSUE AN EJECT CODE
NO
DONE
OPERATOR OR MASTER CARD MANAGEMENT
YES
OPERATOR OR MASTER CARD?
NO
DONE
USER CARD MANAGEMENT
YES
USER CARD?
NO

FIG. 18.

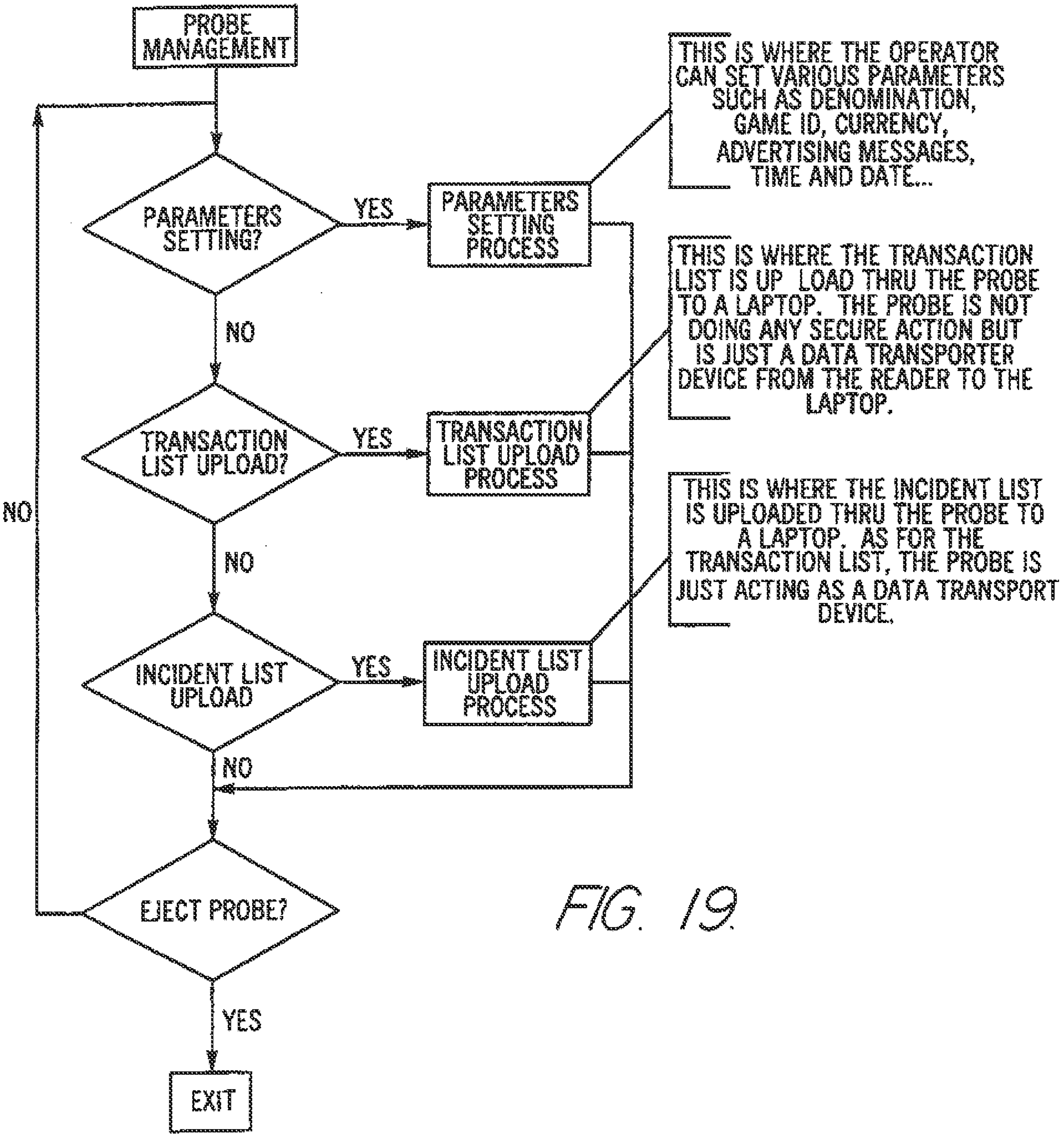

PROBE MANAGEMENT
PARAMETERS SETTING?
YES
PARAMETERS SETTING PROCESS
THIS IS WHERE THE OPERATOR CAN SET VARIOUS PARAMETERS SUCH AS DENOMINATION, GAME ID, CURRENCY, ADVERTISING MESSAGES, TIME AND DATE...
NO
TRANSACTION LIST UPLOAD?
YES
TRANSACTION LIST UPLOAD PROCESS
THIS IS WHERE THE TRANSACTION LIST IS UP LOAD THRU THE PROBE TO A LAPTOP. THE PROBE IS NOT DOING ANY SECURE ACTION BUT IS JUST A DATA TRANSPORTER DEVICE FROM THE READER TO THE LAPTOP.
NO
NO
INCIDENT LIST UPLOAD
YES
INCIDENT LIST UPLOAD PROCESS
THIS IS WHERE THE INCIDENT LIST IS UPLOADED THRU THE PROBE TO A LAPTOP. AS FOR THE TRANSACTION LIST, THE PROBE IS JUST ACTING AS A DATA TRANSPORT DEVICE.
NO
EJECT PROBE?
YES
EXIT

FIG. 19.

FIG. 20.

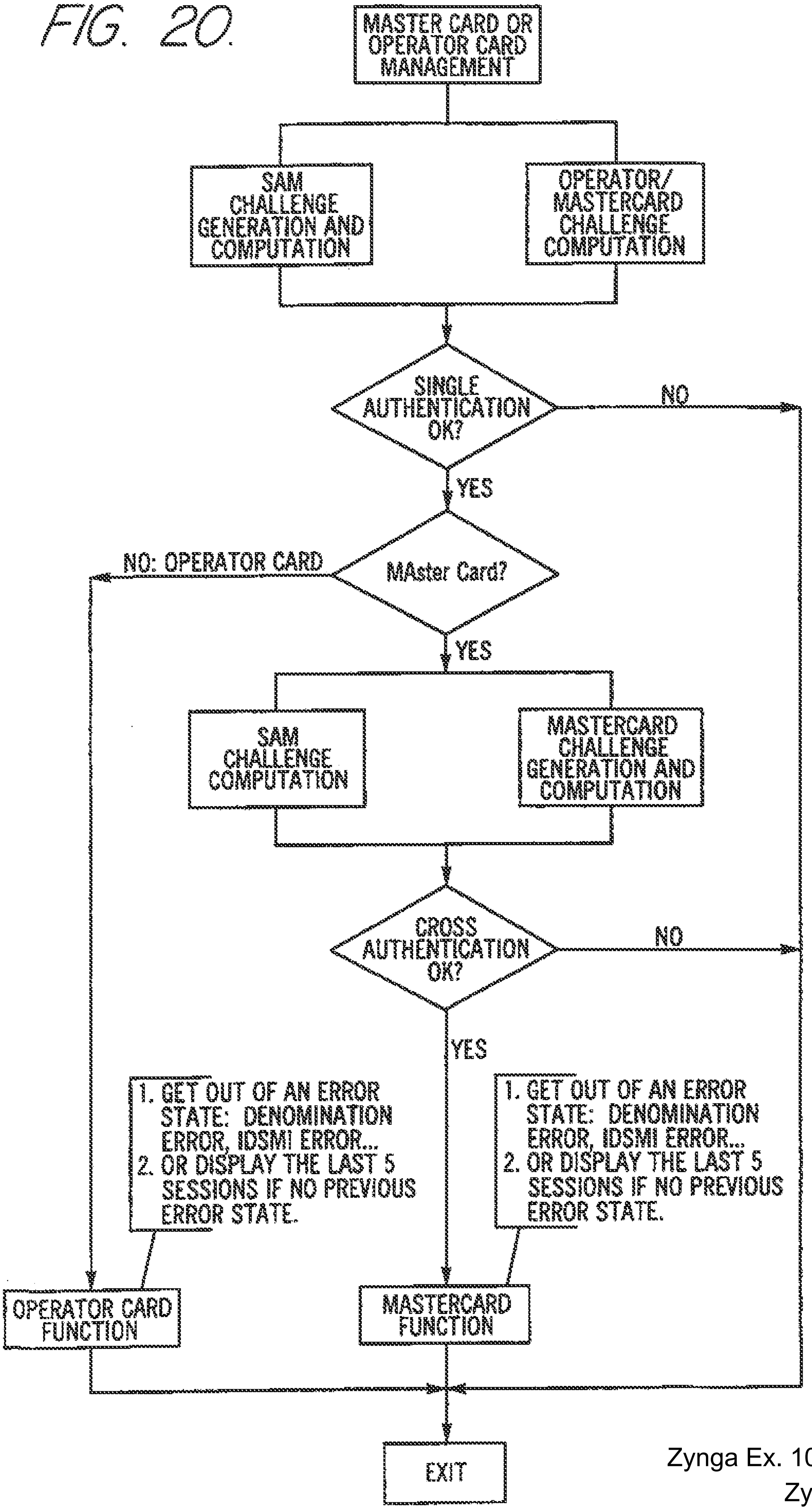
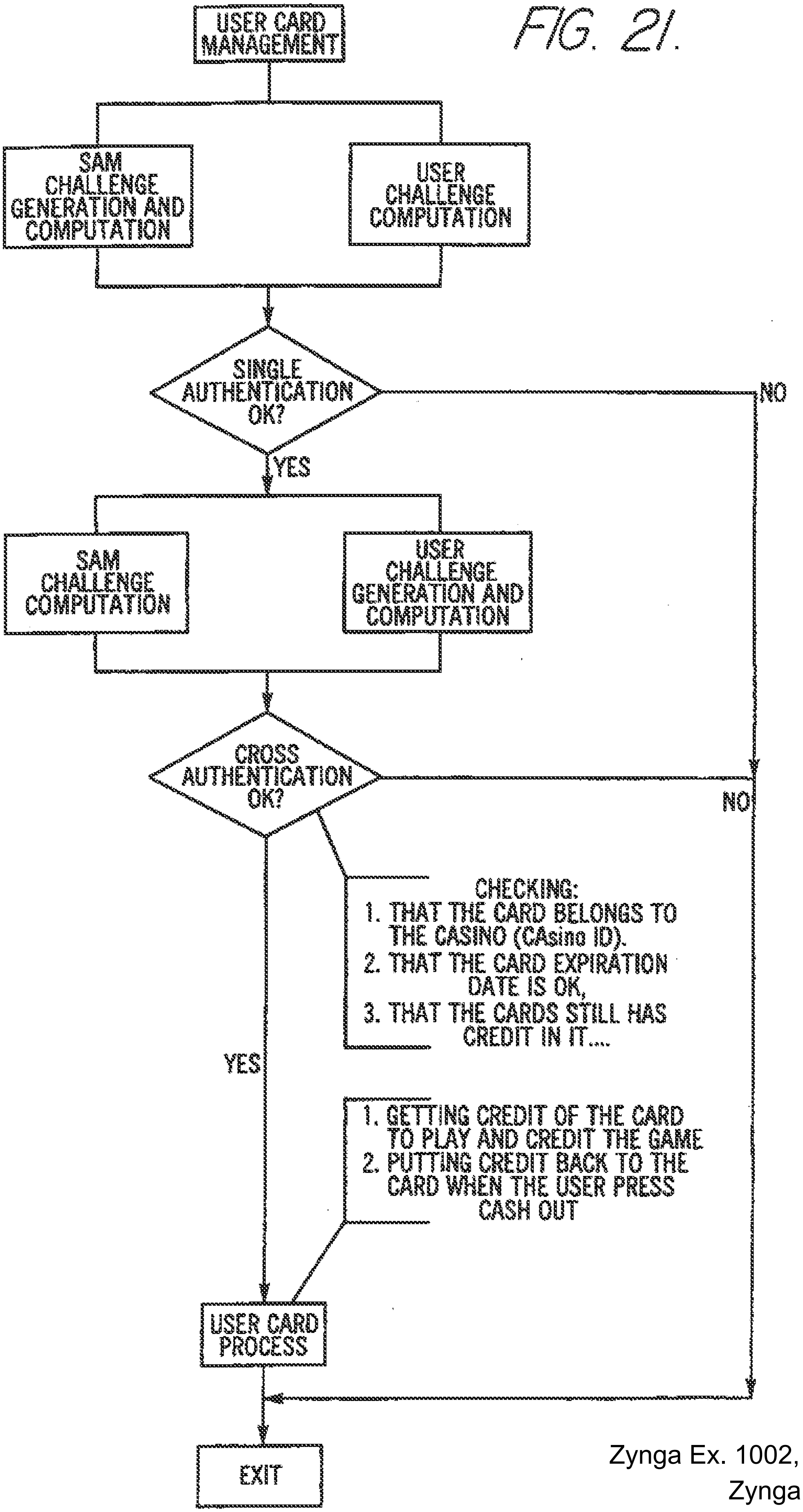

MASTER CARD OR OPERATOR CARD MANAGEMENT
SAM CHALLENGE GENERATION AND COMPUTATION
OPERATOR/ MASTERCARD CHALLENGE COMPUTATION
SINGLE AUTHENTICATION OK?
NO
YES
NO: OPERATOR CARD
MAster Card?
YES
SAM CHALLENGE COMPUTATION
MASTERCARD CHALLENGE GENERATION AND COMPUTATION
CROSS AUTHENTICATION OK?
NO
YES
1. GET OUT OF AN ERROR STATE: DENOMINATION ERROR, IDSMI ERROR...
2. OR DISPLAY THE LAST 5 SESSIONS IF NO PREVIOUS ERROR STATE.
1. GET OUT OF AN ERROR STATE: DENOMINATION ERROR, IDSMI ERROR...
2. OR DISPLAY THE LAST 5 SESSIONS IF NO PREVIOUS ERROR STATE.
OPERATOR CARD FUNCTION
MASTERCARD FUNCTION
EXIT

FIG. 21.


USER CARD MANAGEMENT
SAM CHALLENGE GENERATION AND COMPUTATION
USER CHALLENGE COMPUTATION
SINGLE AUTHENTICATION OK?
NO
YES
SAM CHALLENGE COMPUTATION
USER CHALLENGE GENERATION AND COMPUTATION
CROSS AUTHENTICATION OK?
NO
CHECKING:
1. THAT THE CARD BELONGS TO THE CASINO (CAsino ID).
2. THAT THE CARD EXPIRATION DATE IS OK,
3. THAT THE CARDS STILL HAS CREDIT IN IT....
YES
1. GETTING CREDIT OF THE CARD TO PLAY AND CREDIT THE GAME
2. PUTTING CREDIT BACK TO THE CARD WHEN THE USER PRESS CASH OUT
USER CARD PROCESS
EXIT

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	
Examiner Name	
Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-20
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		CYBS5805CIP

	1	W3C, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) W3C Recommendation 27 April 2007"; http://www.w3.org/TR/REC-soap12-part1-20070427/.	□
	2	BizTalk Labs, "BizTalk Services and Internet Service Bus Technologies."	□
	3	BizTalk Labs, "BizTalk Connectivity Serices."	□
	4	Object Management Group, "CORBA BASICS."	□
	5	Wilkipedia, "RSS."	□
	6	Microsoft Corporation, msdn, "What is Windows Communication Foundation?" 2007.	□
	7	XML-RPC.Com, "simple cross-platform distributed computing, based on the standards of the Internet. XML-RPC Specification."	□
	8	International Search Report mailed February 26, 2003, in related International Application No. PCT/US02/37537, filed November 22, 2002.	□
	9	Written Opinion mailed August 28, 2003, in related International Application No. PCT/US02/37537, filed November 22, 2002.	□
	10	International Preliminary Examination Report mailed February17, 2004, in related International Application No. PCT/US02/37537, filed November 22, 2002.	□
	11	International Search Report mailed February 25, 2003, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	Thierry Brunet de Courssou
	Art Unit	
	Examiner Name	
	Attorney Docket Number	CYBS5805CIP

	12	Written Opinion mailed September 4, 2003, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□
	13	International Preliminary Examination Report mailed February 11, 2004, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□
	14	International Search Report mailed January 30, 2003, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	15	Written Opinion mailed August 27, 2003, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	16	International Preliminary Examination Report mailed August 12, 2004, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	17	International Search Report mailed February 28, 2003, in related International Application No. PCT/US02/37538, filed November 22, 2002.	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	2109364
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	21-AUG-2007
Filing Date:	
Time Stamp:	20:41:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	**Document Description**	**File Name**	File Size(Bytes) /Message Digest	**Multi Part /.zip**	**Pages (if appl.)**
1		5805CIPIDS1A.pdf	14505848 df7191bbf4d1313b4d339bd85e2d24fcf83c9441	yes	156

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed	1	7
	Foreign Reference	8	24
	Foreign Reference	25	27
	Foreign Reference	28	41
	Foreign Reference	42	47
	Foreign Reference	48	63
	Foreign Reference	64	70
	Foreign Reference	71	78
	Foreign Reference	79	90
	Foreign Reference	91	93
	Foreign Reference	94	131
	Foreign Reference	132	156

Warnings:

Information:

2		5805CIPIDS1B.pdf	15035965 33d98412cafe57b03244c35b6cc4d9af1acab7ce	yes	79

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed	1	2
	Foreign Reference	3	64
	NPL Documents	65	70
	NPL Documents	71	73
	NPL Documents	74	75

	NPL Documents	76	77
	NPL Documents	78	79

Warnings:

Information:

3		5805CIPIDS1C.pdf	8548761 3bbf07bffea06f122914cabd1d568160152f6116	yes	164

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed	1	3
	NPL Documents	4	76
	NPL Documents	77	78
	NPL Documents	79	80
	NPL Documents	81	86
	NPL Documents	87	102
	NPL Documents	103	108
	NPL Documents	109	115
	NPL Documents	116	118
	NPL Documents	119	123
	NPL Documents	124	128
	NPL Documents	129	131
	NPL Documents	132	135
	NPL Documents	136	138
	NPL Documents	139	141
	NPL Documents	142	146

	NPL Documents	147	151
	NPL Documents	152	154
	NPL Documents	155	159
	NPL Documents	160	164
Warnings:			
Information:			
	Total Files Size (in bytes):	38090574	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

8/21/07

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

11/842,147

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY			OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))				75			
SEARCH FEE (37 CFR 1.16(k), (i), or (m))				250			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))				100			
TOTAL CLAIMS (37 CFR 1.16(i))	41 minus 20 =	21	X 25=	525	OR	X 50=	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	1	X 100=	100		X 200=	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A			N/A	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1050		TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT A		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

OR

AMENDMENT B		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)		RATE ($)	ADDI-TIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **GAME TALK SERVICE BUS**, and for which an Application for United States Letters Patent was filed in the United States Patent and Trademark Office on August 20, 2007, as application Serial No. 11/842,147.

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

This application discloses and claims subject matter from application Serial No. 10/120,635, filed April 10, 2002.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37 of the Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent.

I hereby claim foreign priority benefits under Title 35 of the United States Code, Section 119(a)-(d), on any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority Claimed

______ (Number) ______ (Country) ______ (Day/Month/Year Filed) ______ Yes ______ No

I hereby claim benefit under Title 35 of the United States Code, Section 119(e) of United States provisional application Serial No. ________, filed ________________.

I hereby claim benefit under Title 35 of the United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 of the United States Code, Section 112:

10/120,635 (Application Number) April 20, 2002 (Filing Date) pending (Status - patented, pending, abandoned)

The undersigned hereby authorizes the U.S. attorney or agent named herein to accept and follow instructions as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney or agent and the undersigned.

In the event of a change in the persons from whom instructions may be taken, the U.S. attorney or agent named herein will be so notified by the undersigned.

As a named inventor, I hereby appoint Alan W. Young, Registration No. 37,970, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Address all communications to **Alan W. Young** at YOUNG LAW FIRM, P.C., 4370 Alpine Rd., Ste. 106, Portola Valley, CA 94028.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

First and Joint Inventor Name: Thierry Brunet de Courssou

Residence Address: 975 Seven Hills Dr., Apt. 1317, Henderson, NV 89052, US

Post Office Address: (same as above)

Citizenship: France

Signature: ______________ Date: **August 30, 2007**

Electronic Patent Application Fee Transmittal

Application Number:	11842147
Filing Date:	
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Filer:	Alan W. Young/Nita Miller
Attorney Docket Number:	CYBS5805CIP

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	65

Electronic Acknowledgement Receipt

EFS ID:	2145679
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	30-AUG-2007
Filing Date:	
Time Stamp:	22:13:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$65
RAM confirmation Number	6310
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/Message Digest	Multi Part /.zip	Pages (if appl.)

1	Oath or Declaration filed	5805CIPSIGNEDDECL.pdf	63774 945ff227698 66c37ea03d3a2ae22f7e26336db0e	no	2
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8142 45b408d60c15950eded971b5a089d3e59ece6942	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	71916	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/842,147	08/21/2007	3711	1115	CYBS5805CIP	41	4

CONFIRMATION NO. 2880

22430
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY, CA94028

FILING RECEIPT

Date Mailed: 09/04/2007

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Thierry Brunet de Courssou, Henderson, NV;

Assignment For Published Patent Application

CYBERVIEW TECHNOLOGY, INC., Palo Alto, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CIP of 10/120,635 04/10/2002
which claims benefit of 60/332,593 11/23/2001

Foreign Applications

If Required, Foreign Filing License Granted: 08/31/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US11/842,147**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

GAME TALK SERVICE BUS

Preliminary Class

273

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under

37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/842,147	08/21/2007	3711	1115	CYBS5805CIP	41	4

CONFIRMATION NO. 2880

UPDATED FILING RECEIPT

22430
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY, CA94028

Date Mailed: 09/04/2007

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Thierry Brunet de Courssou, Henderson, NV;

Assignment For Published Patent Application

CYBERVIEW TECHNOLOGY, INC., Palo Alto, CA

Power of Attorney:
Alan Young--37970

Domestic Priority data as claimed by applicant

This application is a CIP of 10/120,635 04/10/2002
which claims benefit of 60/332,593 11/23/2001

Foreign Applications

If Required, Foreign Filing License Granted: 08/31/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US11/842,147**

Projected Publication Date: 12/13/2007

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

GAME TALK SERVICE BUS

Preliminary Class

273

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP

CONFIRMATION NO. 2880

FORMALITIES LETTER

22430
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY, CA 94028

Date Mailed: 09/04/2007

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required. Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*

Replies should be mailed to:
Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199
PART 3 - OFFICE COPY

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Thierry BRUNET DE COURSSOU

Serial No.: 11,842,147

Filed: August 20, 2007

For: **GAME TALK SERVICE BUS**

Atty. Docket No.: CYBS5805CIP

Examiner:

Art Unit: 3711

Confirmation No.: 2880

Customer No.: 22430

Total Pages: 2

NOTICE OF LOSS OF ENTITLEMENT TO SMALL ENTITY STATUS AND PAYMENT OF DEFICIENCY OWED

CERTIFICATE OF FACSIMILE TRANSMISSION UNDER 37 CFR §1.8

I hereby certify that this document and the documents referred to herein are being transmitted by facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, at 571-273-8300, on September 17, 2007.

Nita J. Miller

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants hereby give notice under 37 C.F.R. §1.27(g)(2) of their loss of entitlement to small entity status. Attached hereto is a form PTO-2038 authorizing payment of the deficiency owed pursuant to 37 C.F.R. § 1.28(c)(2), calculated as follows:

Fee Type / Date Paid	Fee Paid In Error	Current Fee	Deficiency
Utility search / August 20, 2007	$250.00	$500.00	$250.00
Utility examination / August 20, 2007	$100.00	$200.00	$100.00
Independent claims / August 20, 2007	$100.00	$200.00	$100.00
TOTAL	$450.00	$900.00	**$450.00**

Respectfully submitted,

Date: September 17, 2007

By:
Alan W. Young
Attorney for Applicants
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\yl\CLIENTS\JMG\CYBS\5805\CIP\5805CIP NOTICE.doc

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:	)	Examiner:
Thierry BRUNET DE COURSSOU	)	Art Unit: 3711
Application No.: 11,842,147	)	Confirmation No.: 2880
Filed: August 20, 2007	)	Customer No.: 22430
For: **GAME TALK SERVICE BUS**	)	
Atty. Docket No.: CYBS5805CIP	)	**PRELIMINARY AMENDMENT**

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Please amend the above application as indicated below.

Amendments to the **Specification** begin on page **2** of this paper.

Remarks begin on page **3** of this paper.

IN THE SPECIFICATION:

Please amend paragraph **[0001]** as follows:

[0001] This **application is related in subject matter to** ~~**is a continuation-in part of application Serial**~~ **Application** No. 10/120,635, filed April 10, 2002, ~~**which claims the benefit under 35 U.S.C. §119(e) of provisional application Serial No. 60/332,593, filed November 23, 2001, both applications of which are**~~ **which application is** hereby incorporated herein by reference in **its entirety** ~~**their entireties**~~.

REMARKS

This Preliminary Amendment is being filed for the purposes of disclaiming priority under 35 U.S.C. §1.20. Submitted herewith in support thereof are a *Supplemental Declaration and Power of Attorney* and a *Supplemental Application Data Sheet.*

Applicants believe that this application is now in condition for examination. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,

Date: October 29, 2007

By:______________________
Alan W. Young
Attorney for Applicants
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\JMG\CYBS\5805\CIP\5805CIP PRELIM AMEND.doc

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **GAME TALK SERVICE BUS**, and for which an Application for United States Letters Patent was filed in the United States Patent and Trademark Office on August 20, 2007, as application Serial No. 11/842,147.

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37 of the Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent.

I hereby claim foreign priority benefits under Title 35 of the United States Code, Section 119(a)-(d), on any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

			Priority Claimed	
____________	____________	____________	______	______
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim benefit under Title 35 of the United States Code, Section 119(e) of United States provisional application Serial No. _________, filed ________________________.

I hereby claim benefit under Title 35 of the United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 of the United States Code, Section 112:

______________________ (Application Number) ______________________ (Filing Date) ______________________ (Status - patented, pending, abandoned)

The undersigned hereby authorizes the U.S. attorney or agent named herein to accept and follow instructions as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney or agent and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorney or agent named herein will be so notified by the undersigned.

As a named inventor, I hereby appoint Alan W. Young, Registration No. 37,970, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Address all communications to **Alan W. Young** at YOUNG LAW FIRM, P.C., 4370 Alpine Rd., Ste. 106, Portola Valley, CA 94028.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

First and Joint Inventor Name: Thierry Brunet de Courssou

Residence Address: 975 Seven Hills Dr., Apt. 1317, Henderson, NV 89052, US

Post Office Address: (same as above)

Citizenship: France

Signature: ______________________ Date: oct 29, 2007

SUPPLEMENTAL APPLICATION DATA SHEET

Application Information

Application number::	**11/842,147**
Filing Date::	**08/20/07**
Application Type::	Regular
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Title::	Game talk service bus
Attorney Docket Number::	CYBS5805CIP
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	21
Total Drawing Sheets::	23
Small Entity?::	Yes
Petition Included?::	No
Secrecy Order in Parent Appln.?::	No

Applicant Information

Applicant Authority Type::	Inventor1
Primary Citizenship Country::	France
Primary Citizenship Status::	Full Capacity
Given Name::	Thierry
Family Name::	Brunet de Courssou
City of Residence::	Henderson
State of Residence::	NV
Country of Residence::	US
Street of Mailing Address::	975 Seven Hills Dr., Apt. 1317
City of Mailing Address::	Henderson
State of Mailing Address::	NV
Country of Mailing Address::	US
Postal or Zip Code of Mailing Address::	89052

Correspondence Information

Correspondence Customer Number::	22430

Representative Information

Representative Customer Number::	22430

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
	~~Continuation-in-part of~~	~~10/120,635~~	~~04/10/02~~
~~10/120,635~~	~~non provisional of~~	~~60/332,593~~	~~11/23/01~~

Foreign Priority Information

Country::	Application number::	Filing Date::	Priority Claimed::

Assignee Information

Assignee Name::	Cyberview Technology, Inc.
Street of Mailing Address::	Two Palo Alto Square, Suite 500
City of Mailing Address::	Palo Alto
State of Mailing Address::	CA
Country of Mailing Address::	US
Postal or Zip Code of Mailing Address::	94306-2122

Electronic Acknowledgement Receipt

EFS ID:	2389716
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	30-OCT-2007
Filing Date:	21-AUG-2007
Time Stamp:	00:12:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	**Document Description**	**File Name**	File Size(Bytes) /Message Digest	**Multi Part /.zip**	**Pages (if appl.)**
1		5805CIPPRELIMAMEND.pdf	233016 b68262a3db2a2eefb30b3275199f3c29718e8f9a	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	3
	Oath or Declaration filed	4	5
	Application Data Sheet	6	7
Warnings:			
Information:			
Total Files Size (in bytes):		233016	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SUPPLEMENTAL APPLICATION DATA SHEET

Application Information

Application number::	11/842,147
Filing Date::	08/20/07
Application Type::	Regular
Subject Matter::	Utility
CD-ROM or CD-R?::	None
Title::	Game talk service bus
Attorney Docket Number::	CYBS5805CIP
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	21
Total Drawing Sheets::	23
Small Entity?::	~~Yes~~ **No**
Petition Included?::	No
Secrecy Order in Parent Appln.?::	No

Applicant Information

Applicant Authority Type::	Inventor1
Primary Citizenship Country::	France
Primary Citizenship Status::	Full Capacity
Given Name::	Thierry
Family Name::	Brunet de Courssou
City of Residence::	Henderson
State of Residence::	NV
Country of Residence::	US
Street of Mailing Address::	975 Seven Hills Dr., Apt. 1317
City of Mailing Address::	Henderson
State of Mailing Address::	NV
Country of Mailing Address::	US
Postal or Zip Code of Mailing Address::	89052

Correspondence Information

Correspondence Customer Number::	22430

Representative Information

Representative Customer Number::	22430

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::

Foreign Priority Information

Country::	Application number::	Filing Date::	Priority Claimed::

Assignee Information

Assignee Name::	Cyberview Technology, Inc.
Street of Mailing Address::	Two Palo Alto Square, Suite 500
City of Mailing Address::	Palo Alto
State of Mailing Address::	CA
Country of Mailing Address::	US
Postal or Zip Code of Mailing Address::	94306-2122

Electronic Acknowledgement Receipt

EFS ID:	2428155
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	05-NOV-2007
Filing Date:	21-AUG-2007
Time Stamp:	22:50:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	5805CIPADS3.pdf	56371 93b78f0d1dcb4224abe02839f2aa87f8d3929a4f	no	2

Warnings:

Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	56371

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP

CONFIRMATION NO. 2880

22430
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY, CA94028

Date Mailed. 11/23/2007

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 02/07/2008. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Patent Publication at 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/842,147		3714	

Correspondence Address / Fee Address Change

The following fields have been set to Customer Number 22430 on 02/04/2008

- Correspondence Address
- Maintenance Fee Address

The address of record for Customer Number 22430 is:
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY,CA 94028

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP

CONFIRMATION NO. 2880

22430
YOUNG LAW FIRM, P.C.
ALAN W. YOUNG
4370 ALPINE ROAD
SUITE 106
PORTOLA VALLEY, CA94028

Title: GAME TALK SERVICE BUS

Publication No. US-2008-0032801-A1
Publication Date: 02/07/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11184214
	Filing Date	2007-08-20
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6210274		2001-04-03	Carlson	
	2	6428413		2002-08-06	Carlson	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11184214
	Filing Date	2007-08-20
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	3116138
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young/Nita Miller
Filer Authorized By:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	07-APR-2008
Filing Date:	21-AUG-2007
Time Stamp:	19:03:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	5805CIPIDS2.pdf	21970 4c9f891d7debd97fb8e8fd122aafd1723d8459ea	no	2

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

Total Files Size (in bytes):	21970

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	4255672
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	07-NOV-2008
Filing Date:	21-AUG-2007
Time Stamp:	18:49:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDS3.pdf	307996 96bcf8e7529bce40b3626265d5588b18a18e66de	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	NPL Documents	4	9
Warnings:			
Information:			
	Total Files Size (in bytes):	307996	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

	1	Canadian Office Action of Sep. 30, 2008 in related Canadian patent application 2,468,026 (Attorney Docket CYBV5805CA).	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST 3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

□ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2008-11-07
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	4419592
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	09-DEC-2008
Filing Date:	21-AUG-2007
Time Stamp:	12:31:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDS4asperPCTISRandWO.pdf	760927 8c6a1151a6f0402d105a402a5012c3069191b879	yes	13

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Information Disclosure Statement (IDS) Filed (SB/08)	1	2
	NPL Documents	3	3
	NPL Documents	4	4
	NPL Documents	5	6
	NPL Documents	7	13
Warnings:			
Information:			
	Total Files Size (in bytes):	760927	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U S Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	BRUNET de COURSSOU, Thierry
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070191102	A1	2007-08-16	Coliz et al.	
	2	20060030383	A1	2006-02-09	Rosenberg et al.	
	3	20040185936	A1	2004-09-23	Block et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	BRUNET de COURSSOU, Thierry
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBS5805CIP

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Notification of Transmittal of the International Search Report And the Written Opinion of the International Searching Authority, Or the Declaration in corresponding PCT application PCT/US08/73559, mailed 05 Dec. 2008.	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08a (05-07)
Approved for use through 09/30/2007 OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

	1	EP Examination Report of February 18, 2009 in related application EP 02 780 726.2	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	5007198
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	22430
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	20-MAR-2009
Filing Date:	21-AUG-2007
Time Stamp:	15:57:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDS5.pdf	296883 0fcb6c5de511239a121563581e1dd2d3e14c782a	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	2
	NPL Documents	3	8
Warnings:			
Information:			
	Total Files Size (in bytes):	296883	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/842,147		3714	

OC000000035583272

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 86195 on 04/20/2009

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 86195 is:

86195
John Todd Craig
1975 Tison Lane
Mount Pleasant, SC 29464

PART 1 - ATTORNEY/APPLICANT COPY

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/842,147		3714	

OC000000036018939

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 86915 on 05/15/2009

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 86915 is:

86915
Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

PART 1 - ATTORNEY/APPLICANT COPY

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070191102	A1	2007-08-16	Coliz et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number³	Country Code² i	Kind Code⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T⁵
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

	1	international Preliminary Examination Report of March 4, 2010 in related PCT application PCT/US2008/073559	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

□ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-06-02
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)

(PCT Rule 44bis.1(c))

To:

YOUNG, Alan, W.
Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028
ETATS-UNIS D'AMERIQUE

Date of mailing *(day/month/year)*
04 March 2010 (04.03.2010)

Applicant's or agent's file reference
MUDA5805PPCT AP00060-25

IMPORTANT NOTICE

International application No. PCT/US2008/073559	International filing date *(day/month/year)* 19 August 2008 (19.08.2008)	Priority date *(day/month/year)* 21 August 2007 (21.08.2007)

Applicant
MUDALLA TECHNOLOGY, INC. et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

Young Law Firm, P.C.
DOCKETED
IDS in Related Cases
Due May 4, 2010
Deadline June 4, 2010

- CYBV5805CIP
- CYBV5805CON
- IGT 6238
- IGT 6239
- IGT 6240

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Masashi Honda

e-mail: pt08.pct@wipo.int

P. ENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference MUDA5805PPCT	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2008/073559	International filing date *(day/month/year)* 19 August 2008 (19.08.2008)	Priority date *(day/month/year)* 21 August 2007 (21.08.2007)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant MUDALLA TECHNOLOGY, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
□	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
□	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
□	Box No. VI	Certain documents cited
□	Box No. VII	Certain defects in the international application
□	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 24 February 2010 (24.02.2010)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Masashi Honda e-mail: pt08.pct@wipo.int

PCT/US2008/073559 05.12.2008

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
ALAN W. YOUNG
YOUNG LAW FIRM, P.C.
4370 ALPINE ROAD, SUITE 106
PORTOLA VALLEY, CA 94028

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

	Date of mailing *(day/month/year)*	05 DEC 2008
Applicant's or agent's file reference MUDA5805PPCT	FOR FURTHER ACTION See paragraph 2 below	
International application No. PCT/US 08/73559	International filing date *(day/month/year)* 19 August 2008 (19.08.2008)	Priority date *(day/month/year)* 21 August 2007 (21.08.2007)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - A63F 9/24 (2008.04)
USPC - 463/42

Applicant MUDALLA TECHNOLOGY, INC.

1. This opinion contains indications relating to the following items:

☒ Box No. I Basis of the opinion

□ Box No. II Priority

□ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

□ Box No. IV Lack of unity of invention

☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

□ Box No. VI Certain documents cited

□ Box No. VII Certain defects in the international application

□ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion 30 November 2008 (30.11.2008)	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/73559

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed.

□ a translation of the international application into ________________ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. □ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

□ a sequence listing

□ table(s) related to the sequence listing

b. format of material

□ on paper

□ in electronic form

c. time of filing/furnishing

□ contained in the international application as filed

□ filed together with the international application in electronic form

□ furnished subsequently to this Authority for the purposes of search

4. □ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/73559

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-41	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-41	NO
Industrial applicability (IA)	Claims	1-41	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-41 lack novelty under PCT Article 33(2) as being anticipated by US 2007/0191102 A1 to Coliz et. al (hereinafter Coliz).

As per claim 1, Coliz discloses a distributed gaming system (see abstract), comprising: a communication bus (see Fig. 3, 4, 5a, para [0057]-[0058] and [0083]-[0084] - wherein the communications can be over a network, LAN or WAN such as the Internet); at least one first node, each including a first computer coupled to the communication bus (see Fig. 3, 4, 5a, para [0034], [0069]-[0070] and [0083]-[0084] - wherein the computer can be a PC or a gaming console or a server); at least one first service oriented software executing in the first computer of each first node (see Fig. 4, 5a, para [0066]-[0070] - wherein the service oriented software is multi-player support for video games running on multiple servers), the first service oriented software including at least one high-level function (see para [0069]-[0070] - wherein the software includes numerous high level functions as part of its game processing) and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus (see Fig. 3 and para [0049]), the first service oriented software being configured to selectively: publish the at least one high-level function (see para [0069]-[0071] and [0087] - wherein tournament and multi-player game servers contain and display much of the functionality); provide the at least one high-level function upon receiving a request to consume the at least one high-level function (see para [0059], [0087] and [0152] - wherein one example of this is the request to query the leader board of the tournament by the player); enable execution of the at least one high-level function upon receiving a request for execution (see para [0069]-[0070], [0077] and [0152] - wherein each of the servers can execute different functions or procedures in response to requests, including the example of querying the leader board); perform a call back upon receiving a request to consume or execute the at least one high level function, and return a reply subsequent to receiving a request for execution of the at least one high-level function (see para [0134] and [0152] - wherein two examples of a function output are a list of tournaments and a position of the user on a leader board); at least one second node, each including a second computer coupled to the communication bus (see Fig. 3, 4, 5a, para [0034], [0069]-[0070] and [0083]-[0084] - wherein the computer can be a PC or a gaming console), and at least one second service oriented software executing in the second computer of each second node (see Fig. 3, 4 and 5a - wherein the service oriented software is the game in the console or the program on the PC), the second service oriented software including at least one function call (see Fig. 2, 3, 4, para [0069]-[0070], [0085]-[0086], [0091] - wherein the game can make multiple function calls to the multi-player servers to perform calculations) and a second service oriented protocol configured to negotiate service messages over the communication bus (see Fig. 3 and para [0049]), the second service oriented software being configured, upon execution of the at least one function call, to selectively: subscribe to or consume the published or provided at least one high-level function (see para [0069]-[0070] - wherein the game software on the console subscribes to the functions that may be performed on the title server or other consoles); request that the at least one first node execute the at least one high-level function (see para [0067]-[0070] - wherein the game software can request that the server perform necessary calculations or respond to user requests); accept the reply subsequent to receiving a reply from the at least one first node, and accept the call-back upon receiving a call-back from the at least one first node (see para [0069]-[0070] - wherein the call-back is routed back to the game software from the server and the reply is integrated into the game experience).

As per claim 2, Coliz discloses the distributed gaming system of claim I, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call (see Fig. 5b-5e and para [0086]).

As per claim 3, Coliz discloses the distributed gaming system of claim I, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a HTTP request (see Fig. 3, para [0049] and [0085] - wherein HTTP is part of a layer of TCP/IP) .

As per claim 4, Coliz discloses the distributed gaming system of claim I, wherein the first service oriented software is configured to enable execution of the at least one high-level function upon receiving a request for execution via a HTTP request (see Fig. 3, para [0049] and [0085] - wherein HTTP is part of a layer of TCP/IP).

As per claim 5, Coliz discloses the distributed gaming system of claim I, wherein the first service oriented software is configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call (see Fig. 5b-5e and para [0086]).

------------------- SEE SUPPLEMENTAL SHEET -------------------

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/73559

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box V.2 - Citations and Explanations

As per claim 6, Coliz discloses the distributed gaming' system of claim 1, wherein the first service oriented software is configured to return a HTTP reply subsequent to receiving a HTTP request for execution of the at least one high-level function (see Fig. 3, para [0049] and [0085] - wherein HTTP is part of a layer of TCP/IP).

As per claim 7, Coliz discloses the distributed gaming system of claim 1, wherein the service oriented protocol is the Service Oriented Architecture Protocol (SOAP) (see Fig. 3, 5b-5f, para [0049], [0086] and [0091] - wherein SOAP is part of TCP/IP and the application also discloses different code segments that are able to utilize each others' functionality, such as through remote procedure calls).

As per claim 8, Coliz discloses the distributed gaming system of claim 1, wherein the communication bus includes loosely coupled and/or tightly coupled nodes (see Fig. 3, 4, 5a, para [0034], [0049], [0052] and [0087]).

As per claim 9, Coliz discloses the distributed gaming system of claim 8, wherein the loosely coupled nodes include nodes coupled via at least one of Ethernet, Wi-Fi, Internet, radio-link, RS-422, microwave link and satellite link (see Fig. 3, 4, 5a, para [0034], [0049], [0052] and [0083] - wherein wireless networks, WAN and the Internet are disclosed).

As per claim 10, Coliz discloses the distributed gaming system of claim 8, wherein the tightly coupled nodes include nodes coupled via at least one of inter-process communication, USB, Bluetooth, RS-232, RS-422 and IEEE I394 Firewire (see para [0042] - disclosing USB and Bluetooth).

As per claim 11, Coliz discloses the distributed gaming system of claim 1, wherein the at least one high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and an outcome determination function (see para [0069] - wherein the functions performed can include graphics rendering and outcome determination).

As per claim 12, Coliz discloses the distributed gaming system of claim 1, wherein the at least one first node includes one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine (see [0069]-[0070], [0083]-[0084], Fig. 2-4 and 5a - wherein the first node can include a game machine, PC or a server) .

As per claim 13, Coliz discloses the distributed gaming system of claim l, wherein the at least one second node includes at least one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine (see [0069]-[0070], [0083]-[0084], Fig. 2-4 and 5a - wherein the first node can include a game machine, PC or a different server).

As per claim 14, Coliz discloses the distributed gaming system of claim 1, wherein the first service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI (see Fig. 4, para [0056], [0086] and [0153] - wherein the COM interface is disclosed and notifications are sent concerning changes in ranking and eligibility for tournaments).

As per claim 15, Coliz discloses the distributed gaming system of claim 1, wherein the second service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI (see para [0065], [0086] and [0153] - wherein one console becomes unavailable a notification is sent to the other devices and notification updates to rankings are based on the events on other consoles).

As per claim 16, Coliz discloses the distributed gaming system of claim 1, wherein security over the communication bus is provided by implementation of at least one of the IPSec protocol, the VPN tunneling protocol and the SSL protocol (see para [0049], [0057] and [0059] - wherein SSL provides for security encryption over a TCP/IP network).

As per claim 17, Coliz discloses the distributed gaming system of claim 1, wherein the at least one second node includes a gaming machine (see Fig. 3 and para [0069]-[0070]).

As per claim 18, Coliz discloses the distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine (see Fig. 2 and para [0038] - wherein the node comprising the cpu and communication bus is inside the gaming machine - Xbox).

As per claim 19, Coliz discloses the distributed gaming system of claim 1, wherein the at least one first node includes a gaming machine (see Fig. 3 and para [0069]-[0070]).

As per claim 20, Coliz discloses the distributed gaming system of c1aim 1, wherein the at least one first node is included inside a gaming machine (see Fig. 2 and para [0038] - wherein the node comprising the cpu and communication bus is inside the gaming machine - Xbox).

As per claim 21, Coliz discloses the distributed gaming system of claim 1, wherein the at least one second node is a gaming machine played by a player and is configured to execute at least one function call during a game session (see Fig. 4 and para [0069]-[0070] - wherein the function calls include image rendering, input processing and environment mapping).

———————— SEE SUPPLEMENTAL SHEET ————————

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US 08/73559

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Supplemental Box 1 and Box V.2 - Citations and Explanations

As per claim 22, Coliz discloses the distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine played by a player and is configured to execute at least one function call during a game session (see Fig. 2, 4 and para [0038] and [0070] - wherein the second node can be the game running on the cpu contained in the gaming machine and making local function calls).

As per claim 23, Coliz discloses the distributed gaming system of claim 1, wherein the at least one first node is configured for load balancing with another one of the at least one first node (see Fig. 4, para [0055], [0066] and [0067]-[0068]).

As per claim 24, Coliz discloses the distributed gaming system of claim 1, wherein the negotiating of service messages on the communication bus include at least one of naming (see para [0097] - wherein each tournament is given a unique id), discovery, message routing (see para [0053]), publishing eventing (see Fig. 6 and para [0095] - wherein the tournament is created and listed), subscribing eventing - (see para [0096] - wherein users can join the tournament), message transformations, workflows, and communication recovery from nodes powering'-off then on again (see para [0063] - wherein the data center keeps devices informed about other devices being disconnected from the network).

As per claim 25, Coliz discloses a distributed gaming system (see abstract), comprising: a communication bus (see Fig. 3, 4, 5a, para [0057]-[0058] and [0083]-[0084] - wherein the communications can be over a network, LAN or WAN such as the Internet); a first gaming machine coupled to the communication bus (see Fig. 3, 4, para [0034], [0069]-[0070]); the first gaming machine being configured to selectively publish, execute and provide at least one high-level function (see para [0069]-[0070], [0095], [0098] and [0152] - wherein the functions can be distributed across consoles or a single console can act as a server for the session and provide the associated functions or create an instance of a tournament), and a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine (see Fig. 3, 4, para [0034], [0069]-[0070] and [0134] - wherein the second gaming machine is any one of the plurality of consoles connected to the network and users on those consoles can join the specific tournament), and selectively request that the first gaming machine execute the at least one high-level function (see para [0058]-[0059], [0134] and [0152] - wherein a console can request that the title server or console acting as a server list the various tournaments or the position of the user on a leader board).

As per claim 26, Coliz discloses the distributed gaming system of claim 25, wherein the first gaming machine is further configured to perform a call back upon receiving a request to consume or execute the at least one high-level function, and return a reply (see para [0134] and [0152] - wherein the console is acting as a server and two examples of a function output are a list of tournaments and the position of the user on a leader board) and wherein the second gaming machine is further configured to accept the reply subsequent to receiving the call-back from the first gaming machine (see para [0069]-[0070] - wherein the call-back is routed back to the game software from the first console acting as a server and the reply is integrated into the game experience on the second console).

As per claim 27, Coliz discloses the distributed gaming system of claim 25, further including a service-oriented device coupled to the communication bus (see Fig. 4), the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine (see Fig. 4 and para [0052], [0056] and [0058] - wherein the data center includes a server farm and tournament and title servers are also connected to the network), the service oriented device being configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function (see Fig. 4, para [0069]-[0070] - wherein the data center, title or tournament servers may designate specific functions regarding multi-player interactions to the consoles or alternatively execute such functions themselves).

As per claim 28, Coliz discloses a method for distributed gaming over a communication bus, comprising: providing a first gaming machine and coupling the first gaming machine to the communication bus (see Fig. 3, 4, para [0034] and [0069]-[0070]); publishing, by the first gaming machine, a first high-level function over the communication bus (see para [0069]-[0070], [0095] and [0098] - wherein a user may create an instance of a tournament); providing a node coupled to the communication bus (see Fig. 3, 4 and para [0069]-[0070] - wherein the node can be one of many other consoles connected to the network); receiving, from the node, a request to subscribe to the published first high-level function (see Fig. 3, 4, para [0034], [0069]-[0070] and [0134] - wherein users on the other consoles can join the tournament); accepting the subscription request (see para [0134]-[0135] - players are registered); initiating a gaming session on the first gaming machine (see Fig. 8a, para [0135]-[0136] - wherein game sessions are initiated once the numbers of players per session is decided), and responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus (see para [0069]-[0070] and [0140] - wherein multi-player interactions can be carried out by the hosting console acting as the server and passed on to the network).

As per claim 29, Coliz discloses the method of claim 28, wherein the receiving step is carried out with the node including a second gaming machine (see Fig. 3 and para [0069]-[0070]).

As per claim 30, Coliz discloses the method of claim 28, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine (see para [0075] - wherein the system disclosed can be used for personal computers as well as consoles).

As per claim 31, Coliz discloses the method of claim 28, wherein the high-level function includes at least one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function (see para [0069] - wherein the functions performed can include graphics rendering and outcome determination).

------------------ SEE SUPPLEMENTAL SHEET ------------------

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

	International application No. PCT/US 08/73559

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Supplemental Box 2 and Box V.2 - Citations and Explanations

As per claim 32, Coliz discloses the method of claim 28, further comprising a step of receiving, from the node, a request that the first gaming machine executes the high-level function (see para [0059], [0087], [0140] and [0152] - wherein one example of this is the request to query the leader board of the tournament by the player).

As per claim 33, Coliz discloses the method of claim 28, further comprising a step of the first gaming machine performing a call back upon receiving the request to consume or execute the high-level function (see para [0069]-[0070],[0134] and [0152] - wherein the console is acting as a server and two examples of a function output are a list of tournaments and the position of the user on a leader board).

As per claim 34, Coliz discloses the method of claim 28, wherein the second providing step is further carried out with the node being configured to selectively publish, subscribe, provide, execute and request that the first gaming machine execute the high level function (see Fig. 4, para [0069]-[0070] - wherein the data center, title or tournament servers may designate specific functions regarding multi-player interactions to the consoles or alternatively execute such functions themselves).

As per claim 35, Coliz discloses a method for distributed gaming over a communication bus, comprising: providing a first node and coupling the first node to the communication bus (see Fig. 3, 4, para [0034] and [0069]-[0070] - wherein the data center and the tournament and title servers are connected to the bus); publishing, by the first node, a high-level function over the communication bus (see para [0069]-[0070], [0095] and [0098] - wherein the tournament server may host tournaments and the title server may have tournament listings); providing a first gaming machine coupled to the communication bus (see Fig. 3 and 4); receiving, from the first gaming machine, a request to subscribe to the published high-level function (see Fig. 3, 4, para [0034], [0069]-[0070] and [0134] - wherein users on consoles can join the tournament); accepting the subscription request (see para [0134]-[0135] - players are registered); initiating a gaming session on the first gaming machine (see Fig. 8a, para [0135]-[0136] - wherein game sessions are initiated once the numbers of players per session is decided), and responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus (see para [0069]-[0070] and [0140] - wherein multi-player interactions can be carried out by the title server, tournament server or other elements in the data center and passed on to the network).

As per claim 36, Coliz discloses the method of claim 35, wherein the receiving step is carried out with the first node including a second gaming machine (see Fig. 3, 4 and para [0069]-[0070]).

As per claim 37, Coliz discloses the method of claim 35, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine (see Fig. 4 and para [0052], [0056] and [0058] - wherein the data center includes a server farm and tournament and title servers are also connected to the network).

As per claim 38, Coliz discloses the method of claim 35, wherein the high-level function includes one of a business function, and audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function (see para [0069] - wherein the functions performed can include graphics rendering and outcome determination).

As per claim 39, Coliz discloses the method of claim 35, further comprising a step of receiving, from the first gaming machine, a request that the node execute the first high-level function (see para [0059], [0069]-[0070], [0087], [0140] and [0152] - wherein one example of this is the request to query the leader board of the tournament by the player).

As per claim 40, Coliz discloses the method of claim 35, further comprising a step of the node performing a call back upon receiving the request to consume or execute the high-level function (see para [0069]-[0070], [0134] and [0152] - wherein two examples of function outputs are the list of tournaments available and the position of the user on a leader board).

As per claim 41, Coliz discloses the method of claim 35, wherein the second providing step is further carried out with the first gaming machine being configured to selectively publish, subscribe, provide, execute and request that the node execute the high level function (see Fig. 4, para [0069]-[0070] - wherein the console, acting as a server may designate specific functions regarding multi-player interactions to the other consoles or alternatively execute such functions locally).

Claims 1-41 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used by industry.

Electronic Acknowledgement Receipt

EFS ID:	7732209
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	02-JUN-2010
Filing Date:	21-AUG-2007
Time Stamp:	16:55:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	5805CIPIDSofJune022010.pdf	520552 bef63d9b111b138810725a674b48a2655896c2d3	no	3

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

2	NPL Documents	5805PPCTIPERofMarch042010.pdf	366664 04ae38e817310fb5940a64a775a97c81cf5590a6	no	8

Warnings:

Information:

Total Files Size (in bytes):	887216

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010014881	A1	2001-08-16	Drummond Jay Paul	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1	00/54214	WO	A1	2000-09-14	Bionetrix Systems Corp		□
	2	98/08581	WO	A1	1998-03-05	Barcelou David M		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Communication pursuant to Article 94(3) EPC of April 9, 2010 in related EP application 02789831.1	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-07-06
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{7} :
G06K 9/00

A1

(11) International Publication Number: WO 00/54214

(43) International Publication Date: 14 September 2000 (14.09.00)

(21) International Application Number: PCT/US00/05722

(22) International Filing Date: 7 March 2000 (07.03.00)

(30) Priority Data:
09/264,726 9 March 1999 (09.03.99) US

(71) Applicant: BIONETRIX SYSTEMS CORPORATION [US/US]; 8150 Leesburg Pike, Suite 1230, Vienna, VA 22182 (US).

(72) Inventors: BIANCO, Peter, G.; 7710 Whiterim Terrace, Potomac, MD 20854 (US). BOON, William, T.; 13170 Flynn Court, Bristow, VA 20136 (US). STERLING, Robert, B.; 3941 Washington Street, Kensington, MD 20895 (US). WARE, Karl, R.; 3244 Pope Street, S.E., Washington, DC 20020 (US).

(74) Agents: SOKOHL, Robert, E. et al.; Sterne, Kessler, Goldstein & Fox P.L.L.C., Suite 600, 1100 New York Avenue, N.W., Washington, DC 20005–3934 (US).

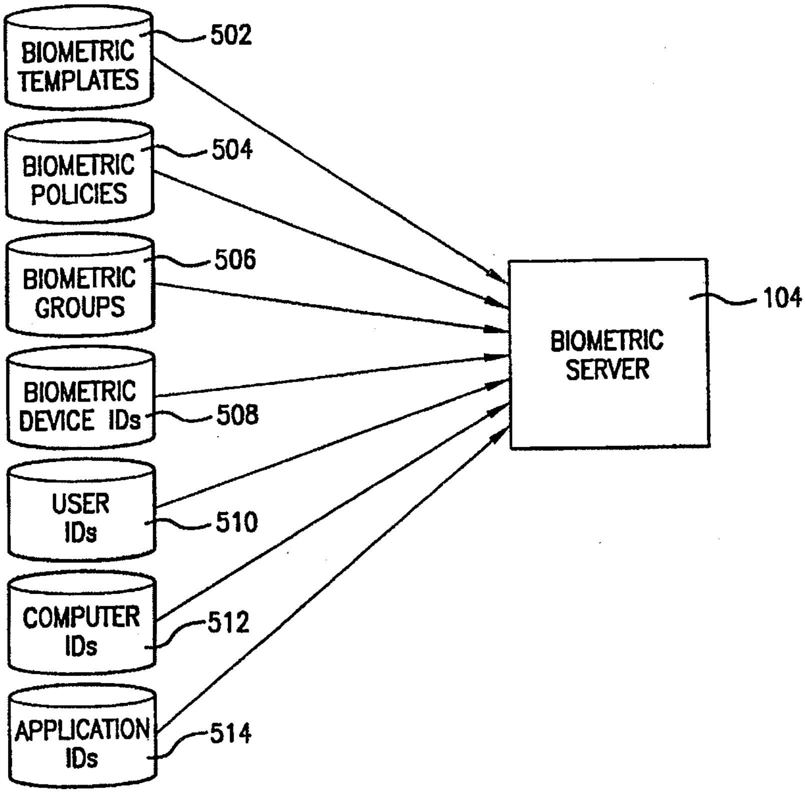
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ALLOWING ACCESS TO ENTERPRISE RESOURCES USING BIOMETRIC DEVICES

(57) Abstract

A system, method and computer program product that utilizes biometric measurements for the authentication of users to enterprise resources. The system includes a biometric server that stores the engine and collections of data required by the system to authenticate users. The collections of data include biometric templates (502), biometric policies (504), biometric groups (506), biometric device IDs (508), users IDs (510), computer IDs (512) and application IDs (514). In the present invention, it is the biometric policies (504) that determine the way or method in which a user is to be authenticated by the system. The pre–defined biometric policies (504) include an OR policy, an AND policy, a contingent policy, a random policy and a threshold policy. The execution of the biometric template (502) is created and stored in the biometric server (104) each time a user enrolls in a different biometric device (508). Biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece		Republic of Macedonia	**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's	**NZ**	New Zealand		
CM	Cameroon		Republic of Korea	**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

System, Method and Computer Program Product for Allowing Access to Enterprise Resources Using Biometric Devices

Background of the Invention

Field of the Invention

The present invention relates generally to a system, method and computer program product for allowing access to enterprise resources, and more particularly to the utilization of biometric measurements for the authentication of users, and thus access, to enterprise resources.

Related Art

Enterprise resources include computers, applications and data. Computers are often connected using one or more networks. There are many types of computer networks. Various types of networks include, but are not limited to, local-area networks (LAN), wide-area networks (WAN), the Internet and intranets. In general, a computer network may or may not be private. A typical private network is centrally controlled.

The resulting connectivity provided by a network enables several features such as sharing of data and other resources on the network. For example, networks enable applications such as electronic mail, network file systems (sharing of data using disks accessed over networks), distributed processing (different computers executing different parts of a program, generally in parallel) and sharing of printers and servers. These applications usually result in enhanced communication capabilities, efficient use of resources, and/or faster processing of data, thereby leading to productivity gains within an enterprise.

Provision of network connectivity and applications generally entails the operation of several network elements implemented according to predefined interfaces. Network elements include, but are not limited to, hardware circuits/devices and software entities (e.g., a software object, a process or a thread) which may operate according to interface specifications to provide the network connectivity or applications. The interfaces may be based on open protocols or proprietary protocols.

An open interface is public. Examples of open interfaces are Transmission Control Protocol/Internet Protocol (TCP/IP) and IEEE 802 family of protocols, both of which are commonly used in the networking community. Alternately, a proprietary interface is privately owned and controlled. An example of a proprietary interface is System Network Architecture (SNA) implemented mostly at IBM. Following is a brief description of the various types of networks.

A LAN connects computers that are geographically close together (e.g., in the same building). LANS are typically private networks being owned and controlled by an enterprise.

A WAN connects computers that are farther apart geographically and are connected by telephone lines or radio waves (e.g., in multiple offices and distant geographies). WANS are also typically private networks owned and controlled by an enterprise. Multiple LANs can be connected by a WAN.

The Internet is a global network connecting millions of computers. As of 1998, the Internet has more than 100 million users worldwide, and that number is growing rapidly. More than 100 countries are linked into exchanges of data, news and opinions. Unlike private networks which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Users can choose which Internet services to use and which local services to make available to the global Internet community. There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

An ISP is a company that provides access to the Internet. For a monthly fee, the ISP gives you a software package, username, password and access phone number. Equipped with a modem, a user can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. In addition to serving individuals, ISPs also serve large individual enterprises, providing a direct connection from the enterprise's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs).

An intranet is a privately owned and controlled network. An intranet's host sites may look and act just like any other host site, but a firewall surrounding an intranet fends off unauthorized access. Like the Internet itself, intranets are used to share information (i.e. data). Secure intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols.

As enterprise resources grow so does the complexity and importance of protecting them. In general, the administration of resource protection involves determining the type of identification mechanism to protect enterprise resources, maintaining the integrity of the chosen identification mechanism, managing users, determining which enterprise resources to protect and determining alternative ways of allowing a user access to enterprise resources when the normal way of authentication is faulty. The administration of resource protection in a network is not only a complex and expensive task, but it may conflict with the desired productivity the networking of resources provides.

As discussed above, one of the results of networking together enterprise resources is the increase in productivity through enhanced communication and more efficient use of the resources. While this increase in productivity is important to any enterprise, so is the protection of its resources. While a network works to provide easier access to enterprise resources, an authentication mechanism for protecting the same resources works to restrict access to them. Therefore, so as to not offset the increase in productivity a network provides to an enterprise, an enterprise needs to balance adequate resource protection with an efficient means of administering such protection.

Summary of the Invention

The present invention is directed to a system, method and computer program product that utilizes biometric measurements for the authentication of users to enterprise resources. The system includes a biometric server that stores the engine and collections of data required by the system to authenticate users. The collections of data include biometric templates, biometric policies, biometric groups, biometric device IDs, user IDs, computer IDs and application IDs. In the present invention, the biometric policies determine the way or method in which a user is to be authenticated by the system. The execution of the biometric policies involves the use of one or more biometric templates. One unique biometric template is created and stored in the biometric server each time a user enrolls in a different biometric device. Biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. These measurements, called biometric measurements, may include, but are not limited to, measurements of finger and hand geometry, retina and facial images, weight, DNA data, breath, voice, typing stroke and signature.

The types of data stored in the biometric server are partially determined through the operations of an enrollment station and an administration station. The enrollment station is used to enroll users into biometric system. The administration station is used to perform overall management duties and to initially setup the data in biometric server. A satellite enrollment station can be used to enroll users into biometric system at remote locations. Finally, an alternate biometric server is a backup or standby server to biometric server. The alternate biometric server ensures that the system is always available to authenticate users.

The biometric policies of the present invention provide flexibility to the level of protection for individual enterprise resources. The pre-defined biometric polices include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. This is done through the layering of both biometric devices and non-biometric devices. The layering of devices allows for the combination of one or more devices in a logical way (via biometric policies) to protect each enterprise resource. The present invention also allows different threshold values to be set for each biometric device. In other words, the present invention can tailor the authentication level based on probability that each user must pass before the user gains access to enterprise resources (e.g., 1/1000, 1/10,000, or 1/1000,0000 that the user is who claims to be).

Another feature of the present invention is directed to a method of storing both biometric templates and digital certificates in a hierarchical structure for ease of access to the biometric templates and the digital certificates. Another feature of the present invention is directed to utilizing the system of the present invention as a roaming profile server in a certificate authority system.

Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

Brief Description of the Figures

The present invention will be described with reference to the accompanying drawings, wherein:

FIG. 1 is a block diagram of the physical components of a biometric authentication system connected by a network according to a preferred embodiment of the present invention;

FIG. 2 is a block diagram of a typical enterprise network system incorporating the biometric authentication system according to a preferred embodiment of the present invention;

FIG. 3 is a block diagram of a computer system preferably used to implement the present invention;

FIG. 4 illustrates the dynamic steps to establish communication between a client and a server executing an object-oriented program. For illustration purposes, FIG. 4 is broken into nine(9) figures including FIG. 4A, FIG. 4B, FIG. 4C, FIG. 4D, FIG. 4E, FIG. 4F, FIG. 4G, FIG. 4H and FIG. 4I;

FIG. 5 illustrates various collections of data stored in the biometric server of the present invention;

FIG. 6 is a flowchart illustrating a typical sequence of steps an administrator may take to initially setup a biometric server;

FIG. 7 is a block diagram of the objects involved in authenticating a user by the present invention;

FIGs. 8A and 8B are a flowchart depicting the high-level operation of authenticating a user by the present invention;

FIG. 9 is a flowchart illustrating the typical operation of a biometric device as it tests a user;

FIG. 10 is a block diagram of the objects involved in starting the authentication process of the present invention with "live" biometric data;

FIG. 11 presents a flowchart depicting the high-level operation of the objects in FIG. 10;

FIG. 12 is a block diagram of the objects involved in the enrollment process of the present invention;

FIG. 13 is a flowchart illustrating the typical operation of the enrollment process of the present invention;

FIG. 14 is a window or screen shot generated by the graphical user interface of the present invention;

FIG. 15 is a chart illustrating the layering process of the present invention;

FIG. 16 is a flowchart illustrating the process of layering using biometric policies of the present invention;

FIG. 17 is a flowchart illustrating the steps involved in executing an OR policy of the present invention;

FIG. 18 is a flowchart illustrating the steps involved in executing an AND policy of the present invention;

FIG. 19 is a flowchart illustrating the steps involved in executing a CONTINGENT policy of the present invention;

FIG. 20 is a flowchart illustrating the steps involved in executing a RANDOM policy of the present invention;

FIG. 21 is a flowchart illustrating the steps involved in executing a THRESHOLD policy of the present invention;

FIG. 22 is a flowchart illustrating the steps involved in executing OR policy having a list of biometric policies of the present invention;

FIG. 23 is a flowchart illustrating the steps involved in executing an AND policy having a list of biometric policies of the present invention;

FIG. 24 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of biometric policies of the present invention;

FIG. 25 is a flowchart illustrating the steps involved in executing an OR policy having a list of policies or devices of the present invention;

FIG. 26 is a flowchart illustrating the steps involved in executing an AND policy having a list of policies or devices of the present invention;

FIG. 27 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of policies or devices of the present invention;

FIG. 28 illustrates an enterprise connected by a WAN incorporating multiple biometric systems of the present invention;

FIG. 29 is a block diagram illustrating how the present invention can be integrated with a public key system;

FIG. 30 is a diagram illustrating various types of networks and how each type of network can be connected to other networks;

FIG. 31 is a flowchart illustrating the steps involved in executing a CONTINGENT policy having a list of biometric policies of the present invention;

FIG. 32 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a list of biometric policies of the present invention;

FIG. 33 is a flowchart illustrating the steps involved in executing a CONTINGENT policy having a list of policies or devices of the present invention; and

FIG. 34 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a list of policies or devices of the present invention.

Detailed Description of the Preferred Embodiments

A. Overview of the Invention

The inventors of the present invention recognized that a solution did not exist that effectively balances the protection of resources with ease of access to the same resources in a networked environment. The general solution of the present invention is twofold. First, use as adequate an identification mechanism as possible to protect enterprise resources. And second, provide a method and system that utilizes the adequate identification mechanism to provide effective authentication to resources in a networked environment. This method and system for authentication must not decrease the productivity that a network provides an enterprise.

1. Determining an Adequate Identification Mechanism

Billions of dollars have been lost by thousands of enterprises due to inadequate authentication to enterprise resources. For years enterprises have protected valuable resources through various types of identification mechanisms that do not conclusively authenticate a user. These inadequate identification mechanisms include, but are not limited to, passwords, smart cards and tokens. The reason why passwords, smart cards and tokens do not conclusively authentic a user is due to a human factor involved with using these identification mechanisms. In fact, the weakest link in authentication is the human factor.

The human factor creates problems that can lead to unauthorized access since these mechanisms require a user to either know something and/or keep something in his or her possession. For example, password identification requires a user to remember a password. Whereas, tokens and smart cards require a user to have the token or smart card in his or her possession to gain access to enterprise resources. Anything a user knows or has in possession can be compromised.

When inadequate authentication exists people gain unauthorized access to enterprise resources. While a user who gains unauthorized access can be a "cracker" or "hacker" (e.g., a person outside the enterprise), more often the user is from within the enterprise itself (e.g., an employee of the enterprise). An example of this is as follows. As discussed above, password identification requires User A to remember a password. If User A's password is written down, or User B sees User A typing a password at a keyboard, then User B can use User A's password to effectively be User A as far as the enterprise is concerned. The result is that User B now has access to all the resources User A has access to. As with passwords, a similar scenario can happen with tokens or smart cards when User A misplaces a token or smart card and User B finds it. The damage that can be done to resources in a networked environment far exceeds the damage that can be done to resources contained within a single computer (e.g., not networked).

Many enterprises reduce the cost and complexity of administering its resource protection by incorporating a process called "single sign-on." Single sign-on provides each user with one password, token or smart card to access all enterprise resources. Most people can remember one password without writing it down and/or keep track of one token or smart card. While this reduces the complexity and cost of administering resource protection, it reduces the probability that the user gaining access is authentic. Now, one password may compromise all enterprise resources.

The probability that the user gaining access is authentic can be increased by forcing each user to use multiple passwords, tokens or smart cards for different resources. Many people have difficulty in managing multiple passwords, tokens or smart cards. This increases the likelihood that a user will write down passwords or misplace tokens and smart cards. When this happens, once again all enterprise resources may be compromised.

Another aspect of why password, tokens or smart cards are inadequate identification mechanisms involves the sharing of these between users. An example that can cost an enterprise millions of dollars a year is a practice called "buddy punching." Buddy punching typically involves two users or employees within an enterprise that requires its employees to use a password to "punch in and out" of work each day. Password, or even tokens and smart cards, make is easy for one employee to "punch in" another employee at the beginning of the day and then "punch out" that same employee at the end of the day. The practice of "buddy punching" allows an employee who stays home a particular day to still have the benefit of receiving a paycheck for that day.

Therefore, the inventors of the present invention recognized that an identification mechanism is needed that avoids the weakest link in authentication that is a result of the human factor discussed above.

2. *Biometric Identification Mechanism: An Adequate Authentication Mechanism*

A biometric identification mechanism eliminates the weakest link caused by the human factor. Biometric identification mechanisms, or biometric devices, utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. Biometric identification mechanisms include two basic categories of biometric measurements. The first category involves measuring a unique characteristic found on a user's body. This may include, but is not limited to, finger and hand geometry, retina and facial images, weight, DNA data and breath. The second category involves measuring a user's behavioral characteristics. This may include, but is not limited to, voice, typing stroke and signature. In general, anything that can be measured on a user that is unique can be used as a biometric measurement.

While anything that can be measured on a user that is unique can be used as a biometric measurement, the best biometric measurements to use for authentication purposes depend on the consistency over time of the biometric measured. For example, user weight is a biometric measurement. Because weight is a biometric measurement that fluctuates frequently for many people, it is not a desirable biometric measurement to use for authentication purposes.

The general process of using biometric identification mechanisms as an authentication mechanism is as follows. The user is prompted for a particular biometric measurement that is used by a biometric device to generate a value. The value gets stored in a template as stored biometric data. When the user wants to gain access to a resource that is protected by the biometric device, the user is prompted for live biometric data. The live biometric data is matched with the stored biometric data. In reality, the live biometric data and the stored biometric data will never be exactly the same. Therefore, a user must come within some tolerance to pass the biometric device and gain access to the protected resources. As mentioned above, the biometric device utilizes a scientific technique to identify a user based on biometric measurements. The tolerance is typically predetermined by the vendor for the particular biometric device used.

A specific example of how biometric identification works can be illustrated by a typical fingerprint device. A fingerprint device measures the geometry of a fingerprint. First, a user is prompted for multiple samples of a fingerprint. For each sample, a number of characteristics or measurements are identified. Then, for all of the multiple samples, a number of common characteristics or measurements are identified. The common characteristics or measurements are processed through a unique algorithm which generates a unique template to store the biometric data. When a "live" fingerprint is presented for identification, it is processed through the same algorithm. If the output from the "live" process matches the stored biometric data within a certain tolerance, the user is considered to be authenticated and gains access to which ever resource the fingerprint device is protecting.

A specific example of how biometric identification works when behavioral measurements are involved can be illustrated by a typical signature device. Here, a user is prompted for multiple samples of a signature. For each sample, characteristics or measurements are identified. The characteristics or measurements include the pressure, sequence of events, direction, relative vectors and speed. One example of the sequence of events is to identify that when the user signed his or her signature, that "t" was crossed before "I" dotted. An example of direction is that the user crossed a "t" from right to left. Relative vectors may include the information that "F" is 2.1 the height of "e." Finally, speed recorded is the time it took the user to sign a signature from start to finish.

As with fingerprint devices, common characteristics or measurements are identified for the multiple samples. These common characteristics or measurements are processed through a unique algorithm which generates a unique template to store the biometric data. When a "live" signature is presented for identification, it is processed through the algorithm. If the output from the "live" process matches the stored biometric data within a certain predetermined tolerance, the user is considered to be authenticated.

The use of biometric identification mechanisms as a means for authentication eliminates the problems discussed above involving the use of passwords, tokens or smart cards. Because biometric measurements involve either a unique characteristic found on a user's body (e.g., fingerprint) or a user's behavioral characteristics (e.g., signature), it is impossible for users to forget or lose the mechanism of authenticating themselves. Now, it is impossible for User

B to "steal" the mechanism of authenticating User A to the enterprise. Likewise, the practices of users sharing passwords and "buddy punching" are eliminated.

While the use of biometric devices can conclusively authenticate a user, the inventors of the present invention recognized that a method and system was needed that utilizes biometric devices to provide effective authentication to resources in a networked environment while not decreasing the productivity a network provides an enterprise.

Most enterprises contained in one office today have a LAN. But, more often enterprises today span multiple offices and distant geographies. These enterprises typically have a WAN. As discussed above, networks provide increased productivity to an enterprise by allowing users easy access to all the resources on the network. This is true independent of which office the user is at and where the resource is located within the enterprise. In contrast, resource protection limits the accessability of resources to a user without first being authenticated. Therefore, if the administration of resource protection is not efficient, then the increase in productivity gained by networking is lost. Simply put, if the right user cannot gain access to needed resources, then the enterprise suffers from a decrease in productivity. Yet, if unauthorized users gain access to enterprise resources, then the enterprise also suffers from a potential decrease in productivity. This potential decrease in productivity is due partly to resource loss.

The present invention overcomes limitations that are encountered when resource protection is used in a networked environment. The present invention has the following benefits: (1) flexibility to use the right biometric measurement for an environment; (2) allows user mobility within the enterprise; (3) flexibility in the degree of authentication required to protect each resource; (4) allows remote enrollment of users into a resource protection system; (5) allows remote refreshing of biometric templates; and (6) ensures the integrity of software loaded on remote computers in the network. The present invention also allows different threshold values to be set for each biometric device. In other words, the present invention can tailor the authentication level based on probability that each user must pass before gains access to enterprise resources (e.g., 1/1000, 1/10,000, or 1/1000,0000 that the user is who claims to be).

3. *Biometric Authentication System*

FIG. 1 is a block diagram of the functional components of biometric authentication system 102 (also called "biometric system" herein) connected by network 114 according to a preferred embodiment of the present invention. Biometric system 102 includes biometric server 104, enrollment station 106, administration station 108, alternate biometric server 110 and satellite enrollment station 112. Network 114 connects the functional components of biometric system 102. The connectivity provided by network 114 enables such features as the sharing of data and other resources on biometric system 102.

The topology of network 114 as shown in FIG. 1 is called a bus topology. In general, the topology of a network is the geometric arrangement of functions (i.e., computers) within the system. Other common types of network topologies include star and ring topologies. Although the present invention is illustrated in FIG. 1 as incorporating a bus topology, the present invention can equally be applied to other topologies.

Biometric server 104 stores the engine for biometric system 102. Biometric server 104 also stores collections of data required by biometric system 102. Both the functions of the engine and the data stored in biometric server 104 will be discussed in further detail below. The types of data stored in biometric server 104 are partially determined through the operations of enrollment station 106 and administration station 108. Enrollment station 106 is used to enroll users into biometric system 102. Enrollment station 106 has attached to it every type of biometric device used by biometric system 102 to enroll and ultimately authenticate users. When a user is enrolled into biometric system 102, the user may be enrolled with as many biometric devices as the administrator deems necessary.

Administration station 108 is used by the administrator of biometric system 102 to do perform overall management duties. The administrator can also use administration station 108 to generate various reports. The reports may include a list of different types of data stored in biometric server 104 (e.g., a list of the currently enrolled users in biometric system 102). In addition, administration station 108 is typically used to setup the initial data in biometric server 104. Another component is satellite enrollment station 112. Enrollment station 112 is used to enroll users into biometric system 102 at remote locations. Satellite enrollment station 112 may have as many biometric devices attached to it as administration station 108, but alternatively may also be a scaled down version of administration station 108.

One or more alternate biometric servers 110 are backup or standby servers to biometric server 104. Alternate biometric server 110 stores the exact same data as biometric server 104. Only in the event that biometric server 104 fails does alternate biometric server 110 become active and take over the responsibility of authenticating users. The purpose of alternate biometric server 110 is to ensure that biometric system 102 is always available to authenticate users.

There are other ways to ensure the availability of biometric system 102, however, including: biometric server 104 and alternate biometric server 110 having equal responsibility to authenticate users; administration station 108 backup and tape and/or CD-ROM backup. The biometric server 104 and alternate biometric server 110 having equal responsibility to authenticate users means that they are both active at all times. There is a constant synchronization between biometric server 104 and alternate biometric server 110. In the event that one or the other server fails, the other server takes over the responsibility of authenticating users. When the failed server becomes active again, it initiates synchronization with the other server.

Another way to ensure the availability of biometric system 102 is through administration station 108 backup. Here, administration station 108 acts like a master biometric repository. Administration station 108 updates all active biometric servers 104 simultaneously. The final way to ensure the availability of biometric server 102 is through a tape and/or CD-ROM backup.

Although a preferred embodiment of the present invention includes all of the functional components of biometric system 102 discussed above, several (or all) components may be combined as long as the functionality of each component still exists within biometric system 102 as described above. For example, enrollment station 106 and administration station 108 can be combined into one functional component. In addition, several components of biometric system 102 are optional. For example, an enterprise may not have the need to remotely enroll users or may just desire not to. Therefore, satellite enrollment station 112 would not be needed.

4. Network System

As mentioned above, various types of networks include, but are not limited to, LANs, WANs, the Internet and intranets. An enterprise may utilize one type of network or any combination of the different types of networks. FIG. 30 is a diagram illustrating the various types of networks and how each type of network can be connected to other networks.

FIG. 30 includes LAN 3002, LAN 3004, LAN 3006, LAN 3008, WAN 3010, Internet 3012, firewall 3014, connection 3016, host 3018, connection 3020, connection 3022, connection 3024, connection 3026, connection 3028 and connection 3030. Connections 3016, 3024, and 3026 through 3030 are typically provided by an ISP.

As shown in FIG. 30, LAN 3002, LAN 3004 and LAN 3006 are connected to WAN 3010. LAN 3008 and host 3018 are also connected to WAN 3010 via the Internet 3012. Connections 3020 and 3022 are typically virtual private networks (VPN). A VPN is a network that is constructed by using public wires to provide connectivity. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Host 3018 may have a type of access to WAN 3010 called dial-up access. Dial-up access refers to connecting a host (i.e., device) to a network via a modem and a public telephone network. Dial-up access is really just like a phone connection, except that the parties at the two ends are computer devices rather than people. Because dial-up access uses normal telephone lines, the quality of the connection is not always good and data rates are limited. An alternative way to connect two computers is through a leased line, which is a permanent connection between two devices. Leased lines provide faster throughput and better quality connections, but they are also more expensive.

WAN 3010 can also be implemented as an intranet as described above. Thus, firewall 3014 can be used to protect WAN 3010 by fending off unauthorized access. Many network systems today incorporate a firewall. A firewall is a system designed to prevent unauthorized access to or from a network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. Once a user is authorized to access the network, firewalls are further designed to prevent unauthorized transfer of data to and from the network. All data entering or leaving the intranet pass through the firewall, which examines each transmission and blocks those that do not meet the specified security criteria. Firewalls can be implemented in both hardware and software, or a combination of both. A firewall is considered a first line of defense in protecting private information (i.e., data).

FIG. 2 is a block diagram of an enterprise network system 202 incorporating biometric system 102 according to a preferred embodiment of the present invention. It is important to note that network system 202 may be one type of network or any combination of the different types of networks described in reference to FIG. 30 above. Referring again to FIG. 30, various functional components of biometric system 102 can be physically located at one or more locations in FIG. 30. For example, biometric system 102 may be located at LAN 3002, LAN 3004, LAN 3006, LAN 3008, WAN 3010 and/or host 3018.

In addition to the components of biometric system 102, network system 202 includes one or more applications, such as application 204, one or more application interfaces, such as application interface 206, one or more user computers, such as user computer 208, one or more remote/web computers, such as remote/web computer 210, web server 212 and web server interface 214. All of the components in network system 202 are considered resources of the enterprise. Network 114 connects both the functional components of biometric system 102 and the additional functional components of network system 202. This connectivity enables such features as the sharing of data and other resources on network system 202.

Examples of application 204 may include, but are not limited to, electronic mail and word processing. Each application 204 has an application interface 206 that allows it to communicate over network 114 to other resources or components in network system 202. In addition, network system 202 includes one or more of user computer 208. Each user computer 208 is located within the enterprise and typically has one or more biometric devices attached to it. User computer 208 is one location where users can gain access to network system 202. To facilitate user access, each computer 208 provides an interface for users to be authenticated by biometric system 102.

Remote/web computer 210 provides the same functions as user computer 208, but remote/web computer 210 accesses network 114 via the Internet. In order for remote/web computer 210 to connect to network 114, it must go through web server 212. Web server interface 214 allows web server 212 to communicate over network 114 to other resources or components in network system 202, including biometric system 102.

In a preferred embodiment of the present invention, users can be required to be authenticated by biometric system 102 when they try to access various points in network system 202. These various access points include network system 202 itself, one or more of application 204 and/or one or more of user computer 208. Because enterprise networks today typically span multiple offices and distant geographies, the different access points in network system 202 may potentially have very different environments. The inventors of the present invention recognized that there is a need for flexibility to use the appropriate biometric device or measurement for the environment. To achieve this flexibility there is a need for many different types of biometric devices to be utilized in network system 202.

5. The Need for the Appropriate Biometric Measurement for an Environment

The appropriate biometric measurement must be used for an environment. The type of environment depends on the location in the network of the biometric device that will be reading the biometric measurement. As mentioned above, biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. Biometric measurements, may include, but are not limited to, measurements of finger and hand geometry, retina and facial images, weight, DNA data, breath, voice, typing stroke and signature. There are two aspects of the environment that must be addressed in order to determine the appropriate biometric measurement for that particular environment: a physical aspect and a psychological aspect.

The physical aspect of the environment involves, but is not limited to, lighting and noise. For example, in an environment with poor lighting, a user's iris or facial image may be difficult for the biometric device to measure. Likewise, in a noisy environment a user's voice may be hard to measure.

The psychological aspect of the environment involves the comfort level of users. An example of exceeding a user's comfort level is requiring a user to give a DNA sample to gain access to enterprise resources he or she must access every day. There are certain comfort levels that users of a network have come accustomed to and may refuse to exceed that level.

The result of not using the appropriate biometric measurement for the environment increases the likelihood that the user will not gain access to required resources when needed, thus decreasing enterprise productivity. This happens when the biometric device cannot read a biometric measurement or when users refuse to give the required "live" biometric data for authentication. Therefore, what is needed is the flexibility to use the appropriate biometric measurement for the environment.

The flexibility to use the appropriate biometric measurement for the environment results in the need for many different types of off-the-shelf biometric devices in a single network. Therefore, the authentication task is often complicated by the fact that each of the biometric devices may be provided by several vendors. Currently, biometric devices must conform to a pre-defined interface (or standard) to operate as a part of an integrated network. While the availability of each biometric device from multiple vendors may lead to reduction in prices, the management of networks having biometric devices from different vendors poses additional limitations.

For example, some vendors may allow their biometric devices to be managed from proprietary platforms only. Some vendors may support standards based network management applications (e.g., Simple Network Management Protocol), but the integration of the management of their devices into a network often requires extensive training. For example, the installation of the software to work (i.e., interface) with a network may require training from the vendor. Administrators may need more training for providing on-going support. Such training may need to be provided each time a new biometric device is added to the network. In addition, substantial effort may be required on the part of the vendors to develop software which interfaces with an enterprise's existing network. The resulting overhead due to development and training is unacceptable in most enterprises. This problem of conformity to a pre-defined interface to operate as a part of an integrated network applies equally as well to non-biometric devices.

6. Open Interface

The open interface of the present invention includes a device open interface to allow for the integration of biometric system 102 with biometric devices. The device open interface of the present invention provides an interface that all incompatible biometric and non-biometric devices can communicate with. This provides flexibility to an enterprise in several ways. One way it provides flexibility is that an enterprise can now use the appropriate biometric measurement for the environment.

Another way the present invention's device open interface provides flexibility is by allowing an enterprise to integrate existing non-biometric devices into biometric system 102 (FIG.1). This flexibility is important because all users within an enterprise do not have to be enrolled into biometric system 102 at the same time. Also, some users may never have to be enrolled into biometric system 102 and still be able to gain access to network system 202 (FIG. 2).

Another flexibility provided by the device open interface is by allowing an enterprise to supplement biometric system 102 with non-biometric devices or new biometric devices as they are developed. As mentioned above, biometric devices utilize a scientific technique to identify a user based on biometric measurements. The device open interface provided by the present invention allows an enterprise the flexibility to use any off-the-shelf biometric or non-biometric device to protect a resource. As will be shown later, the flexibility of the open interface enables administrators to combine biometric devices via biometric policies for the authentication of users.

The device open interface is propriety software that is used to communicate to biometric devices in order to retrieve live sample data, match live sample data against stored data (i.e., biometric templates), enroll an individual on each biometric device, and allow administrators to set threshold values. A threshold value indicates the level of identification the biometric device must determine for the user to pass the device. Furthermore, the device open interface has the ability to detect that the biometric device is present, signs of life readings (e.g., that a human is actually present and not a mannequin), etc.

Other open interfaces can be added as needed, including an application open interface, a database open interface and a directory open interface.

B. Preferred Implementation of the Present Invention

1. A Preferred Environment

Biometric server 104, enrollment station 106, administration station 108, alternate biometric server 110 and satellite enrollment station 112 could be implemented using computer 302 as shown in FIG. 3. Obviously, more than one of these functional components could be implemented on a single computer 302.

Computer 302 includes one or more processors, such as processor 304. Processor 304 is connected to communication bus 306. Computer 302 also includes main memory 308, preferably random access memory (RAM). Control logic 310 (i.e., software) and data 312 (such as the data stored in biometric server 104) are stored in the main memory 308, and may also be stored in secondary storage 314.

Computer 302 also includes secondary storage 314. Secondary storage 314 includes, for example, hard disk drive 316 and/or removable storage drive 318, representing a floppy disk drive, a magnetic tape drive, a compact disk drive, etc. Removable storage drive 318 reads from and/or writes to removable storage unit 320 in a well known manner.

Removable storage unit 320, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, etc. As will be appreciated, removable storage unit 320 includes a computer usable storage medium having stored therein computer software and/or data.

Computer programs (also called computer control logic) are stored in main memory 308, secondary storage 314 and/or removable storage unit 320. Such computer programs, when executed, enable computer 302 to perform the functions of the present invention as discussed herein. In particular, the computer programs, when executed, enable processor 304 to perform the functions of the present invention. Accordingly, such computer programs represent controllers of computer 302.

In another embodiment, the invention is directed to a computer program product comprising a computer readable medium having control logic (computer software) stored therein. The control logic, when executed by processor 304, causes processor 304 to perform the functions of the invention as described herein.

In another embodiment, the invention is implemented primarily in hardware using, for example, a hardware state machine. Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

Computer 302 also includes input devices 322 and display devices 324. Input devices 322 include a keyboard, a mouse, a microphone, a camera, etc. Display devices 324 include a computer monitor, a printer, a speaker, a projector, etc.

2. *A Preferred Software Programming Language and Network Architecture*

As discussed above, computer programs when executed, enable computer 302 to perform the functions of the present invention as discussed herein. In a preferred embodiment, the present invention is implemented using computer programs written in an object-oriented programming language. Object-oriented programming is a type of programming in which programmers define not only the data type of a data structure, but also the types of operations (functions) that can be applied to the data structure. In this way, the data structure becomes an object that includes both data and functions. In addition, programmers can create relationships between one object and another. For example, objects can inherit characteristics from other objects.

One of the principal advantages of object-oriented programming techniques over procedural programming techniques is that they enable programmers to create modules that do not need to be changed when a new type of object is added. A programmer can simply create a new object that inherits many of its features from existing objects. This makes object-oriented programs easier to modify. To perform object-oriented programming, one needs an object-oriented programming language (OOPL). C++ and Smalltalk are two of the more popular languages, and there are also object-oriented versions of Pascal.

While a preferred embodiment of the present invention is implemented using computer programs written in an object-oriented programming language, the present invention can also be implemented using procedural programming languages, etc.

As discussed above, one or more of computers 302 is connected by a network. A preferred embodiment of the present invention uses a type of network architecture called a peer-to-peer object architecture. Before peer-to-peer object architecture can be understood, a type of network architecture called client/server architecture must be described. Client/server architecture is a network architecture in which each computer or process on the network is either a client or a server. Servers are computers or processes dedicated to managing disk drives (file servers), printers (print servers), applications/functions or network traffic (network servers). In fact, a server is any computer or device that allocates resources for an application. Clients are personal computers or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, execution of functions and even processing power.

FIG. 4 illustrates the dynamic steps to establish communication that occur between a client and a server executing an object-oriented program. In FIG. 4A, the client has switchboard object 402 and listen object 404 waiting for a request from the server. In FIG. 4B, init object 406 determines that it needs to perform a specific task. In FIG. 4C, init object 406 creates comm object 408. Comm object 408 is used to communicate with the client. Then, comm object 408 makes a connection to listen object 404 in FIG. 4D. Once comm object 408 makes the connection, listen object 410 creates comm object 410 and relocates comm object 410 to switchboard object 402. Comm object 410 is used to communicate back to the server (i.e., between the two piers), via comm object 408.

At this point, as shown in FIG. 4F, there is two-way communication between the client and the server (i.e., between the two piers) through comm object 408 and comm object 410. Init object 406 knows which receiver object needs to be created by the client (i.e., receiving pier) to preform the specific task required. Therefore, once this communication is established, init object 406 sends a request to the client (i.e., receiving pier) to create the specific receiver object. In FIG. 4G, switchboard object 402 receives the request, via comm object 410, and creates receiver object 412. Once receiver object 412 is created, comm object 410 is relocated to receiver object 412 in FIG. 4H. Now, as shown in FIG. 4I, init object 406 and receiver object 412, via comm object 408 and comm object 410, can communicate back and forth until receiver object 412 completes the task requested by init object 406.

As stated above, a preferred embodiment of the present invention uses a type of network architecture called a peer-to-peer object architecture. A peer-to-peer object architecture is when each computer in the network has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Therefore, in a preferred embodiment of the present invention, all computers 302 can operate as either a server or a client.

As discussed above, one advantage of using an object-oriented programming language is that it allows programmers to create modules that do not need to be changed when a new type of object is added. This advantage will be further illustrated as the present invention is described in detail.

C. Biometric Server Data of the Present Invention

As stated above, biometric server 104 of FIG. 1 is the engine of biometric system 102. In fact, it is this engine that ultimately determines whether or not a user is authenticated by biometric system 102. In addition, biometric server 104 stores data accessed by biometric system 102. The data stored in biometric server 104 can be configured in one of two ways. One way is through the use of a database. The other way is through the use of a directory.

The first way that data in biometric server 104 can be configured involves the use of a database to facilitate access to the data. In general, a database is a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database is similar to an electronic filing system. To access information from a database, you need a database management system (DBMS). This is a collection of programs that enables you to enter, modify organize, and select data in a database.

Traditional databases are organized by tables, fields, records, and files. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address, and telephone number.

An alternative concept in database design is known as Hypertext. In a Hypertext database, any object, whether it be a piece of text, a picture, or a film, can be linked to any other object. Hypertext databases are particularly useful for organizing large amounts of disparate information, but they are not designed for numerical analysis.

The present invention may also be implemented using a standard database access method called Open DataBase Connectivity (ODBC). The goal of ODBC is to make it possible to access any data from any application, regardless of which DBMS is handling the data. ODBC manages this by inserting a middle layer, called a database driver , between an application and the DBMS. The purpose of this layer is to translate the application's data queries into commands that the DBMS understands. For this to work, both the application and the DBMS must be ODBC-compliant – that is, the application must be capable of issuing ODBC commands and the DBMS must be capable of responding to them.

The second way that data in biometric server 104 can be configured involves the use of a directory to facilitate access to the data. A preferred embodiment of the present invention utilizes a hierarchical directory called a X.500 directory. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. In addition to utilizing a X.500 directory, a Lightweight Directory Access Protocol (LDAP) may also be utilized.

LDAP is a set of protocols for accessing directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

In the following sections, the various collections of data stored in biometric server 104 are first discussed with reference to FIG. 5. Next, with reference to FIG. 6, a typical sequence of steps an administrator may take to initially setup biometric server 104 is discussed. Engine functions of biometric server 104 is discussed in Section D with reference to FIGs. 7-13.

1. Data Stored in Biometric Server

In FIG. 5, biometric server 104 (FIG. 1) stores collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. One or more unique biometric template 502 is created and stored in biometric server 104 each time a user enrolls on a different biometric device. Biometric template 502 stores the user's unique biometric measurement for a particular biometric device, which is then used to match against the user's "live" biometric measurement when the biometric device is attempting to identify the user.

Biometric policies 504 determine the method or way in which a user is to be authenticated by biometric server 104. Specific pre-defined policies provided by the present invention include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. The present invention also allows the administrator to define other biometric policies 504. The specific way in which each policy is executed is described later in detail.

Each pre-defined biometric policy 504 has a list of devices associated with it. The list of devices identifies the biometric devices that are used to execute the particular biometric policy 504. Each biometric device in the list of devices has a threshold value and a timeout value associated with it. The threshold value (e.g., false acceptance rate) indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

Each administrator defined biometric policy 504 can either have a list of biometric policies or a list of policies or devices. The list of biometric policies identifies the biometric policies that are used to execute the particular biometric policy 504. The list of policies or devices identifies the biometric policies and/or devices that are used to execute the particular biometric policy 504.

FIG. 5 illustrates that biometric groups 506 are also stored in biometric server 104. Biometric groups 506 are a logical way of combining one or more users that need access to the same set of resources. For example, all users in the accounting department of an enterprise need specific resources to perform accounting tasks. Therefore, one of biometric group 506 can be defined as "accounting group." Here, when a user is put into "accounting group," that user (once authenticated by biometric system 102) has access to the same resources as all the other users in "accounting group."

Each user can be put into one or more biometric groups 506. When the user attempts to gain access to a resource in a particular group, the user must be authenticated by whichever biometric policy 504 is associated with that particular group. When a user first attempts to log into network system 202, biometric system 102 may be implemented so that the user has a default biometric group 506 and is therefore first authenticated by the biometric policy 504 associated with the user's default biometric group 506. An example of default biometric groups 506 may be dependent on the location from which the user is attempting to gain access to network system 202. Possible different locations include from a location within network system 202 itself and from a remote location outside of network system 202.

Another way in which multiple biometric groups 506 for a single user may be implemented in biometric system 102 is to query the user for the biometric group 506 in which the user wishes to be authenticated into. An additional way is for biometric system 102 to prioritize each user's biometric groups 506. Here, if the user is authenticated by biometric system 102 into a biometric group 506 with a higher priority, then the user is automatically authentication into the user's biometric groups 506 that have a lower priority. One possible way in which the priority scheme may be implemented is to give a higher priority to biometric groups 506 that the most difficult biometric policies 504 associated with them.

A biometric device ID 508 identifies a biometric device. Each biometric device has a unique ID. Thus, the collection of biometric device IDs 508 of FIG. 5 allows the present invention to uniquely identify each biometric device in network system 102 (FIG. 2). Similarly, a user ID 510 uniquely identifies a user in network system 102.

As discussed above, various points a user may be required to be authenticated at by biometric system 102 include network system 202, one or more host computers, application 204 and/or user computer 208 of FIG. 2. Each computer 208 and application 204 within network system 202 must be registered. This registration is done by assigning unique IDs to each computer 208 and application 204, as will be discussed below. A computer ID 512 uniquely identifies each computer 208 in network system 202. Similarly, an application ID 514 uniquely identifies each application 204 in network system 202. Thus, collections of computer IDs 512 and application IDs 514 allow the present invention to uniquely identify each location in network system 120 that a user may be required to be authenticated at by biometric system 102.

2. *Setup of Biometric Server Data*

In the present invention, preferably the administrator of biometric system 102 determines the data that is stored in biometric server 104. FIG. 6 is a flowchart illustrating a typical sequence of steps an administrator may take to initially setup biometric server 104. In step 602, a unique computer ID 512 is assigned to each computer in network system 202. In step 603, a unique application ID 514 is assigned to each application in network system 202. Similarly, in step 604, a unique biometric device ID 508 is assigned to each biometric device in network system 202. Next, as shown in step 606, a determination is made as to which biometric devices will be attached to each computer 208 (FIG. 2).

In step 608, biometric groups 506 to be used within biometric system 102 are defined. In particular, the administrator defines each biometric group 504 by determining a logical grouping of resources within network system 202 that each member of that biometric group 504 will need to access. Next, in step 610, biometric policies 504 are defined. Each biometric policy 504 has associated with it a list of devices. Biometric policies 504 determine the method or way in which a user is to be authenticated by biometric server 104. One biometric policy 504 is assigned to each biometric group 506 in step 612. In step 613, one biometric policy 504 is assigned to each application ID 514.

In step 614, for every user that needs to gain access to network system 202 resources, the user is assigned a unique user ID 510. Then, each new user is put into a biometric group 506 in step 616. Once the user's biometric group 506 is determined, then in step 618, the types of devices the user needs to be enrolled in are determined by looking at the biometric policy 504 assigned to the user's biometric group 506. Once it is known which biometric policy 504 will be applied, a biometric template 502 is created for each biometric device 508 associated with the biometric policy 504 by enrolling the user in each device. This is shown in step 620. Alternatively, a biometric template 502 can be created for each biometric device within network system 202. Finally, in step 622, each computer ID 512, biometric device ID 508, biometric group 506, biometric policy 504, user ID 510, biometric template 502 and application ID 514 is stored in biometric server 104.

The steps shown in FIG. 6 can be performed in a variety of orders as should be apparent to those skilled in the art. Once biometric server 104 is setup (i.e., biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514 are all defined) the administrator interacts via a graphical user interface (GUI) to customize biometric server 104.

FIG. 14 is a sample window or screen shot generated by the GUI of the present invention. FIG. 14 illustrates the data stored in biometric server 104 as being logically stored in five tree structures (with the exclusion of application IDs 514). The five tree structures include biometric users tree 1402, biometric groups tree 1404, biometric computers tree 1406, biometric policy tree 1408 and biometric devices tree 1410. Biometric users tree 1402 includes a list of user IDs 510 registered by the administrator. As illustrated in FIG. 14, "Administrator" and "bobs" are two examples of user IDs 510. Biometric groups tree 1404 includes a list of biometric groups 506 as defined by the administrator. Examples of biometric groups include "Account Operators" and "Administrators."

Biometric computers tree 1406 includes a list of computer IDs 512. The list of computer IDs 512 represent the computers registered by the administrator. Examples of computer IDs 512 includes "BSCLAPTOP" and "BSCLAPTOP1." The fourth tree illustrated in FIG. 14 is biometric policy tree 1408. Biometric policy tree 1408 includes the list of both pre-defined and administrator-defined biometric policies 504. Pre-defined biometric policies 504 include "OR policy," "AND policy," "CONTINGENT policy," "RANDOM policy" and "THRESHOLD policy." Finally, biometric devices tree 1410 includes a list of biometric device IDs 508 registered by the administrator. Examples of biometric device IDs include "BSC Password Device" and "Visionics FaceIt."

An additional tree structure not shown in FIG. 14 is an application tree. As discussed above, a user may be required to be authenticated if the user attempts to access a particular application associated with a biometric policy 504. Although an application tree is not shown in the sample window of FIG. 14, the GUI of the present invention may be modified to include not only an application tree, but any other type of tree the administrator may deem to be desirable.

The present invention also allows for an administrator to define information groups. Information groups are a logical way of combining users that need access to the same types of information within each application in network system 202. For example, one possible type of application within network system 202 is a database containing information about each user. The administrator of biometric system 102 may determine that only the human resource department should have access to user medical information. Here, one information group can be defined as "medical information." The users put into "medical information" are only those users in the human resource department. Therefore, a biometric policy 504 can be associated either directly with an application ID or with an information group to authenticate users prior to allowing them access to information in applications.

The present invention, through the use of the GUI, is preferably implemented as a "drag and drop" application. "Drag and drop" applications allow an administrator to drag objects to specific locations on the screen to perform actions on them. For example, in the Macintosh environment, you can drag a document to the trashcan icon to delete it. This is a classic case of "drag and drop" functionality. When implemented well, drag-and-drop functionality is both faster and more intuitive than alternatives, such as selecting options from a menu or typing in commands. Nevertheless, the present invention is not limited to being implemented as a "drag and drop" application.

Referring back again to FIG. 14, an example of "drag and drop" functionality is the ability of the administrator to drag the "OR Policy" to the "Administrators" biometric group to either define or redefine the policy for that group. Another example includes dragging user ID "Administrator" to the "Administrators" biometric group. Now, the user who has user ID "Administrator" must pass the "OR Policy" to be authenticated by biometric system 102 (FIG. 1).

The administrator may also drag a biometric policy 504 to an application ID 514 (not shown in FIG. 14). For example, if the administrator drags the "AND Policy" to a particular application ID, then every user who attempts to access the application that the application ID is assigned to must pass the "AND Policy." Thus, the present invention provides different levels of authentication granularity. For example, a particular user may be assigned to a biometric group 506 that allows access to a spreadsheet if the user passes two biometric devices. However, to gain access to a payroll application, the user must also pass a third biometric device. Users that are not members of the biometric group 506 do not even have the opportunity to access the payroll application. The present invention provides complete flexibility to protect network resources.

As mentioned above in reference to FIG. 6, in step 620, a biometric template 502 is created for the user for each biometric device that is determined to be in the list of devices associated with a biometric policy 504 that is further associated with the user's biometric group 506. Therefore, there is a possibility that a user may not be enrolled in a particular biometric device that the user is required to pass in order to gain access to a particular application. This situation occurs when the biometric policy 504 that is assigned to the user's biometric group 506 and the biometric policy 504 that is assigned to the application ID 514 have different biometric devices in their list of devices. One way to avoid such a situation is to enroll the user with every biometric device in biometric system 102 and not just with the biometric devices that are determined to be in the biometric policy 's 504 list of devices that is associated with the user's biometric group 506. As illustrated above, various duties exist within biometric system 102. The discussion above infers that it is the administrator who performs all of these duties. In actuality, these duties can be delegated to multiple people having different positions within biometric system 102 (FIG. 1). These positions can include an administrator (with limited duties from the ones described above), a biometric policy manager, a device hardware and software manager and an enrollment manager. The administrator has actual administrative privileges within biometric system 102. The actual duties of the administrator could be limited to the adding and deleting of users, biometric groups 506 (FIG. 5), computers 208 (FIG. 2) and applications 204 (FIG. 2) with biometric system 102. Another position within biometric system 102 is the biometric policy manager. This position is akin to a security officer. The biometric policy manager is responsible for defining biometric policies 504 and attaching them to both biometric groups 506 and application IDs 514. The biometric policy manager would also be responsible for the combinations of biometric devices and for the strength of the threshold value associated with each biometric device.

Another position within biometric system 102 is a device hardware and software manager. This person is responsible for managing the software and hardware for biometric devices within biometric system 102. The device hardware and software manager will install the biometric devices, keep the versions up to date and maintain the devices. The final position is an enrollment manager. This person is given the ability to enroll users onto biometric system 102. Responsibility includes taking the new users through the process of enrolling for the different devices. The enrollment manager is generally a nontechnical person working in the human resource department of an enterprise. For simplicity, the following discussion will refer only to an administrator. It should be understood that the administrator may be one person performing one, all, or any number of the positions described above.

D. Biometric Server Functions of the Present Invention

In one embodiment of the present invention, biometric server 104 is implemented as computer 302 operating as described in reference to FIG. 3 above. Computer 302 executes computer programs to enable it to perform the functions of the present invention. Thus, biometric server 104 executes computer programs to perform its functions. As discussed above, the computer programs executed by biometric server 104 are preferably written in an object-oriented programming language and executed in a peer-to-peer object architecture.

An advantage of any object-oriented program, and thus also with computer programs executed by biometric server 104, is that they enable programmers to create modules that do not have to be changed when a new type of object is added. An object includes both the data and functions required to perform a task. Thus, by implementing the functions to be performed by biometric server 104 as objects, created modules do not need to be changed when a new type of object (or function) is added. This implementation of the present invention reduces complexity and thus increases efficiency. This interchangeability of functions (implemented as objects) of the present invention is explained in more detail in reference to FIGs. 7, 8, 12 and 13 below.

Described above with reference to FIG. 4, is the dynamic steps involved in establishing communication between a client and a server executing an object-oriented program. As biometric server 104 of the present invention executes its various functions, the same dynamic steps involved in communication between the server and client occur for each function as shown in FIGs. 4A through 4I. FIG. 4 shows a generic init object 406 and a generic receiver object 412. As is shown in FIGs.7 and 12, for each type of function performed by biometric server 104, init object 406 and receiver object 412 are replaced by specific init and receiver objects that perform their specific functions.

The types of functions performed by biometric server 104, through the execution of computer software, includes authenticating a user and enrolling a user. For simplicity, the figures used to illustrate the individual functions of biometric server 104 do not include switchboard object 402 and listen object 404 of FIG. 4.

1. Authenticating a User

FIG. 7 is a block diagram of the objects involved in authenticating a user of the present invention. As described above, a peer-to-peer object architecture is when each computer in the network has equivalent capabilities and responsibilities (e.g., a single computer can perform as a server and then at other times perform as a client). This allows for each computer in the network to initiate communication with any other computer in the network. FIG. 7 includes biometric server 104 (FIG. 1), computer 208 (or alternatively remote/web computer 210, both from FIG. 2), authentication interface 704, authentication interface 706, authentication object 708, database object 710, policy object 712, comm object 716, comm object 718, authentication object 720 and biometric device object 722. Here, biometric server 104 is performing as the server and computer 208 is performing as the client.

It is important to note that authentication interface 704 and authentication interface 706 are not part of the present invention. In fact, authentication interface 704 and authentication interface 706 are specific to the particular operating system and/or application the present invention is interfacing with. In general, operating systems provide a software platform on top of which other programs, called applications, can run. Applications must be written to run on top of a particular operating system. The choice of operating system, therefore, determines to a great extent the applications that can be run. Examples of operating systems include Windows NT, UNIX and Solaris. The present invention interfaces with the applicable operating system through application interface 706.

Authentication object 708 replaces init object 406 (FIG. 4). Authentication object 708 is used to request computer 208 to authenticate a user. Comm object 716 is attached to authentication object 708 and replaces comm object 408 (FIG. 4). Authentication object 708 and authentication object 720 communicate, via comm object 716 and comm object 718.

Policy object 712 is also attached to authentication object 708. Policy object 712 differs depending on the specific biometric policy 504 (FIG. 5). As discussed above, it is biometric policy 504 (FIG. 5) that determines the method or way in which a user is to be authenticated by biometric server 104. It is important to note that a user is not authenticated until he or she passes biometric policy 504. In the present invention, a user is never authenticated by solely passing one or more biometric devices without also passing his or her biometric policy 504. The type of communication between authentication object 708 and authentication object 720 is very dependent on the particular biometric policy 504 being used to authenticate the user.

In FIG. 7, database object 710 stores the data described above in reference to FIG. 5. The data includes collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. Authentication object 720 replaces receiver object 412 (FIG. 4). Authentication object 720 is used to perform the specific task requested by authentication object 708. Comm object 718 replaces comm object 410 (FIG. 4). Finally, biometric device object 722 is used to identify the user by determining if the user passes the biometric device. Biometric device object 722 differs depending on what biometric device the user is attempting to pass.

FIGs. 8A and 8B present a flowchart depicting the high-level operation of the objects in FIG. 7. In step 802, a user is at computer 208 and types in user ID 510 (FIG. 5) given to him or her by the administrator. Authentication interface 704 recognizes this as a login request. As mentioned above, to facilitate user access, each computer 208 provides an interface for users to be authenticated by biometric system 102 (FIG. 1). This interface is authentication interface 704. In step 804, authentication interface 704 sends the login request, which includes a computer ID 512 (FIG. 5) and user ID 510, to biometric server 104. Application interface 706 actually receives the login request. Based on the fact that the request is one for login, authentication object 708 gets initialized in step 806 (e.g., the login request starts the engine in biometric system 102). Prior to authentication object 708 being initialized, it is a generic init object 406 as described in reference to FIG. 4.

In step 808, authentication object 708 creates database object 710 and passes user ID 510 to it. Based on user ID 510, database object 710 determines the user's biometric group 506 (FIG. 5) in step 810. As described previously, the administrator has already determined which biometric group 506 the user is in. Based on biometric group 506, database object 710 determines the biometric policy 504 (FIG. 5) that is assigned to biometric group 506.

In step 811, database object 710 determines whether the required biometric templates 502 (FIG. 5) for the user are stored in biometric object 710 to execute the user's biometric policy 504. In addition, database object 710 also determines if computer 208 has the required biometric devices attached to it to execute the user's biometric policy 504. If the required biometric templates 502 or the required biometric devices do not exist, then control transfers to step 836. In step 836, biometric server 104 communicates, via authentication interface 706 and authentication interface 704, to computer 208 that the user cannot be authenticated. Authentication interface 704 then denies the user access. At this point the flowchart in FIGs. 8A and 8B ends. Alternatively, if in step 811 the required biometric templates 502 and the required biometric devices do exist, then control transfers to step 812.

In step 812, database object 710 creates policy object 712 and relocates policy object 712 to authentication object 708. Policy object 712 knows the specific type of biometric policy 504 (e.g. OR policy, AND policy, etc.), the list of devices for biometric policy 504 and the required biometric templates 502. There is one biometric template 502 for each biometric device ID (FIG. 5) 508 listed in the list of devices. Each biometric template 502 contains the user's stored biometric data to be used in testing the user on a particular biometric device. In addition, each biometric device in the list of devices has associated with it a threshold value and a timeout value. As explained above, the threshold value indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

In step 814, communication is established between biometric server 104 and computer 208. This communication is established exactly as described in reference to FIG. 4. In step 816, based on biometric policy 504 and its list of devices, authentication object 708 sends a request to computer 208 to test the user on a particular biometric device. The request includes biometric device ID

508, biometric template 502, the threshold value and the timeout value. Biometric template 502, the threshold value and the timeout value are all determined by user ID 510 and biometric device ID 508.

In step 818, based on the request, authentication object 720 is created. In step 820, authentication object 720 looks at biometric device ID 508 and creates biometric device object 722. Authentication object 720 then passes to biometric device object 722 biometric template 502, the threshold value and the timeout value. In step 822, biometric device object 722 tests the user on the specific biometric device and returns the results to authentication object 720. The results include a score and whether the user passed or failed the biometric device. Authentication object 720 then sends the results back to authentication object 708 in step 824, via comm object 718 and comm object 716.

In step 826, authentication object 708 looks at both the results and policy object 712 and determines whether the user passed biometric policy 504, failed biometric policy 504 or needs to be tested on another biometric device. Policy object 712 determines how many different biometric devices the user needs to be tested on. In step 828, if the user passed biometric policy 504, then control transfers to step 830. In step 830, the fact that the user passed biometric policy 504 is communicated, via authentication interface 706 and authentication interface 704, to computer 208. Authentication interface 704 then allows the user access to enterprise resources. Alternatively, if in step 828, the user did not pass biometric policy 504, then control transfers to step 832.

In step 832, if the user failed biometric policy 504, then control transfers to step 834. In step 834, the fact that the user failed biometric policy 504 is communicated, via authentication interface 706 and authentication interface 704, to computer 208. Authentication interface 704 then denies the user access to enterprise resources. Alternatively, if in step 832, the user did not fail biometric policy 504, then control transfers to step 836. In step 836, the next biometric device to test the user on is determined and another request is sent to authentication object 720. At this point control returns to step 820 and the user gets tested on the next biometric device. The flowchart in FIG. 8 continues until the user either passes or fails biometric policy 504.

Step 822 of FIG 8. is further explained in FIG. 9. FIG. 9 is a flowchart illustrating the typical operation of a biometric device as it tests a user. In step 902, the biometric device receives a request to test a user. The request includes the user's biometric template 502, a threshold value and a timeout value. Again, the threshold value and timeout value are user ID 510 and biometric device ID 508. In step 904, the biometric device prompts the user for "live" biometric data. In step 906, the biometric device attempts to read the "live" biometric data.

The biometric device, in step 908, determines whether or not the biometric data has been read. As discussed above, if the environment is not conducive for reading the particular biometric measurement (e.g., the environment has poor lighting and the biometric device is trying to read facial image data), then the biometric device may not be able to read the "live" biometric data. If the "live" biometric data has not been read in step 908, then in step 910, the actual time the biometric device has attempted to read the "live" biometric data is compared to the timeout value. If the actual time is greater than or equal to the timeout value, then control transfers to step 912 and the user fails the biometric device. Alternatively, if the actual time is less than the timeout value, then control transfers back to step 906 and the biometric device attempts to read the "live" biometric data again. This loop continues until either the "live" biometric data has been read or the actual time is greater than or equal to the timeout value (i.e., the time expires to read the "live" biometric data).

In step 908, if the "live" biometric data has been read, then control transfers to step 914. In step 914, a score is determined by matching the "live" biometric data with the data stored in biometric template 502. In step 916, the score determined by step 914 is compared to the threshold value. If the score is greater than or equal to the threshold value, then control transfers to step 918. In step 918, the user passes the biometric device and the flowchart in FIGs. 8A and 8B ends. Alternatively, in step 916, if the score is less than the threshold value then control passes to step 920. In step 920, the actual time is once again compared to the timeout value. If the actual time is greater than or equal to the timeout value, then control transfers to step 922 and the user fails the biometric device. At this point the flowchart in FIG 9 ends. If the actual time is less than the timeout value, then control transfers back to step 906 and the device attempts again to read the "live" biometric data.

The process described above to authenticate a user shows biometric template 502 being matched on the client side (i.e., at computer 208). While this is a preferred embodiment of the present invention, it is important to recognize that biometric template 502 can just as easily be matched on the server side (i.e., at biometric server 104).

As pointed out above, it is the login request that starts the engine in biometric system 102 to authenticate a user. The login request is initiated by a user typing in a user ID 510 (FIG. 5). In another embodiment of the present invention, it is "live" biometric data that identifies the user and starts the engine in biometric system 102 to authenticate a user. FIG. 10 is a block diagram of the objects involved in starting the authentication process of the present invention with "live" biometric data. FIG. 10 includes computer 208 (or alternatively remote/web computer 210, both from FIG. 2), monitor object 1004, biometric device object 1006, identify user ID object 1008 and database object 1010.

Monitor object 1004 is provided by the present invention for each computer 208 in the enterprise where the administrator desires to have "live" biometric data start off the engine in biometric system 102 to authenticate a user. Monitor object 1004 is up and waiting for "live" biometric data to be presented. In addition, monitor object 1004 is specialized (e.g., a fingerprint monitor object waits for "live" fingerprint data and a facial image monitor object waits for "live" facial image data).

FIG. 11 presents a flowchart depicting the high-level operation of the objects in FIG. 10. In step 1102, monitor object 1004 is waiting for "live" biometric data to be presented. In step 1104, once "live" biometric has been presented, monitor object 1004 creates biometric device object 1006. Because monitor object 1004 is specialized, there is no need for monitor object 1004 to be aware of any biometric device IDs 508 (FIG. 5). In step 1106, biometric device object 1006 causes a biometric device to read the "live" biometric data. This "live" biometric gets returned to monitor object 1004.

In step 1108, monitor object 1004 sends an identify request to identify user ID object 1008. The identify request includes the "live" biometric data and computer ID 512 (FIG. 5). The "live" biometric data is used to to identify user ID object 1008 on biometric server 104 (FIG. 1). Computer ID 512 uniquely identifies computer 208. Although not illustrated in FIGs. 10 and 11 for simplicity reasons, the same steps in establishing communication between objects must occur as shown in FIG. 4. In step 1110, identify user ID object 1008 creates a database object 1010 and passes to it the "live" biometric data. Database object 1010 contains the same data as described in reference to database object 710 in FIG. 7. In step 1112, an attempt is made to match the "live" biometric data with biometric data stored in a biometric template 502 (FIG. 5).

In step 1114, if a match was successful, then control transfers to step 1116. In step 1116, the user ID 510 (FIG. 5) that belongs to the matching biometric template 502 is determined. In step 1118, once user ID 510 is determined, then the authentication process proceeds as described in step 804 in FIG. 8. If in step 1114 a match was not successful, then control transfers to step 1120. In step 1120, the user is prompted to present "live" biometric data and control transfers back to step 1102. Because monitor object 1004 is always waiting for "live" biometric data to be presented, it does not matter if the same user presents the next "live" biometric data. Each time "live" biometric data is presented to monitor object 1004, it does not distinguish it from previously presented "live" biometric data.

2. *Enrolling a User*

As stated above, one of the advantages of object-oriented programming techniques over procedural programming techniques is that they enable programmers to create modules that do not need to be changed when a new type of object is added. This advantage is illustrated in FIG. 12. FIG. 12 is a block diagram of the objects involved in the enrollment process of the present invention. FIG. 12 includes biometric server 104 (FIG. 1), enrollment interface 1206, enrollment object 1208, comm object 1214, policy object 1212, database object 1210, enrollment station 106 (FIG. 1), enrollment interface 1204, enrollment object 1220, comm object 1218 and biometric device object 1222. Here, biometric server 104 is performing as the server and enrollment station 106 is performing as the client.

Enrollment station 106 is used to enroll users into biometric system 102. Enrollment station 106 has attached to it every type of biometric identification device used by biometric system 102 to identify and ultimately authenticate users.

It is important to note that enrollment interface 1204 and enrollment interface 1206 are not part of the present invention. In fact, enrollment interface 1204 and enrollment interface 1206 are specific to the particular operation system the present invention is interfacing with.

Enrollment object 1208 replaces init object 406 (FIG. 4). Enrollment object 1208 is used to request enrollment station 106 to enroll a user on a biometric device. Comm object 1214 is attached to enrollment object 1208 and replaces comm object 408 (FIG. 4). Enrollment object 1208 and enrollment object 1220 communicate, via comm object 1214 and comm object 1218.

Policy object 1212 is also attached to enrollment object 1208. Policy object 1212 is the same as policy object 712 (FIG. 7). As discussed above, it is the policy that determines the method or way in which a user is to be authenticated by biometric server 104. Database object 1210 stores the same data as database object 710 as described in reference to FIG. 7. Enrollment object 1220 replaces receiver object 412 (FIG. 4). Enrollment object 1220 is used to perform the specific task in enrolling a user on a biometric device. Comm object

1218 replaces comm object 410 (FIG. 4). Finally, biometric device object 1222 is used to enroll the user by requesting multiple samples of a particular type of "live" biometric data from the user. Biometric device object 1222 uses the samples of biometric data to create an unique biometric template 502 (FIG. 5) for the user.

FIG. 13 presents a flowchart depicting the high-level operation of the objects in FIG. 12. In step 1302, a user is at enrollment server 106 and types in user ID 510 (FIG. 5) given to the user by the administrator. Enrollment interface 1204 recognizes this as an enrollment request. To facilitate user enrollment, enrollment station 106 provides an interface for users to be enrolled by biometric system 102 (FIG. 1). This interface is enrollment interface 1204. In step 1304, enrollment interface 1204 sends an enrollment request, which includes computer ID 512 (FIG. 5) and user ID 510, to biometric server 104. Enrollment interface 1206 actually receives the enrollment request. Based on the fact that the request is one for enrollment, enrollment object 1208 gets initialized in step 1306 (e.g., the enrollment request starts the engine in biometric system 102). Prior to enrollment object 1208 being initialized, it is generic init object 406 as described in reference to FIG. 4.

In step 1308, enrollment object 1208 creates database object 1210 and passes user ID 510 to it. Based on user ID 510, database object 1210 determines the user's biometric group 506 (FIG. 5) in step 1310. As described previously, the administrator has already determined which biometric group 506 the user is in. Based on biometric group 506, database object 1210 determines the biometric policy 504 (FIG. 5) that is assigned to biometric group 506.

In step 1312, database object 1210 creates policy object 1212 and relocates policy object 1212 to enrollment object 1208. Policy object 1212 knows the specific type of biometric policy 504 (e.g. OR policy, AND policy, etc.) and its list of devices for that biometric policy 504. In step 1314, communication is established between biometric server 104 and enrollment station 106. This communication is established exactly as described in reference to FIG. 4. In step

1316, based on the list of devices, enrollment object 1208 sends a request to enrollment station106 to test the user on a particular biometric device. The request includes biometric device ID 508 (FIG. 5) that identifies the particular biometric device the user is to be enrolled in.

In step 1318, based on the request, enrollment object 1220 is created. In step 1320, enrollment object 1220 looks at biometric device ID 508 and creates biometric device object 1222. Biometric device object 1222 causes the biometric device to enroll the user in step 1322. In particular, the user is asked to give biometric measurements a few different times. For example, the user may be asked to give multiple fingerprint measurements for each finger. The enrollment of a user in a device creates a biometric template 502 (FIG. 5). In step 1324, enrollment object 1220 sends biometric template 502 to enrollment object 1208, via comm object 1218 and comm object 1214. Then, in step 1326, enrollment object 1208 stores biometric template 502 in database object 1210.

In step 1328, it is determined based on the list of devices, if the user needs to be enrolled in another biometric device. Although the user should at least be enrolled in the biometric devices listed in his or her list of devices, the administrator can decide to enroll the user in a biometric device not listed in the list of devices. If in step 1328, it is determined the user does not need to be enrolled in another biometric device, then control transfers to step 1330 and the flowchart in FIG. 13 ends. Alternatively, if the user does need to be enrolled in another biometric device, then control transfers to step 1332. In step 1332, the next biometric device to enroll the user in is determined and a request is sent to enrollment object 1220. The request includes biometric device ID 508 for the next biometric device. Control transfers again to step 1320. This process continues until the user is enrolled in all the required biometric devices.

As described with reference to FIGs. 12 and 13, in one embodiment of the present invention the user is enrolled through enrollment station 106. Typically, enrollment station 106 and the administrator are physically located at the same location within the enterprise. When a new user needs to enroll into the resource protection system, it may not be convenient for that user to physically be at the same location as administration. This presents two additional limitations for networked environments.

The first limitation deals with the use of any identification device. To enroll a user into biometric system 102 (FIG. 1) an administrator needs to be sure that the user enrolling is really the right person. This is difficult to do when the user and administrator are not physically at the same location.

The second limitation deals with the use of biometric identification devices. Many biometric measurements change over time. For example, people grow older, lose or gain weight, etc. In the case of biometric templates storing a user's facial image, the biometric data in the template may need to be updated from time to time. Once again, if the user and administrator are not physically at the same location in the network, the administrator needs to be sure the user requesting to update a template is really the person he or she says.

The inventors of the present invention recognized that what is needed is a scheme for remotely authenticating a user prior to allowing that user to either enroll or re-enroll with a particular biometric device to update a biometric template. Remote enrollment and/or re-enrollment (refreshing of biometric templates) can be either initiated by the administrator or the user.

There are several scenarios of where remote enrollment and/or re-enrollment is used. The first scenario already mentioned above is when the administrator and the user desiring to be enrolled or re-enrolled in biometric system 102 are not physically at the same location in the network. The administrator still needs to authenticate the user first. There are at least two possible solutions to this problem. The first involves assigning a temporary password (or token or smart card) to the user. The user goes to one of remote/web computers 210 (FIG. 2) and types in the password. Once biometric system 102 authenticates the user by the password, then the user starts the enrollment process. Of course, the temporary password expires after one use. In the case of re-enrollment (refreshing of templates) if the user is currently enrolled in multiple biometric devices, then one of the other biometric devices can be used to authenticate the user prior to allowing the user to refresh a biometric template 502 (FIG. 5) on the desired biometric device.

The second solution for remote enrollment and/or re-enrollment takes advantage of the fact that certain biometric devices are attached to remote/web computer 210. Several examples involve the use of facial image and voice recognition biometric devices. If an administrator is familiar with how the user looks, then the administrator can use video conferencing to authenticate the user prior to allowing the enrollment process to begin. If an administrator is familiar with the user's voice, then a voice recognition device can be used to speak to the administrator to authenticate the user.

A second scenario is when an enterprise desires not to use an administrator to enroll users into biometric system 102. Here, if the enterprise has an existing non-biometric identification system in place, it is easy to changeover from its existing system to biometric system 102. What is important to note is that the integrity of the existing non-biometric identification system must not be in question. For instance, if User B has access to another User A's password, then User B can enroll into biometric system 102 and gain access to User A's resources. Assuming the integrity of the existing identification system is good, then the method of authentication of the existing identification system is used to introduce the user to biometric system 102. Once the user is introduced to biometric system 102, the user can no longer gain access to enterprise resources through the old method. This is also important because it provides flexibility in rolling out biometric system 102 by not having to enroll all users at the same time.

E. Biometric Policies

The inventors of the present invention recognized a limitation when identification devices are used in any environment, whether or not the environment is networked. Enterprises with many resources have the desire to protect some resources more than others. For example, an enterprise may not care if its electronic bulletin board is accessed by every user in the enterprise. Whereas, an enterprise may want only the enterprise president to access merger and acquisition information. If an enterprise applies the same level of protection to all its resources, then one of two scenarios will occur. The first scenario is applying a lower-end level of protection to all resources. Here the result is inadequate authentication to some network resources. The second scenario is applying a higher-end level of protection to all resources. While this scenario may adequately protect all resources in the network, it would make the administration of resource protection more complex and thus decrease network productivity.

Biometric policies 504 (FIG. 5) of the present invention provides the flexibility to apply the appropriate level of protection to each network resource without decreasing network productivity. As discussed above, it is the biometric policies 504 of the present invention that determine the method or way in which a user is to be authenticated by biometric server 104 (FIG. 1). It is important to note that a user is not authenticated until he or she passes a biometric policy 504. In the present invention, a user is never authenticated by solely passing one or more biometric devices without the user also passing his or her biometric policy 504.

The specific way in which biometric policies 504 provide flexibility to the level of protection for each resource is through the layering of identification devices, including both biometric and non-biometric devices. The layering of identification devices allows the administrator of biometric system 102 (FIG. 1) to combine one or more identification devices in a logical way to protect each resource. Layering also allows the administrator to adjust the level of identification each biometric device must determine in order for the user to pass the biometric device. This is accomplished through threshold values as described above.

FIG. 15 is a chart illustrating an example of the layering process of biometric system 102 for a particular enterprise. Chart 1502 has columns and rows. Users can be required to be authenticated by biometric system 102 when they try to access various points in network system 202. The columns of chart 1502 represent the various points in network system 202. The various points (in this particular enterprise) include network system 202 itself, one or more of applications 204, one or more of user computers 208, Internet access 1504 and dial-in access 1506. The rows in chart 1502 represent the identification devices used in biometric system 102. The identification devices include both biometric and non-biometric devices. Non-biometric devices (in this particular enterprise) include password and smart card devices. Biometric devices (in this particular enterprise) include fingerprint, voice recognition, facial image and signature.

Once the administrator identifies the various points in network system 202 that require protection and the identification devices, the administrator determines the layering process of the present invention. The layering process for a single resource can include the steps illustrated by FIG. 16.

FIG. 16 is a flowchart that illustrates the process of layering for a single resource of the present invention. In step 1602, a resource in network system 202 that requires protection is identified. In step 1604, the non-biometric devices that are going to be utilized in protecting the resource are identified. Here, the administrator may decide to not use any non-biometric devices. In step 1606, the biometric devices that are going to be utilized in protecting the resource are identified. Again, the administrator may decide to use zero, one or more of the biometric devices. Finally, in step 1608, for each identified biometric device its threshold value is determined. Chart 1502 (FIG. 15) illustrates the possible values of threshold value as being L (low), M (medium) and H (high). The present invention is not limited to representing the values of threshold values this way. In fact, possible values of threshold values can be represented in other ways. One possible way is numerically where the threshold value can have as many different values as the administrator desires.

Referring again to FIG. 15, network system 202 is protected by two biometric devices and no non-biometric devices. The two biometric devices include a fingerprint device and a voice recognition device. Fingerprint device's threshold value is set at M. Voice recognition device's threshold value is set at L. Therefore, for a user to access network system 202, the user might *potentially* be tested on both a fingerprint device and a voice recognition device. When tested, the user might have to pass the fingerprint device with at least a M threshold value and pass the voice recognition device with at least a L threshold value.

The reason why the user might only *potentially* be tested on both devices is because ultimate authentication into biometric system 102 is governed by biometric polices 504. For example, an OR biometric policy would only require the user from above to pass either the fingerprint device or the voice recognition device. The only way the user will be tested on both devices is if the user fails the first device tested on. An AND biometric policy requires the user to be tested on both biometric devices to be authenticated. But even with the AND biometric policy the user may be tested on one of the biometric devices. If the user fails the first biometric device tested on, then the user automatically fails the AND policy and there is no need to test the user on the second biometric device.

Although biometric policies 504 have been introduced above, this section explains in detail the various pre-defined biometric policies and administrator-defined policies provided by the present invention. As explained above, each biometric policy has a list of devices associated with it. The list of devices identifies the biometric devices that are used to execute the biometric policy. Each biometric device in the list of devices has a threshold value and a timeout value associated with it. The threshold value indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

As stated above, the present invention not only provides specific pre-defined biometric policies but also allows the administrator to define other administrator-defined policies. The specific pre-defined biometric polices include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. The pre-defined biometric policies are limited to having only biometric devices in their list of devices. This limits being able to use non-biometric devices to protect a resource. Therefore, the present invention also provides administrator-defined policies having a list of policies or devices. An additional administrator-defined type of policy includes biometric policies within a policy. Described in detail below, are the pre-defined biometric policies and the administrator-defined policies.

1. OR Policy

The user passes an OR policy of the present invention if the user passes one of the biometric devices in the list of devices. FIG. 17 is a flowchart illustrating the steps involved in executing the OR policy of the present invention. In step 1702, the n number of biometric devices in the list of devices greater than two is determined. An OR policy will typically have at least two different biometric devices in its list of devices. In step 1704, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1706. In step 1708, the first score is compared to a first biometric device threshold value. If the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1710. In step 1710, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1708 the first score is less than the first biometric device threshold value, then control transfers to step 1712.

In step 1712, the second biometric device in the list of devices is determined. Once the second biometric device is determined, the user is tested on the second biometric device to produce a second score in step 1714. In step 1716, the second score is compared to a second biometric device threshold value.

If the second score is greater than or equal to the second biometric device threshold value, then control transfers to step 1718. In step 1718, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1716 the second score is less than the second biometric device threshold value, then control transfers to step 1720.

In step 1720, if n is not greater than zero, then control transfers to step 1722. If control transfers to step 1722 it means that the list of devices has only two biometric devices in it and the user has failed both biometric devices. In step 1722, the user has failed the OR policy and the flowchart in FIG. 17 ends. Alternatively, if in step 1720 n is greater than zero, then control transfers to step 1724. In this situation the list of devices has more than two biometric devices in it. In step 1724, the next biometric device is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 1726. In step 1728, the next score is compared to a next biometric device threshold value. If the next score is greater than or equal to the next biometric device threshold value, then control transfers to step 1730. In step 1730, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1728 the next score is less than the next biometric device threshold value, then control transfers to step 1732.

In step 1732, one is subtracted from n and control returns to step 1720. In step 1720, if n is not greater than zero then the user has failed all the biometric devices in the list of devices. Here, control transfers to step 1722. In step 1722, the user has failed the OR policy and the flowchart in FIG. 17 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1720 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 17 continues until the user has either failed all the biometric devices or the user passes one biometric device in the list of devices.

Although the OR policy will typically have at least two different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the OR policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the OR policy by being tested on the fingerprint device with the left index finger and by being tested on the fingerprint device with the right index finger. The user only needs to pass the fingerprint device using one of the biometric measurements to pass the OR policy. Other single biometric devices that can be used to test multiple biometric measurements are facial image (different angles of a face), retina image (right and left retina), hand geometry (right and left hand), voice recognition (two different phrases), different lighting (visible and infra red), etc.

2. *AND Policy*

The user passes an AND policy of the present invention if the user passes all of the biometric devices in the list of devices. FIG. 18 is a flowchart illustrating the steps involved in executing the AND policy of the present invention. In step 1802, the n number of biometric devices in the list of devices greater than two is determined. An AND policy will typically have at least two different biometric devices in its list of devices. In step 1804, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1806. In step 1808, the first score is compared to a first biometric device threshold value. If the first score is less than the first biometric device threshold value, then control transfers to step 1810. In step 1810, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1808 the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1812.

In step 1812, the second biometric device in the list of devices is determined. Once the second biometric device is determined, the user is tested on the second biometric device to produce a second score in step 1814. In step 1816, the second score is compared to a second biometric device threshold value. If the second score is less than the second biometric device threshold value, then control transfers to step 1818. In step 1818, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1816 the second score is greater than or equal to the second biometric device threshold value, then control transfers to step 1820.

In step 1820, if n is not greater than zero, then control transfers to step 1822. If control transfers to step 1822 it means that the list of devices has only two biometric devices in it and the user has passed both biometric devices. In step 1822, the user has passed the AND policy and the flowchart in FIG. 18 ends. Alternatively, if in step 1820 n is greater than zero, then control transfers to step 1824. In this situation the list of devices has more than two biometric devices in it. In step 1824, the next biometric device is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 1826. In step 1828, the next score is compared to a next biometric device threshold value. If the next score is less than the next biometric device threshold value, then control transfers to step 1830. In step 1830, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1828 the next score is greater than or equal to the next biometric device threshold value, then control transfers to step 1832.

In step 1832, one is subtracted from n and control returns to step 1820. In step 1820, if n is not greater than zero then the user has passed all the biometric devices in the list of devices. Here, control transfers to step 1822. In step 1822, the user has passed the AND policy and the flowchart in FIG. 18 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1820 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 18 continues until the user has either passed all the biometric devices or the user fails one biometric device in the list of devices.

Although the AND policy will typically have at least two biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the AND policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the AND policy by being tested on the fingerprint device with the left index finger and by being tested on the fingerprint device with the right index finger. The user needs to pass the fingerprint device using both of the biometric measurements to pass the AND policy. As mentioned above with the OR policy, the other single biometric devices can also be used with the AND policy to test multiple biometric measurements.

3. CONTINGENT Policy

The user passes a CONTINGENT policy of the present invention if either the user exceeds a minimum threshold (i.e., a first biometric device threshold value) associated with a first biometric device or if the user exceeds a contingent threshold associated with the first biometric device and the user exceeds a minimum threshold (i.e., a contingent biometric device threshold value) associated with a contingent biometric device. FIG. 19 is a flowchart illustrating the steps involved in executing the CONTINGENT policy of the present invention. The are typically two different biometric devices in the list of devices for the CONTINGENT policy. In step 1902, a contingent threshold value is determined. In step 1904, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1906.

In step 1908, the first score is compared to a first biometric device threshold value. If the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1910. In step 1910, the user has passed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1908 the first score is less than the first biometric device threshold value, then control transfers to step 1912.

In step 1912, the first score is compared to the contingent threshold value. In step 1912, if the first score is less than the contingent threshold value, then control transfers to step 1914. In step 1914, the user has failed the CONTINGENT policy. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1912 the first score is greater than or equal to the contingent threshold value, then control transfers to step 1916. The contingent threshold value is used to give the user a second chance to pass the CONTINGENT policy and thus be authenticated by biometric system 102.

In step 1916, the contingent biometric device in the list of devices is determined. The type of biometric device selected for the contingent biometric device may be based environmental conditions as discussed above. Once the contingent biometric device is determined, the user is tested on the contingent biometric device to produce a contingent score in step 1918. In step 1920, the contingent score is compared to a contingent biometric device threshold value. If the contingent score is less than the contingent biometric device threshold value, then control transfers to step 1924. In step 1924, the user has failed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1920 the contingent score is greater than or equal to the contingent biometric device threshold value, then control transfers to step 1922. In step 1922, the user has passed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has been authenticated by biometric system 102.

Although the CONTINGENT policy will typically have two biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the CONTINGENT policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the CONTINGENT policy by being tested on the fingerprint device with the user's left index finger first. If the user passes the fingerprint device with his or her left index finger, then the user passes the CONTINGENT policy. If the user fails the fingerprint device with his or her left index finger, and the first score is greater than or equal to the contingent threshold value score, the user is tested on the fingerprint device with the right index finger. As mentioned above with the OR policy, the other single biometric devices can also be used with the CONTINGENT policy to test multiple biometric measurements.

4. RANDOM Policy

The user passes a RANDOM policy of the present invention if the user passes a random biometric device. FIG. 20 is a flowchart illustrating the steps involved in executing a RANDOM policy of the present invention. In step 2002, the n number of biometric devices in the list of devices is determined. A RANDOM policy will typically have at least two different biometric devices in its list of devices. In step 2004, a random number from one to n is picked and the random number is set equal to x. In step 2006, the ✗ biometric device in the list of devices is determined. Once the ✗ biometric device is determined, the user is tested on the ✗ biometric device to produce a score in step 2008.

In step 2010, the score is compared to a biometric device threshold value. If the score is less than the biometric device threshold value, then control transfers to step 2012. In step 2012, the user has failed the RANDOM policy and the flowchart in FIG. 20 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2010 the score is greater than or equal to the biometric device threshold value, then control transfers to step 2014. In step 2014, the user has passed the RANDOM policy and the flowchart in FIG. 20 ends. At this point the user has been authenticated by biometric system 102.

The RANDOM policy is used to request a random biometric measurement from the user each time the user attempts to be authenticated by biometric system 102. Another embodiment of the RANDOM policy is to modify the list of devices to be a list of either fingerprints or word phrases. Here, the user may be tested on a random fingerprint (e.g., the index finger of the user's left hand). Alternatively, the user may be tested on a random word phrase (e.g., "My name is Bob Smith.").

Although the RANDOM policy will typically have at least two different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with any one of multiple biometric measurements to pass the RANDOM policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the RANDOM policy by being tested on any one of the user's fingers. If the user passes the fingerprint device with the random finger, then the user passes the RANDOM policy. As mentioned above with the OR policy, the other single biometric devices can also be used with the RANDOM policy to test multiple biometric measurements.

5. *THRESHOLD Policy*

The user passes a THRESHOLD policy of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more biometric devices in the list of devices. FIG. 21 is a flowchart illustrating the steps involved in executing a THRESHOLD policy of the present invention. In step 2102, the n number of biometric devices in the list of devices greater than one is determined. A THRESHOLD policy typically has one or more different biometric devices in its list of devices. In step 2104 a total threshold score is determined. In step 2106, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 2108.

In step 2110, a temp score is set equal to the first score. In step 2112, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 2114. In step 2114, the user has passed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2112 the temp score is less than the total threshold score, then control transfers to step 2116.

In step 2116, if n is not greater than zero, then control transfers to step 2118. In step 2118, the user has failed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2116 n is greater than zero, then control transfers to step 2120. In step 2120, the next biometric device in the list of devices is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 2122.

In step 2124, temp score gets multiplied by the next score and the product gets stored back into temp score. In another embodiment of the RANDOM policy, temp score may be added to the next score and the sum stored back into temp score. In step 2126, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 2128. In step 2128, the user has passed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2126 the temp score is less than the total threshold score, then control transfers to step 2130.

In step 2130, one is subtracted from n and control returns to step 2116. In step 2116, if n is not greater than zero then the user has been tested all the biometric devices in the list of devices. Here, control transfers to step 2118. In step 2118, the user has failed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2116 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 21 continues until the user has either been tested on all the biometric devices in the list of devices or temp score is greater than or equal to the total threshold score.

Although the THRESHOLD policy typically has one or more different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with any one of multiple biometric measurements to pass the THRESHOLD policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the THRESHOLD policy by being tested on multiple fingers until the total threshold score is reached. As mentioned above with the OR policy, the other single biometric devices can also be used with the THRESHOLD policy to test multiple biometric measurements.

6. *Biometric Policies Having a List of Biometric Policies*

As discussed above, the present invention allows for administrator-defined policies. Once type of administrator-defined policy is a biometric policy having a list of biometric policies. Here, instead of the biometric policy having a list of biometric devices as discussed above, this type of biometric policy has a list of biometric policies. The types of biometric policies that can be listed in the list of biometric policies include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy (all described above). This type of policy is also limited to testing a user on biometric devices only.

The other type of administrator-defined policy is a policy having a policy list of policies or devices. This administrator-defined policy allows for the use of non-biometric devices.

a. OR Policy Having a List of Biometric Policies

The user passes an OR policy having a list of biometric policies of the present invention if the user passes one of the biometric policies in the list of biometric policies. FIG. 22 is a flowchart illustrating the steps involved in executing the OR policy having a list of biometric policies of the present invention. In step 2202, the n number of biometric policies in the list of biometric policies greater than two is determined. The OR policy will always have at least two biometric policies in its list of biometric policies. In step 2204, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 2206. Here, the steps in the flowchart that applies to the first biometric policy are executed. For example, if the first biometric policy is a CONTINGENT policy, then the flowchart in FIG. 19 would be executed. Referring to FIG. 19, the outcome of FIG. 19 is either the user passes or fails the CONTINGENT policy. Therefore, this information gets returned to step 2206 of FIG. 22.

In step 2208, if the user passes the first biometric policy, then control transfers to step 2210. In step 2210, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2208 the user fails the first biometric policy, then control transfers to step 2212.

In step 2212, the second biometric policy in the list of biometric policies is determined. Once the second biometric policy is determined, the second biometric policy is executed in step 2214. Here, the steps in the flowchart that applies to the second biometric policy are executed. For example, the second biometric policy can be the same type of policy as the first biometric policy or it can be one of the other biometric policies.

In step 2216, if the user passes the second biometric policy, then control transfers to step 2218. In step 2218, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2216 the user fails the second biometric policy, then control transfers to step 2220.

In step 1220, if n is not greater than zero, then control transfers to step 2222. If control transfers to step 2222 it means that the list of biometric policies has only two biometric policies in it and the user has failed both biometric policies. In step 2222, the user has failed the OR policy and the flowchart in FIG. 22 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2220 n is greater than zero, then control transfers to step 2224. In this situation the list of biometric policies has more than two biometric policies in it. In step 2224, the next biometric policy is determined. Once the next biometric policy is determined, the next biometric policy is executed in step 2226.

In step 2228, if the user passes the next biometric policy, then control transfers to step 2230. In step 2230, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2228 the user fails the next biometric policy, then control transfers to step 2232.

In step 2232, one is subtracted from n and control returns to step 2220. In step 2220, if n is not greater than zero then the user has failed all the biometric policies in the list of biometric policies. Here, control transfers to step 2222. In step 2222, the user has failed the OR policy and the flowchart in FIG. 22 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2220 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 22 continues until the user has either failed all the biometric policies or the user passes one biometric policy in the list of biometric policies.

b. AND Policy Having a List of Biometric Policies

The user passes an AND policy having a list of biometric policies of the present invention if the user passes all of the biometric policies in the list of biometric policies. FIG. 23 is a flowchart illustrating the steps involved in executing an AND policy having a list of biometric policies of the present invention. In step 2302, the n number of biometric policies in the list of biometric policies greater than two is determined. This type of AND policy will always have at least two biometric policies in its list of biometric policies. In step 2304, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 2306. Here, the steps in the flowchart that applies to the first biometric policy are executed. For example, if the first biometric policy is a AND policy, then the flowchart in FIG. 18 would be executed. Referring to FIG. 18, the outcome of FIG. 18 is either the user passes or fails the AND policy. Therefore, this information gets returned to step 2306 of FIG. 23.

In step 2308, if the user fails the first biometric policy, then control transfers to step 2310. In step 2310, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2308 the user passes the first biometric policy, then control transfers to step 2312.

In step 2312, the second biometric policy in the list of biometric policies is determined. Once the second biometric policy is determined, the second biometric policy is executed in step 2314. Here, the steps in the flowchart that applies to the second biometric policy are executed.

In step 2316, if the user fails the second biometric policy, then control transfers to step 2318. In step 2318, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2316 the user passes the second biometric policy, then control transfers to step 2320.

In step 1320, if n is not greater than zero, then control transfers to step 2322. If control transfers to step 2322 it means that the list of biometric policies has only two biometric policies in it and the user has passed both biometric policies. In step 2322, the user has passed the AND policy and the flowchart in FIG. 23 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2320 n is greater than zero, then control transfers to step 2324. In this situation the list of biometric policies has more than two biometric policies in it. In step 2324, the next biometric policy is determined. Once the next biometric policy is determined, the next biometric policy is executed in step 2326.

In step 2328, if the user fails the next biometric policy, then control transfers to step 2330. In step 2330, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2328 the user passes the next biometric policy, then control transfers to step 2332.

In step 2332, one is subtracted from n and control returns to step 2320. In step 2320, if n is not greater than zero then the user has passed all the biometric policies in the list of biometric policies. Here, control transfers to step 2322. In step 2322, the user has passed the AND policy and the flowchart in FIG. 23 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2320 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 23 continues until the user has either passed all the biometric policies or the user fails one biometric policy in the list of biometric policies.

c. RANDOM Policy Having a List of Biometric Policies

The user passes a RANDOM policy having a list of biometric policies of the present invention if the user passes a random biometric policy. FIG. 24 is a flowchart illustrating the steps involved in executing the RANDOM policy having a list of biometric policies of the present invention. In step 2402, the n number of biometric policies in the list of biometric policies is determined. This type of RANDOM policy will always have at least two biometric policies in its list of biometric policies. In step 2404, a random number from one to n is picked and the random number is set equal to ✗. In step 2406, the ✗ biometric policy in the list of biometric policies is determined. Once the ✗ biometric policy is determined, the ✗ biometric policy is executed in step 2408. Here, the steps in the flowchart that applies to the first biometric policy are executed.

In step 2410, if the user passes the ✗ biometric policy, then control transfers to step 2412. In step 2412, the user has passed the RANDOM policy and the flowchart in FIG. 24 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2410 the user fails the ✗ biometric policy, then control transfers to step 2414. In step 2414, the user has failed the RANDOM policy and the flowchart in FIG. 24 ends. At this point the user has not been authenticated by biometric system 102.

The RANDOM policy having a list of biometric policies is used to request the user to pass a random biometric policy 504 each time the user attempts to be authenticated by biometric system 102.

d. CONTINGENT Policy Having a List of Biometric Policies

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a CONTINGENT policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a CONTINGENT policy having a list of biometric policies of the present invention if either the user exceeds a minimum threshold (i.e., a first composite threshold value) associated with a first biometric policy or if the user exceeds a contingent threshold associated with the first biometric policy and the user exceeds a minimum threshold (i.e., a contingent threshold value) associated with a contingent biometric policy. FIG. 31 is a flowchart illustrating the steps involved in executing the CONTINGENT policy having a list of biometric policies of the present invention. With this type of CONTINGENT policy there is always two biometric policies in the list of biometric policies.

In step 3102, a contingent threshold value is determined. In step 3104, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, then the first biometric policy is executed in step 3106. The results from the execution of the first biometric policy are whether or not the user passed the first biometric policy and a first composite threshold value.

In step 3108, whether the user passed the first biometric policy is determined. If the user passed the first biometric policy, then control transfers to step 3110. In step 3110, the user has passed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3108 the user failed the first biometric policy, then control transfers to step 3112.

In step 3112, the first composite threshold value is compared to the contingent threshold value. If the first composite threshold value is less than the contingent threshold value, then control transfers to step 3114. In step 3114, the user has failed the CONTINGENT policy. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3112 the first composite threshold value is greater than or equal to the contingent threshold value, then control transfers to step 3116. The contingent threshold value is used to give the user a second chance to pass the CONTINGENT policy and thus be authenticated by biometric system 102.

In step 3116, the contingent biometric policy in the list of biometric policies is determined. Once the contingent biometric policy is determined, then the contingent biometric policy is executed in step 3118. In step 3120, if the user passed the contingent biometric policy, then control transfers to step 3122. In step 3122, the user has passed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3120 the user failed the contingent biometric policy, then control transfers to step 3124. In step 3124, the user has failed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has not been authenticated by biometric system 102.

e. THRESHOLD Policy Having a List of Biometric Policies

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a THRESHOLD policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a THRESHOLD policy having a list of biometric policies of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more biometric policies in the list of biometric policies. FIG. 32 is a flowchart illustrating the steps involved in executing the THRESHOLD policy having a list of biometric policies of the present invention. In step 3202, the n number of biometric policies in the list of biometric policies greater than one is determined. This type of THRESHOLD policy can have one or more biometric policies in its list of biometric policies. In step 3204 a total threshold score is determined. In step 3206, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 3208. The results from the execution of the first biometric policy are whether or not the user passed the first biometric policy and a first composite threshold value.

In step 3210, a temp score is set equal to the first composite threshold value. In step 3212, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 3214. In step 3214, the user has passed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3212 the temp score is less than the total threshold score, then control transfers to step 3216.

In step 3216, if n is not greater than zero, then control transfers to step 3218. In step 3218, the user has failed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3216 n is greater than zero, then control transfers to step 3220. In step 3220, the next biometric policy in the list of biometric policies is determined. Once the next biometric policy is determined, the next biometric policy gets executed in step 3222. The results from the execution of the next biometric policy are whether or not the user passed the next biometric policy and a next composite threshold value.

In step 3224, temp score gets multiplied by the next composite threshold value and the product gets stored back into temp score. In step 3226, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 3228. In step 3228, the user has passed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3226 the temp score is less than the total threshold score, then control transfers to step 3230.

In step 3230, one is subtracted from n and control returns to step 3216. In step 3216, if n is not greater than zero then all the biometric policies in the list of biometric policies have been executed. Here, control transfers to step 3218. In step 3218, the user has failed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3216 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 32 continues until all the biometric policies in the list of biometric policies have been executed or temp score is greater than or equal to the total threshold score.

7. *Biometric Policies having a List of Policies or Devices*

The other type of administrator-defined policy is a biometric policy with a policy list of policies or devices. This administrator-defined policy allows for the combined use of biometric devices, non-biometric devices and/or biometric policies. This type of policy gives added flexibility that all the other policies mentioned above do not provide. With this type of policy, it is possible for a user to be authenticated by biometric system 102 by being tested on a single non-biometric device. This is important because it provides flexibility in converting to biometric system 102 by not having to enroll all users at the same time with biometric devices. Here, a user can continue to use the non-biometric device the user has always used to log into biometric system 102.

There are two ways in which biometric system 102 provides flexibility in rolling out biometric system 102 by not having to enroll all users at the same time with biometric devices. The first way is by not assigning a user to a biometric group 506. Here, when biometric system 102 discovers that the user does not have a biometric group 506, the previous way of allowing users to gain access to enterprise resources (e.g., passwords, tokens or smart cards) takes control to authenticate the user. The second way is when the administrator has assigned the user to a biometric group 506. The second way involves an OR policy with a list of policies or devices of the present invention as described below.

If the user has been assigned to a biometric group 506, then the flexibility of not requiring all users to be enrolled in biometric devices at the same time requires a slight variation from what was described in reference to FIGs. 8A and 8B above. As described above, in step 811, database object 710 (FIG. 7) determines whether the required biometric templates 502 (FIG. 5) for the user are stored in biometric object 710 (FIG. 7) to execute the user's biometric policy 504 (FIG. 5). In addition, database object 710 also determines if computer 208 (FIG. 2) has the required biometric devices attached to it to execute the user's biometric policy 504. If the required biometric templates 502 or the required biometric devices do not exist, then control transfers to step 836. In step 836, biometric server 104 (FIG. 1) communicates to computer 208 that the user cannot be authenticated. Authentication interface 704 (FIG. 7) then denies the user access. Therefore, to provide the flexibility of not requiring all users to be enrolled in biometric devices at the same time, biometric server 104 knows when to skip over step 811 (e.g., a flag) and go directly to step 812 (FIGs. 8A and 8B).

a. OR Policy Having a List of Policies or Devices

The user passes an OR policy having a list of policies or devices of the present invention if the user passes one of the elements in the list of policies or devices. FIG. 25 is a flowchart illustrating the steps involved in executing the OR policy having a list of policies or devices of the present invention. In step 2502, the n number of elements in the list of policies or devices greater than two is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of OR policy will always have at least two elements in its list of polices or devices. In step 2504, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 2506.

In step 2506, the first element is either a biometric or a non-biometric device. FIGs. 8A, 8B and 9 involve the user being tested on a biometric device. Referring again to FIGs. 8A, 8B and 9, when a user gets tested on a biometric device, the result returned includes both a score and whether the user passed or failed the biometric device. The flowchart in FIG. 25 utilizes the information of whether the user passed or failed only. As with biometric devices, when the user is tested on a non-biometric device, the result includes whether the user passed or failed the non-biometric device. Thus, in step 2506, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2504, if the first element is a biometric policy, then control transfers to step 2508. In step 2508, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy). Whether the first element is a biometric policy or a device, controls transfers to step 2510.

In step 2510, if the user passes the first element, then control transfers to step 2512. In step 2512, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). An example of the flexibility biometric system 102 provides by not forcing all users to be enrolled in biometric system 102 at the same time can be illustrated here. Assume the non-biometric device the user has used in the past to gain access to enterprise resources is a password device. If the first element in the list of policies or devices is a password device, the user can be authenticated by biometric system 102 by passing the password device.

Alternatively, if in step 2510 the user fails the first element, then control transfers to step 2514. In step 2514, it is determined whether the second element in the list of policies or devices is a biometric policy. If the second element is not a biometric policy, then control transfers to step 2516. In step 2516, the second element is either a biometric or a non-biometric device. The user is tested on the second element and the result indicates whether the user passed or failed the second element (i.e, the device).

Alternatively, in step 2514, if the second element is a biometric policy, then control transfer to step 2518. The second element is executed to determine whether the user passes or fails the second element (i.e., the biometric policy). Whether the second element is a biometric policy or a device, controls transfers to step 2520. In step 2520, if the user passes the second element, then control transfers to step 2522. In step 2522, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2520 the user fails the second element, then control transfers to step 2524.

In step 2524, if n is not greater than zero, then control transfers to step 2526. If control transfers to step 2526 it means that the list of policies or devices has only two elements in it and the user has failed both elements. In step 2526, the user has failed the OR policy and the flowchart in FIG. 25 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2524 n is greater than zero, then control transfers to step 2528. In this situation the list of policies or devices has more than two elements in it.

In step 2528, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 2530. In step 2530, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device).

Alternatively, in step 2528, if the next element is a biometric policy, then control transfer to step 2532. The next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy). Whether the next element is a biometric policy or a device, controls transfers to step 2534. In step 2534, if the user passes the next element, then control transfers to step 2536. In step 2536, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2534 the user fails the next element, then control transfers to step 2538.

In step 2538, one is subtracted from n and control returns to step 2524. In step 2524, if n is not greater than zero then the user has failed all the elements in the list of policies or devices. Here, control transfers to step 2526. In step 2526, the user has failed the OR policy and the flowchart in FIG. 25 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2524 n is greater than zero, this means there are still more elements in the list of policies or devices. The flowchart in FIG. 25 continues until the user has either failed all the elements or the user passes one element in the list of policies or devices.

b. AND Policy Having a List of Policies or Devices

The user passes an AND policy having a list of policies or devices of the present invention if the user passes all of the elements in the list of policies or devices. FIG. 26 is a flowchart illustrating the steps involved in executing the AND policy having a list of policies or devices of the present invention. In step 2602, the n number of elements in the list of policies or devices greater than two is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of AND policy will always have at least two elements in its list of polices or devices. In step 2604, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 2606.

In step 2606, the first element is either a biometric or a non-biometric device. In step 2606, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2604, if the first element is a biometric policy, then control transfers to step 2608. In step 2608, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy). Whether the first element is a biometric policy or a device, controls transfers to step 2610.

In step 2610, if the user fails the first element, then control transfers to step 2612. In step 2612, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2610 the user passes the first element, then control transfers to step 2614. In step 2614, it is determined whether the second element in the list of policies or devices is a biometric policy. If the second element is not a biometric policy, then control transfers to step 2616. In step 2616, the second element is either a biometric or a non-biometric device. The user is tested on the second element and the result indicates whether the user passed or failed the second element (i.e, the device).

Alternatively, in step 2614, if the second element is a biometric policy, then control transfer to step 2618. The second element is executed to determine whether the user passes or fails the second element (i.e., the biometric policy). Whether the second element is a biometric policy or a device, controls transfers to step 2620. In step 2620, if the user fails the second element, then control transfers to step 2622. In step 2622, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2620 the user passes the second element, then control transfers to step 2624.

In step 2624, if n is not greater than zero, then control transfers to step 2626. If control transfers to step 2626 it means that the list of policies or devices has only two elements in it and the user has passed both elements. In step 2626, the user has passed the AND policy and the flowchart in FIG. 26 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2624 n is greater than zero, then control transfers to step 2628. In this situation the list of policies or devices has more than two elements in it.

In step 2628, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 2630. In step 2630, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device).

Alternatively, in step 2628, if the next element is a biometric policy, then control transfer to step 2632. The next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy). Whether the next element is a biometric policy or a device, controls transfers to step 2634. In step 2634, if the user fails the next element, then control transfers to step 2636. In step 2636, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2634 the user passes the next element, then control transfers to step 2638.

In step 2638, one is subtracted from n and control returns to step 2624. In step 2624, if n is not greater than zero then the user has passed all the elements in the list of policies or devices. Here, control transfers to step 2626. In step 2626, the user has passed the AND policy and the flowchart in FIG. 26 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2624 n is greater than zero, this means there are still more elements in the list of policies or devices. The flowchart in FIG. 26 continues until the user has either passed all the elements or the user fails one element in the list of policies or devices.

c. *RANDOM Policy Having a List of Policies or Devices*

The user passes a RANDOM policy having a list of policies or devices of the present invention if the user passes a random element. FIG. 27 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of policies or devices of the present invention. In step 2702, the n number of elements in the list of policies or devices is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of RANDOM policy will always have at least two elements in its list of polices or devices. In step 2704, a random number from one to n is picked and the random number is set equal to x. In step 2706, it is determined whether the ✗ element in the list of policies or devices is a biometric policy. If the ✗ element is not a biometric policy, then control transfers to step 2708.

In step 2708, the ✗ element is either a biometric or a non-biometric device. In step 2708, the user is tested on the ✗ element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2706, if the ✗ element is a biometric policy, then control transfers to step 2710. In step 2710, the ✗ element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the ✗ element (i.e., the biometric policy). Whether the ✗ element is a biometric policy or a device, controls transfers to step 2712.

In step 2712, if the user passes the ✗ element, then control transfers to step 2714. In step 2714, the user has passed the RANDOM policy and the flowchart in FIG. 27 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2712 the user fails the ✗ element, then control transfers to step 2716. In step 2716, the user has failed the RANDOM policy and the flowchart in FIG. 27 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1).

This type of RANDOM policy is used to request the user to pass a random biometric policy 504 or identification device each time the user attempts to be authenticated by biometric system 102.

d. CONTINGENT Policy Having a List of Policies or Devices

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a CONTINGENT policy having a list of policies or devices. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a CONTINGENT policy having a list of policies or devices of the present invention if either the user exceeds a minimum threshold associated with a first element or if the user exceeds a contingent threshold associated with the first element and the user exceeds a minimum threshold associated with a contingent element. FIG. 33 is a flowchart illustrating the steps involved in executing the CONTINGENT policy having a policy list of policies or devices of the present invention. This type of CONTINGENT policy always has two elements in the list of policies or devices. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device.

In step 3302, a contingent threshold value is determined. In step 3304, it is determined whether the first element is a biometric policy. If the first element is not a biometric policy, then control transfers to step 3306. In step 3306, the first element is either a biometric or a non-biometric device. FIGs. 8A, 8B and 9 involve the user being tested on a biometric device. Referring again to FIGs. 8A, 8B and 9, when a user gets tested on a biometric device, the result returned includes both a score and whether the user passed or failed the biometric device. As with biometric devices, when the user is tested on a non-biometric device, the result includes whether the user passed or failed the non-biometric device. This result can be modified to also include a score. Thus, in step 3306, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device) and a first score.

Alternatively, in step 3304, if the first element is a biometric policy, then control transfers to step 3308. In step 3308, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy) and a first composite threshold value. Whether the first element is a biometric policy or a device, control transfers to step 3310.

In step 3310, if the user passes the first element, then control transfers to step 3312. In step 3312, the user has passed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3310 the user fails the first element, then control transfers to step 3314. In step 3314, it is determined whether the first composite threshold value or the first score was returned and it is set equal to temp score.

In step 3316, it is determined whether temp score is less than the contingent threshold value. If the temp score is less than the contingent threshold value, then control transfers to step 3318. In step 3318, the user has failed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3316 it is determined that temp score is greater than or equal to the contingent threshold value, then control transfers to step 3320.

In step 3320, it is determined whether the contingent element is a biometric policy. If the contingent element is not a biometric policy, then control transfers to step 3322. In step 3322, the contingent element is either a biometric or a non-biometric device. Thus, in step 3322, the user is tested on the contingent element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the contingent element.

Alternatively, in step 3320, if the contingent element is a biometric policy, then control transfers to step 3324. In step 3324, the contingent element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the contingent element. Whether the contingent element is a biometric policy or a device, controls transfers to step 3326.

In step 3326, if the user passes the contingent element, then control transfers to step 3328. In step 3328, the user has passed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3326 the user fails the first element, then control transfers to step 3330. In step 3330, the user has failed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has not been authenticated by biometric system 102.

e. THRESHOLD Policy Having a List of Policies or Devices

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a THRESHOLD policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a THRESHOLD policy having a list of policies or devices of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more elements in the list of policies or devices. FIG. 34 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a policy list of policies or devices of the present invention. In step 3402, the n number of elements in the list of policies or devices greater than one is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of THRESHOLD policy will have one or more elements in its list of polices or devices. In step 3404, a total threshold score is determined. In step 3406, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 3408.

In step 3408, the first element is either a biometric or a non-biometric device. In step 3408, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device) and a first score.

Alternatively, in step 3406, if the first element is a biometric policy, then control transfers to step 3410. In step 3410, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy) and a first composite threshold value. Whether the first element is a biometric policy or a device, control transfers to step 3412.

In step 3412, it is determined whether the first composite threshold value or the first score was returned and it is set equal to temp score. In step 3414, if temp score is less than the total threshold score, then control transfers to step 3416. In step 3416, the user has passed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3414 the temp score is greater than or equal to the total threshold score, then control transfers to step 3418.

In step 3418, if n is not greater than zero, then control transfers to step 3420. If control transfers to step 3420 it means that the list of policies or devices has only one element. In step 3420, the user has failed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3418 n is greater than zero, then control transfers to step 3422. In this situation the list of policies or devices has more than one element in it.

In step 3422, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 3424. In step 3424, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device) and a next score.

Alternatively, in step 3422, if the next element is a biometric policy, then control transfer to step 3426. In step 3426, the next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy) and to get a next composite threshold value. In step 3428, it is determined whether the next composite threshold value or the next score was returned and it is set equal to temp2 score. In step 3430, temp score is multiplied temp2 score and the product is stored back in temp score.

In step 3432, if temp score is less than the total threshold score, then control transfers to step 3434. In step 3434, the user has passed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3432 the temp score is greater than the total threshold value, then control transfers to step 3436.

In step 3436, one is subtracted from n and control returns to step 3418. In step 3418, if n is not greater than zero then all the elements in the list of biometric policies have been executed. Here, control transfers to step 3420. In step 3420, the user has failed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3418 n is greater than zero, this means there are still more elements in the list of policies or devices that have not been executed. The flowchart in FIG. 34 continues until all the elements in the list of policies or devices have been executed or temp score is greater than or equal to the total threshold score.

8. Multi-User Biometric Policy

As described above, biometric groups 506 (FIG. 5) are a logical way of combining users that need access to the same set of resources. Some biometric groups 506 are important enough that the biometric policies 504 attached to them require one or more users to be authenticated by biometric system 102 (FIG. 1) to pass the biometric policy 504. This type of biometric policy 504 is called a multi-user biometric policy. The multi-user biometric policy has a list of users. Examples of where the multi-user biometric policy is useful are described next.

The first example involves the various duties that exist within biometric system 102. These duties can be delegated between different positions within biometric system 102. The different positions may include an administrator, a biometric policy manager, a device hardware and software manage and an enrollment manager. Each position must be given the proper authority within biometric system 102 to be able to perform the duties required of that particular position. One way that the proper authority can be given is to create a biometric group 506 for each of the positions. It is very important that only authorized users get put in these biometric groups 506. If an unauthorized user gets put in one or more of these biometric groups 506, then the security of biometric system

102 is compromised. The multi-user biometric policy of the present invention provides the flexibility required for biometric system 102 to ensure that only authorized users get put into one of these biometric groups 506.

The second example involves resources (e.g., computers, applications, data, etc.) within network system 202 (FIG. 2) that need to be protected with the highest security. This type of situation also occurs in non-networked environments. Historically, a bank protects its vault by requiring at least two people to know different parts of the combination in order to open the vault. The multi-user biometric policy of the present invention provides the flexibility required for both networked and non-networked environments in the protection of the types of resources that require the highest security. This is accomplished by defining the required biometric groups 506 and then attaching a multi-user biometric policy to them.

As described above, the multi-user biometric policy has a list of users. Each user in the list of users is represented by the unique user ID 510 that was assigned to that user when he or she enrolled in biometric system 102. The multi-user biometric policy can be implemented as any one of the biometric policies 504 described herein. When biometric server 104 executes the multi-user biometric policy, biometric server 104 first must determine which user IDs 510 are in the list of users. For each user ID 510, biometric server 104 must then determine the biometric policy 504 that particular user must pass in order to be authenticated by biometric system 102. Since the multi-user biometric policy has a list of users, more than one user may have to be authenticated prior to any one user being authenticated by biometric system 102.

An example of how a multi-user biometric policy may be used to protect merger information that no user may gain access to without the president of the enterprise first authorizing it is as follows. The biometric policy 504 attached to the merger information can be defined as an AND multi-user biometric policy with the enterprise president's user ID 510 in the list of users. Here, only users who are also in the list of users may even attempt to gain access to the merger information. No user, even if that user is authenticated by biometric system 102, will gain access to the merger information unless the president also is authenticated by biometric system 102.

All of the above described biometric policies 504 of the present invention provides the flexibility to apply the appropriate level of protection to each network resource without decreasing network productivity. As discussed above, it is the biometric policies 504 that determines the method or way in which a user is to be authenticated by biometric server 104. Although impossible to describe every possible logical variation of biometric policies 504, it should be obvious to one skilled in the art that the logical variations are limitless.

F. Biometric System Security Infrastructure

In general, system security refers to techniques for ensuring that both data stored in a computer and data transported within a system cannot be read or compromised. Inventors of the present invention recognized the importance of securing data within biometric system 102 (FIG. 1). They also recognized the importance of biometric system 102 to integrate easily into existing enterprise security infrastructures.

For example, many network systems today incorporate a firewall. As described above, a firewall is a system designed to prevent unauthorized access and transfer to or from a network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All data entering or leaving the intranet pass through the firewall, which examines each transmission and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. A second line of defense is data encryption. Because many enterprise networks today incorporate one or more firewalls to protect their data, the present invention has been designed in such a way that it integrates easily with existing firewalls.

For greater security, data can be encrypted. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text and encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric key encryption (also called public-key encryption) and symmetric key encryption. As discussed below, the present invention uses encryption to protect data within biometric system 102.

The inventors of the present invention recognized that there are three main areas in network system 202 (FIG. 2) where the security of data must be maintained. These include persistent data stored in biometric server 104 (FIG. 1), data transported across network 114 (FIG. 1) and biometric device software stored in network system 202.

1. Persistent Data Stored in Biometric Server

FIG. 5 illustrates the various collections of persistent data that are stored in biometric server 104 (FIG. 1). Biometric server 104 stores collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. Of these collections of data, biometric templates 502 are especially important to secure. Each biometric template 502 stores a user's unique biometric measurement that is used to match against the user's "live" biometric measurement when the biometric device is attempting to identify the user. Accordingly, the present invention utilizes well-known encryption techniques to protect data stored in biometric server 104.

2. *Data Transported Across the Network System*

All data within biometric system 102 and all data that gets transported to and from biometric system 102, via network 114, must be secure. As mentioned above, biometric templates 502 are especially important to secure because they store user biometric data. As described in reference to the flowchart of FIGs. 8A and 8B above, a preferred process of authenticating a user by biometric system 102 shows biometric template 502 being matched on the client side (i.e., at computer 208 from FIG. 2). In order for biometric template 502 to be matched on the client side, biometric template 502 must be transported over network 114 from biometric server 104 to computer 208. To further ensure the security of biometric templates 502, the present invention transports biometric templates 502 in an encrypted format over network 114 at all times using session keys.

3. *Biometric System Software*

A limitation with all networks is the impossibility for an administrator to know if an unauthorized person is tampering with software loaded on a computer located at a different location from the administrator within the enterprise. Although it is important for a resource protection administrator to be alarmed when biometric system software has been tampered with, it is equally important for the network administrator to be alarmed when other types of software have been tampered with on computers in the network. Therefore, the inventors of the present invention recognized that what is needed is a way of alarming an administrator of a networked system when software has been tampered with on computers in the network.

To protect biometric system software, the present invention incorporates a software integrity object located at each location in network system 202 (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.) that biometric devices are attached to.

The software integrity object of the present invention is always active and its job is to repeatedly check to ensure all biometric system software (i.e., a data file) loaded at the same location as the software integrity object has not been tampered with. This can be done in many ways. One way is for the software integrity object to calculate, for each biometric system software file, a file date, a file size and a byte-wise sum of the file. Also utilized is a mask value and a starting mask value. The software integrity object then executes the following equation (or a similar equation/formula for assuring software integrity):

$$\sum_{i=o}^{\text{Number of Files}} \left[(\text{File Date})_i + (\text{File Size})_i + \left(\sum_{j=o}^{\text{File Size}} (\text{File Byte})_j \right)_i + \text{Item Mask} \right] + \text{Starting Mask}$$

This equation is first executed when the file that is to be protected is first loaded at a location. The first outcome of the equation is stored in a secured environment. The same equation is then repeatedly calculated with the same software. The outcome is then compared to the first outcome stored in the secured environment. If the two do not match, the software integrity object realizes the file containing the software may have been tampered with and sends an alarm to the administrator. The software integrity object is not limited to protecting biometric system software. The software integrity object can be used to protect all software (e.g., files) in network system 202 (FIG. 2).

G. *Biometric Devices and Mobility within a Networked Environment*

The inventors of the present invention recognized a limitation that is encountered when biometric devices are used in a networked environment without biometric system 102 (FIG. 1). As discussed above, for a biometric device to authenticate a user it must have access to the user's biometric template. The present invention provides a scheme for easy access to all user biometric templates 502 such that a user can access network system 202 from any location (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.). The scheme involves storing all biometric templates 502 in a central location. The central location is biometric server 104 (FIG. 1) as described above. Now, via network 114, a user can access his or her biometric template 502 from any location in network system 202. Also, each location in network system 202 knows precisely where to go to locate all biometric templates 502.

Storing all biometric templates 502 in one central location is efficient when network 114 is a LAN. Efficiency problems may arise when network 114 is a WAN. As described above, a WAN connects computers that are farther apart and are connected by data transmission lines or radio waves (e.g., in multiple offices and distant geographies). For example, if an enterprise has multiple offices around the country and all users are accessing one biometric server 104 to gain access to biometric templates 502 for authentication, this is likely to slow down authentication to enterprise resources. To avoid the efficiency problems that will occur if all biometric templates 502 were stored in one biometric server 104, multiple biometric systems 102 can be placed in various locations in network system 202. But here again the problem of a location (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.) in network system 202 not knowing precisely where to go to locate needed biometric templates 502 reoccurs.

The inventors of the present invention solved this problem by two different methods. The first method involves the storing of biometric templates 502 within network system 202 in a hierarchical structure. The second method involves the accessing of a hierarchical directory to locate biometric templates 502 within network system 202.

1. *Hierarchical Storage of Biometric Templates*

FIG. 28 illustrates an enterprise 2800 connected by a WAN incorporating multiple biometric systems 102. Each square in FIG. 28 represents a different office (i.e., location) in enterprise 2800. Each office (i.e., square) has its own LAN and its own biometric system 102. The offices in enterprise 2800 are connected by a WAN.

FIG. 28 shows enterprise 2800 logically organized in a hierarchical structure. Office 2802 is the corporate office and is located at the top of the hierarchical structure. Block 2818 and block 2820 represent logical grouping of offices within enterprise 2800. As shown in FIG. 28, block 2818 includes office 2804, office 2806 and office 2808. Block 2820 includes office 2810, office 2812, office 2814 and office 2816.

The means for determining the logical groupings of offices can involve a number of factors. Several factors can include offices frequently traveled between, grouping offices that do not employ an administrator with offices that do, the adequacy of the WAN connections between various offices, etc.

Because each office has its own biometric system 102, this presents a question of how individual users can avoid having to register at each biometric system 102 and still travel anywhere in enterprise 2800 and be authenticated. One solution is to have a backup copy of all user biometric templates 502 in enterprise 2800 stored in the biometric server at each office. This solution is undesirable for several reasons. As explained in reference to FIG. 1, alternate biometric server 110 is a backup server to biometric server 104 and stores the exact same data. Therefore, it is likely to be expensive to maintain a complete copy of all biometric templates 502 in enterprise 2800 in both biometric server 104 and alternate biometric server 110 at each office. Another reason why this solution is undesirable is the management of various copies of the same biometric template 502 at various locations. When a user refreshes a biometric template 502 (as discussed above) each copy of the old biometric template 502 in enterprise 2800 must be replaced. This increases the possibility that the same biometric template 502 may have different versions in enterprise 2800.

The inventors of the present invention came up with a scheme for hierarchically storing biometric templates within enterprise 2800. In enterprise 2800, all biometric templates 502 are stored at corporate office 2802. Then the additional storage of biometric templates 502 at individual offices depends on the logical block (e.g. either block 2818 or block 2820) the office is in.

The procedure is as follows. First, each office in enterprise 2800 stores the biometric templates 502 for every user enrolled in biometric system 102 at that office. Then, in each logical block, start with the offices at the bottom of the hierarchical structure. For example, in block 2818 start with office 2806 and office 2808. Office 2806 and office 2808 only store the biometric templates 502 for users that were enrolled in biometric systems 102 at those offices. Then, following the hierarchical structure up to office 2804, office 2804 stores the biometric templates 502 for users that were enrolled at office 2804, and also copies of all the biometric templates 502 stored at office 2806 and office 2808. This procedure is repeated until the top of the hierarchical structure is reached (i.e., corporate office 2802).

Thus, with the above hierarchical structure, the farthest any office will have to go to get a user's biometric template is corporate office 2802. For example, say User A was enrolled at office 2812. This means that User A's biometric templates 502 are stored at office 2812, office 2810 and corporate office 2802. If User A travels to office 2806, office 2806 will have to follow the hierarchical structure up to corporate office 2802 to retrieve a copy of User A's biometric templates 502. This scheme allows the biometric templates 502 within enterprise 2800 to be stored at the minimum number of locations, while still providing each user the flexibility to be authenticated by biometric system 102 from any office within the enterprise.

Not only does the hierarchical structure of enterprise 2800 provide ease of access, but also a means of backing up biometric templates 502 within enterprise 2800.

2. *Hierarchical Directory for Locating Biometric Templates*

The second method involves the accessing of a hierarchical directory to locate biometric templates 502 within enterprise 2800 (FIG. 28). As described above, one example of a hierarchical directory is a X.500 directory. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. Therefore, the same scheme as discussed above for storing biometric templates 502 can be used for storing a X. 500 directory. The X.500 directory will include pointers to the offices that user biometric templates 502 are stored.

H. Other Applications

A computer, as described in reference to FIG. 3, is more than the typical desktop computer. For example, both cars and ATM machines incorporate computers, home and office physical security systems incorporate computers, etc. Thus, the present invention is not limited to the protection of resources in a networked environment as described above. Following are just some of the various applications where the present invention can be applied.

1. Digital Certificates

The inventors of the present invention recognized a limitation that is encountered when digital certificates are used in a networked environment without biometric system 102 (FIG. 1). Generally, a digital certificate defines user privileges. More specifically, a digital certificate attaches to an electronic message and is used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public keys, private keys and a variety of other identification information. The applicant's public key is signed by the CA. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. Today, a user must pass a password device, or use a token or smart card, or any combination thereof, to gain access to a digital certificate. Because each user's digital certificate is stored on one computer within the network, the digital certificate is bound to a single computer. This limits the user from going to a different computer to gain access to the network.

The inventors of the present invention recognized that a way of adequately authenticating a user prior to gaining access to his or her digital certificate is needed that avoids the weakest link in authentication caused by the human factor, as discussed above. In addition, the inventors of the present invention recognized that a scheme is needed for easy access to all user digital certificates such that a user can gain access to required resources from any location within the enterprise. Thus, the present invention requires a user to be authenticated by biometric devices to gain access to digital certificates avoids the weakest link in authentication caused by the human factor.

The scheme for easy access to all user digital certificates, such that a user can gain access to his or her digital certificate from any location within the enterprise, is the same scheme as described above in reference to FIG. 28 and the storing of biometric templates 502. In enterprise 2800, all digital certificates are stored at corporate office 2802. Then the additional storage of digital certificates at individual offices depends on the logical block (e.g. either block 2818 or block 2820) the office is in.

The procedure is as follows. First, each office in enterprise 2800 stores the digital certificates for every user that was issued a digital certificate at that office. Then, in each logical block, start with the offices at the bottom of the hierarchical structure. For example, in block 2818 start with office 2806 and office 2808. Office 2806 and office 2808 only store the digital certificates for users that were issued digital certificates at those offices. Then, following the hierarchical structure up to office 2804, office 2804 stores the digital certificates for users that were issued digital certificates at office 2804, and also copies of all the digital certificates stored at office 2806 and office 2808. This procedure is repeated until the top of the hierarchical structure is reached (i.e., corporate office 2802).

Thus, with the above hierarchical structure, the farthest any office will have to go to get a user's digital certificate is corporate office 2802. For example, say User A was issued a certificate at office 2812. This means that User A's digital certificate is stored at office 2812, office 2810 and corporate office 2802. If User A travels to office 2806, office 2806 will have to follow the hierarchical structure up to corporate office 2802 to retrieve a copy of User A's digital certificate. Once it is determined that the user is finished with his or her digital certificate, the digital certificate must be re-retrieved the next time the user requests access to his or her digital certificate

Not only does the hierarchical structure of enterprise 2800 provide ease of access, but also a means of backing up digital certificates within enterprise 2800.

The use of a hierarchical directory to locate biometric templates 502 within enterprise 2800 (FIG. 28) as described above works equally as well for digital certificates. The X.500 directory will include pointers to the offices that user digital certificates are stored.

2. *Roaming Profile Server*

The concept of using a public key to decode a digital certificate attached to a message was introduced above. Some cryptographic systems use two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. For example, when User A wants to send a secure message to User B, User A uses User B's public key to encrypt the message. User B then uses his or her private key to decrypt the message.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. But it is imperative to ensure that users' private keys are kept secret. A user's private keys, among other things, are contained in a unique encrypted user profile. Therefore, a user needs to be adequately authenticated prior to allowing the user access to the user's private keys (i.e., decrypt the user's profile).

There exist public key systems that provide a public key infrastructure. One example of such public key systems is Entrust/PKI™. A public key infrastructure is a comprehensive system that provides public key encryption and digital signature services. The purpose of a public key infrastructure is to manage public keys and digital certificates. By managing keys and digital certificates through a public key infrastructure, an enterprise establishes and maintains a trustworthy networking environment. A public key infrastructure enables the use of encryption and digital signature services across a wide variety of applications.

Public key systems must also manage user profiles. Each profile contains a user's private keys. As mentioned above, the authentication of users prior to allowing them access to their profiles is imperative. Public key systems allow for the authentication of users in one of two ways. The first way is through a password device supplied by the public key system itself. As discussed above, a password device is an inadequate identification mechanism because it can not avoid the weakest link in authentication caused by the human factor.

The second way that public key systems allow for the authentication of users is through an identification device interface. The identification device interface allows third-party vendors of identification devices to create an identity device module that interfaces with it. This way third-party vendors provide the authentication of users prior to allowing them access to their profiles within the public key system.

Various third-party vendors of both biometric and non-biometric devices have created identity device modules for their devices to facilitate user authentication within public key systems. The non-biometric devices (e.g, password, smart cards and tokens) are inadequate identification mechanisms because they can not avoid the weakest link in authentication caused by the human factor.. Alternatively, biometric devices do conclusively authenticate a user by avoiding the weakest link in authentication caused by the human factor. Although a single biometric device can conclusively authenticate a user, the inventors of the present invention recognized that biometric system 102 (FIG. 1) can be used to provide flexibility and additional security in the authentication of users prior to allowing them access to profiles within the public key system. This flexibility and additional security provided by biometric system 102 is the ability to use multiple biometric devices for the authentication of individual users. In addition, the inventors of the present invention recognized that a scheme is needed for easy access to all profiles such that a user can gain access to the user's profile from any location within the enterprise.

FIG. 29 is a block diagram illustrating how biometric system 102 of the present invention can be integrated with a public key system. FIG. 29 includes public key system engine 2902, identification device interface 2904, public key system manager and directory 2906, biometric identity device module 2908, biometric server 104 (FIG. 1) and profile server 2910. Public key system engine 2902, identification device interface 2904 and public key system manager and directory 2906 are not part of the present invention. They are part of a generic public key system. Biometric identity device module 2908, biometric server 104 (FIG. 1) and profile server 2910 are part of the present invention.

Public key system engine 2902 performs the various functions of the public key system. Public key system engine 2902 interacts with the various applications (e.g., e-mail, browsers, etc.) that it provides the use of encryption and digital signatures for. Identification device interface 2904 allows third-party vendors of identification devices to create an identity device module that interfaces with it. Biometric identity device module 2908 is one of these identity device modules that interfaces with identification device interface 2904. Biometric identity device module 2908 acts similar to the open interface of the present invention as described above.

Public key system manager and directory 2906 stores and manages public keys. Biometric server 104 operates exactly as described above. Finally, profile server 2910 stores all of the users' profiles in the public key system. Profile server 2910 is attached to biometric server 104 and acts as a roaming profile server for the public key system.

Biometric identity device module 2908 works with identification device interface 2904 to provide the desired profile from profile server 2910. But prior to providing the desired profile, biometric identity device module 2908 and biometric server 104 work together to authenticate the user. All data transported between biometric identity device module 2908 and biometric server 104 is encrypted. This data includes the profiles and biometric templates 502 (FIG. 5).

Incorporating biometric system 102 (FIG. 1) into a public key system helps to avoid the limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for the environment in which the user is trying to get access to his or her profile, increase user mobility within the enterprise, remotely enroll and re-enroll users into biometric system 102 and to ensure the integrity of software loaded on remote computers.

3. Phone Authentication and Clearance Verification

Phones can be implemented as a voice recognition device. Thus, biometric system 102 (FIG. 1) can be used to authenticate employees for access to various phones within the enterprise. Biometric system 102 can also be used to apply clearance verification for each employee to make certain calls. For phone authentication and clearance verification, biometric groups 506 (FIG. 5) can be defined in such a way that employees in certain biometric groups 506 are only allowed to make certain types of phone calls (e.g., local calls, long-distance calls, 800 calls, 900 calls, etc.) and/or have access to certain phones within the enterprise.

Incorporating biometric system 102 (FIG. 1) into phone authentication and clearance verification helps to avoid some of the limitations discussed above. Biometric system 102 provides the flexibility to use a phone as a voice recognition device, increase employee mobility within the enterprise, apply the needed degree of authentication required to protect each type of phone call and remotely enroll and re-enroll customers into biometric system 102.

4. Access/Facility Control

Current physical access/facility control systems require the user to enter a password to activate and/or deactivate the system. As described above, biometric devices for identification mechanisms eliminate the weakest link caused by the human factor. Biometric devices can be attached to the entry of each physical location in an enterprise that authentication is required for entry. Then, biometric system 102 (FIG. 1) can be used to provide flexibility in protection and efficient administration as described above.

Biometric groups 506 (FIG. 5) can be defined in such a way that users in certain biometric groups 506 are only allowed access to certain physical locations within an enterprise. One problem that any enterprise has with physical access to locations is that one authenticated person may allow one or more unauthenticated people in the location. Here, a facial image device may be utilized to continuously scan a location to determine if any unauthenticated people are present. If the facial image device determines that an unauthenticated person is present, biometric system 102 can alarm the administrator.

Incorporating biometric system 102 (FIG. 1) into a physical access/facility control system helps to avoid limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for the environment in which the entry is located, increase user mobility within the enterprise, apply the needed degree of authentication required to protect each type of physical location, remotely enroll and re-enroll users into biometric system 102 and to ensure the integrity of software loaded at remote entries.

5. *Banking and Financial*

Today, more than ever, adequate authentication mechanisms are needed in the banking and financial industries. Transactions that once required interaction between two people, now are encouraged to be done via ATM machines or automated phone systems. Currently, transactions are approved by a customer entering a correct pin. As the types of human-to-machine transactions increase, so does the number of different pins each user is required to remember. The result is that either customers write their pins down and/or they use the same pin for many different types of transactions. If a pin is written down, this increases the chance that another person will see the pin and use it to gain unauthorized access to transactions.

Incorporating biometric system 102 (FIG. 1) into current banking and financial transaction systems (e.g., ATM machines), avoids all of the limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for an environment in which the ATM machine is located, increase customer mobility, apply the needed degree of authentication required to protect each transaction, remotely enroll and re-enroll customers into biometric system 102 and to ensure the integrity of software loaded on remote ATM machines.

6. Silent Signal

Silent signal is a way of silently signaling for assistance through the use of biometric devices. Silent signal is particularly applicable to access/facility control and the banking and financial industries. This feature of the present invention allows a user to enter a normal (i.e., expected) biometric measurement under normal conditions or an alarm biometric measurement under emergency conditions. One example of silent signal incorporates a fingerprint device. Say a fingerprint device is used for authentication at an ATM machine. Biometric policies 504 (FIG. 5) of biometric system 102 (FIG. 1) can be configured to silently signal police if, for example, the left index finger is used for authentication to the ATM machine during a robbery. Otherwise, the right index finger is used for a normal transaction without the need to signal the police. A similar scenario applies to access/facility control.

Another example of silent signal incorporates a voice recognition device. Here, when a certain phrase is used for authentication to either a physical location or at an ATM machine, the police are silently signaled. In addition, it should be apparent to one skilled in the art that any of the biometric devices mentioned above can be used to implement the silent signal of the present invention.

I. Conclusion

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention. This is especially true in light of technology and terms within the relevant art(s) that may be later developed. Thus, the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What Is Claimed Is:

1. A method for providing user authentication to enterprise resources, comprising the steps of:

(a) setting up a biometric server, said biometric server having stored therein at least one biometric policy that determines whether the user can gain access to the enterprise resources, wherein said biometric policy has associated therewith at least one biometric device;

(b) determining whether the user is authenticated by executing said biometric policy; and

(c) allowing the user access to the enterprise resources if the user passes said biometric policy, otherwise denying access to the user to the enterprise resources.

2. The method claim 1, further comprising the step of enrolling the user for authentication by having the user create a biometric template for each said biometric device, wherein said biometric template includes biometric data unique to the user.

3. The method of claim 1, further comprising forming said biometric policy by selecting one or more said biometric devices that the user must be tested on in order to gain access to the enterprise resources.

4. The method of claim 1, further comprising placing the user within a biometric group, wherein said biometric group defines a set of users with a common characteristic or access privileges.

5. The method of claim 1, wherein step (1) comprises the steps of:

(a) determining initial collections of data stored in said biometric server; and

(b) customizing said collections of data stored in said biometric server.

6. The method of claim 5, wherein step (a) comprises the steps of:

(I) assigning a unique computer ID to each computer in the enterprise;

(ii) assigning a unique biometric device ID to each said biometric device in the enterprise;

(iii) determining which of said biometric devices will be attached to which of said computers by assigning said biometric device IDs to each of said computer IDs;

(iv) forming biometric groups;

(v) creating biometric policies;

(vi) assigning one of said biometric policies to each of said biometric groups;

(vii) assigning a unique user ID to each user who needs to be authenticated;

(viii) putting each of said user IDs into one of said biometric groups; and

(ix) storing said biometric policies, said biometric groups, said biometric device IDs, said user IDs and said computer IDs in said biometric server.

7. The method of claim 2, wherein the step of enrolling the user comprises the steps of:

(a) determining said biometric devices the user must be enrolled in by looking at a list of devices associated with said biometric policy assigned to the user's said biometric group;

(b) creating a biometric template for each of said biometric devices in said list of devices; and

(c) storing each of said created biometric templates in said biometric server.

8. The method of claim 6, wherein step (2) comprises the steps of:

(a) receiving a login request at said biometric server, wherein said login request includes one of said computer IDs and one of said user IDs;

(b) determining which said biometric group said user ID is in;

(c) determining which said biometric policy is assigned to said biometric group;

(d) determining whether said biometric policy can be executed;

(e) returning that the user is not authenticated if the outcome of step (d) is negative;

(f) executing said biometric policy to determine if the user is authenticated; and

(g) returning that the user is authenticated if the outcome of step (f) is positive.

9. The method of claim 8, wherein step (d) comprises the steps of:

I. determining whether said required biometric templates are stored in said biometric server;

ii. determining whether said required biometric device IDs are assigned to said computer ID; and

iii. returning that said biometric policy can be executed if the outcome to both step I and step ii are positive.

10. The method of claim 1, wherein step (1) is performed with an administration station.

11. The method of claim 2, wherein the step of enrolling the user is performed with an enrollment station.

12. The method of claim 8, wherein step (f) comprises the step of testing the user on said biometric devices listed in said list of devices until either the user passes said biometric policy or the user fails said biometric policy.

13. The method of claim 1, wherein said biometric policy is an OR policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said OR policy if the user passes one of said biometric devices in said list of devices.

14. The method of claim 1, wherein said biometric policy is an OR policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said OR policy if the user passes said biometric device while being tested with at least two biometric measurements.

15. The method of claim 1, wherein said biometric policy is an AND policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said AND policy if the user passes all of said biometric devices in said list of devices.

16. The method of claim 1, wherein said biometric policy is an AND policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said AND policy if the user passes said biometric device while being tested with at least two biometric measurements.

17. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with a first biometric device or if the user exceeds a contingent threshold

associated with said first biometric device and the user exceeds a minimum threshold associated with a second biometric device.

18. The method of claim 17, wherein said minimum thresholds and said contingent threshold is set by an administrator.

19. The method of claim 17, wherein said second biometric device is selected based on environmental conditions.

20. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of devices, wherein said list of devices includes only one biometric device, wherein a first biometric measurement and a second biometric measurement are associated with said biometric device, and wherein the user passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with said biometric device and said first biometric measurement or if the user exceeds a contingent threshold associated with said biometric device and said first biometric measurement and the user exceeds a minimum threshold associated with said biometric device and said second biometric measurement.

21. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of devices, wherein said list of devices includes at least two different biometric devices, wherein a random biometric device is determined from said list of devices, and wherein the user passes said RANDOM policy if the user passes said random biometric device.

22. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of devices, wherein said list of devices includes only one biometric device, wherein a random biometric measurement is determined from one or more biometric measurements, and wherein the user

passes said RANDOM policy if the user passes said biometric device while being tested with said random biometric measurement.

23. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested on one or more of said biometric devices in said list of devices.

24. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested with one or more biometric measurements on said biometric device in said list of devices.

25. The method of claim 1, wherein said biometric policy is an OR policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said OR policy if the user passes one of said biometric policies in said list of biometric policies.

26. The method of claim 1, wherein said biometric policy is an AND policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said AND policy if the user passes all of said biometric policies in said list of biometric policies.

27. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user

passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with a first biometric policy or if the user exceeds a contingent threshold associated with said first biometric policy and the user exceeds a minimum threshold associated with a second biometric policy.

28. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, wherein a random biometric policy is determined from said list of biometric policies, and wherein the user passes said RANDOM policy if the user passes said random biometric policy.

29. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested on one or more of said biometric policies in said list of biometric policies.

30. The method of claim 1, wherein said biometric policy is an OR policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said OR policy if the user passes one of said elements in said list of policies or devices.

31. The method of claim 1, wherein said biometric policy is an AND policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said AND policy if the user passes all of said elements in said list of policies or devices.

32. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said

CONTINGENT policy if either the user exceeds a minimum threshold associated with a first element or if the user exceeds a contingent threshold associated with said first element and the user exceeds a minimum threshold associated with a second element.

33. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, wherein a random element is determined from said elements in said list of policies or devices, and wherein the user passes said RANDOM policy if the user passes said random element.

34. The method of claim 1, further comprising having a timeout value associated with said biometric device.

35. A method of storing biometric templates in a hierarchical structure throughout an enterprise, the enterprise having multiple locations, comprising the steps of:

determining a corporate location;

storing all of the biometric templates associated with a group of users at said corporate location;

dividing all of the remaining locations into multiple logical groupings, wherein each logical grouping is associated with a subset of said group of users;

selecting a top level location in each of said logical groupings;

storing at said top level location for each logical grouping all of the biometric templates associated with said subset of users; and

storing at a bottom level location for each of said logical groupings all of said biometric templates associated with a further subset of said subset of users.

36. A method of storing digital certificates in a hierarchical structure throughout an enterprise, the enterprise having multiple locations, comprising the steps of:

determining a corporate location;

storing all of the digital certificates associated with a group of users at said corporate location;

dividing all of the remaining locations into multiple logical groupings, wherein each logical grouping is associated with a subset of said group of users;

selecting a top level location in each of said logical groupings;

storing at said top level location for each logical grouping all of the digital certificates associated with said subset of users; and

storing at a bottom level location for each of said logical groupings all of said digital certificates associated with a further subset of said subset of users.

37. A system for controlling access to enterprise resources, comprising:

a biometric server having stored therein biometric data related to a plurality of users and at least one biometric policy that determines whether said users can gain access to the enterprise resources;

at least one computer connected to said biometric server;

a plurality of biometric devices, wherein said biometric policy has associated therewith at least one of said plurality of biometric devices; and

wherein said biometric server includes means for determining whether said user can access said enterprise resources, wherein said user gains access to the enterprise resources by passing said biometric policy.

38. The system of claim 37, further comprising means for enrolling each of said users, wherein said means for enrolling includes creating a biometric

template for each of said plurality of biometric devices, wherein said biometric template includes biometric data unique to a particular user.

39. The system of claim 37, further comprising means for creating biometric policies and biometric groups, wherein each said biometric groups includes one or more users.

40. The system of claim 39, wherein said biometric group defines one or more users that are allowed access to the same subset of enterprise resources.

41. The system of claim 37, further includes a communication means for connecting said biometric server to one or more remote computers.

42. The system of claim 37, further comprising a secondary server that duplicates all data within said biometric server.

43. The system of claim 37, wherein said biometric server further stores biometric device ID's, User ID's, Computer ID's and Application ID's.

44. The system of claim 37, wherein said means for determining is implemented as an object.

45. The system of claim 37, further comprises a graphical user interface that allows an administrator to create biometric groups and define biometric policies.

46. The system of claim 37, further comprising a roaming profile server having one or more user profiles, wherein said biometric server is utilized to access each of said user profiles.

47. The system of claim 37, wherein said computer is a phone.

48. The system of claim 37, wherein said computer is an ATM machine.

49. The system of claim 37, wherein said computer is attached to a physical location.

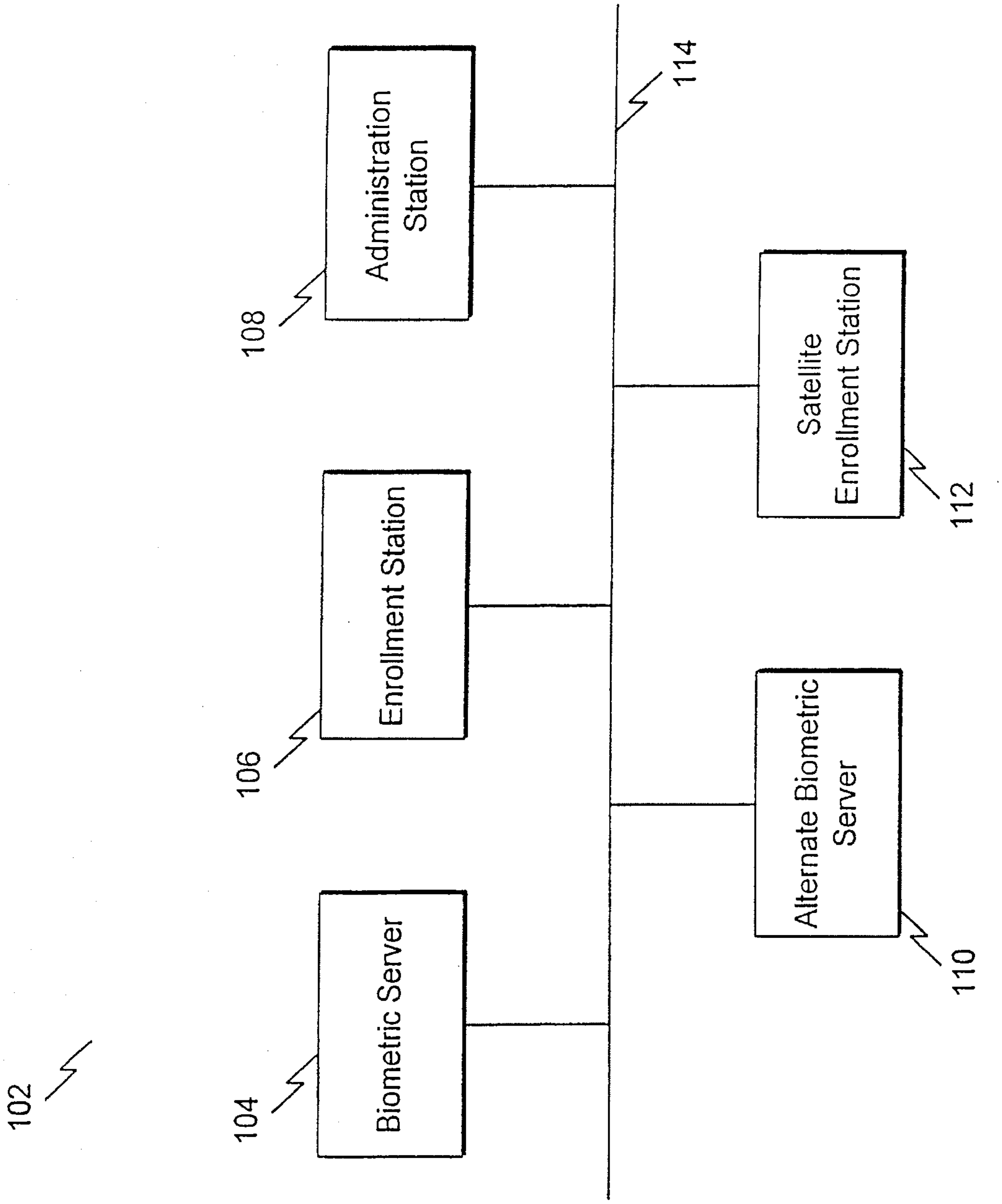

102
104
Biometric Server
106
Enrollment Station
108
Administration Station
114
110
Alternate Biometric Server
112
Satellite Enrollment Station

FIG.1

2/48

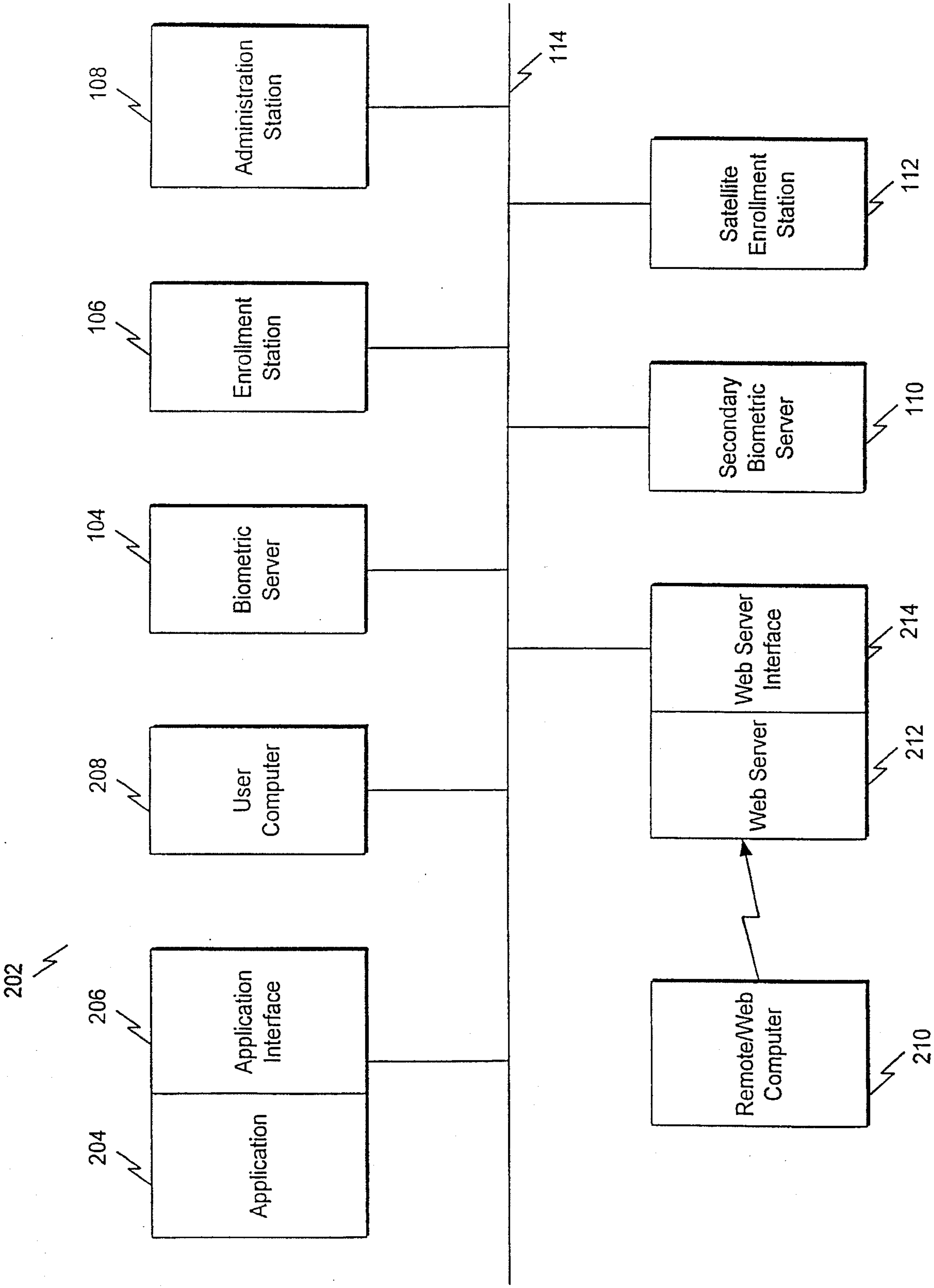

108
Administration Station
114
106
Enrollment Station
104
Biometric Server
208
User Computer
202
206
Application Interface
204
Application
112
Satellite Enrollment Station
110
Secondary Biometric Server
214
Web Server Interface
212
Web Server
210
Remote/Web Computer

FIG.2

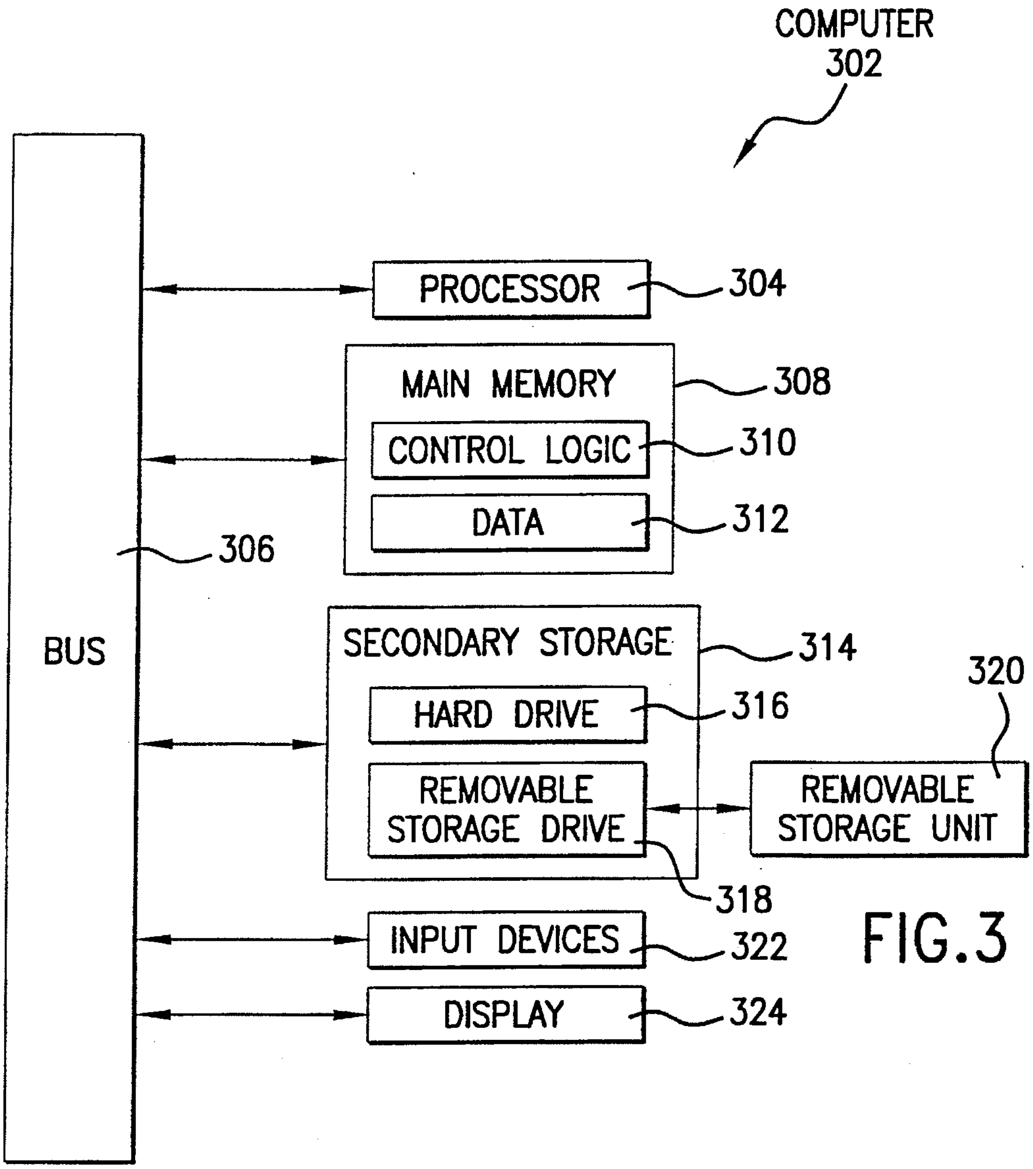

COMPUTER
302
PROCESSOR
304
MAIN MEMORY
308
CONTROL LOGIC
310
DATA
312
306
BUS
SECONDARY STORAGE
314
HARD DRIVE
316
320
REMOVABLE STORAGE DRIVE
REMOVABLE STORAGE UNIT
318
INPUT DEVICES
322
DISPLAY
324

FIG.3

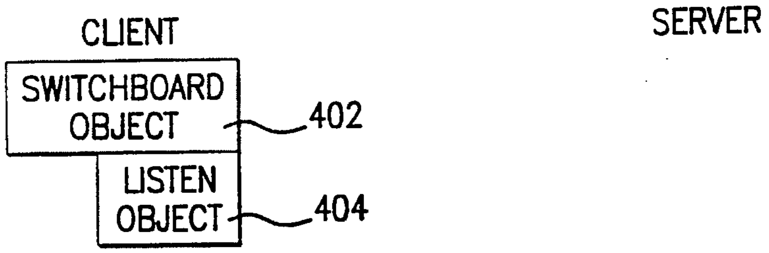


FIG. 4A

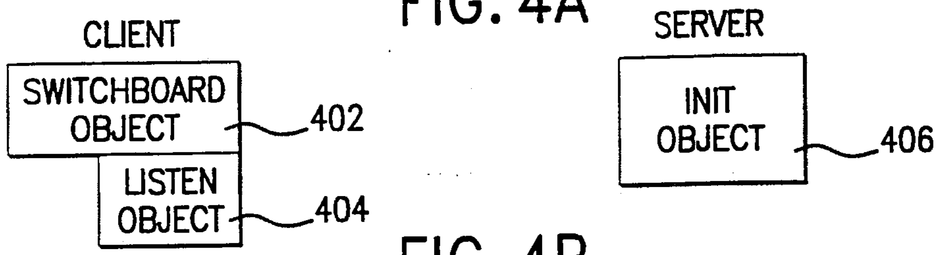


FIG. 4B

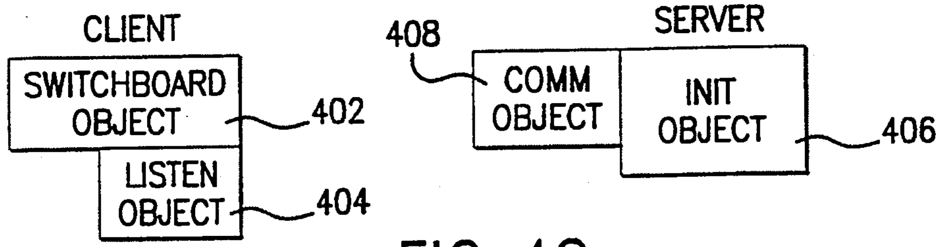


FIG. 4C

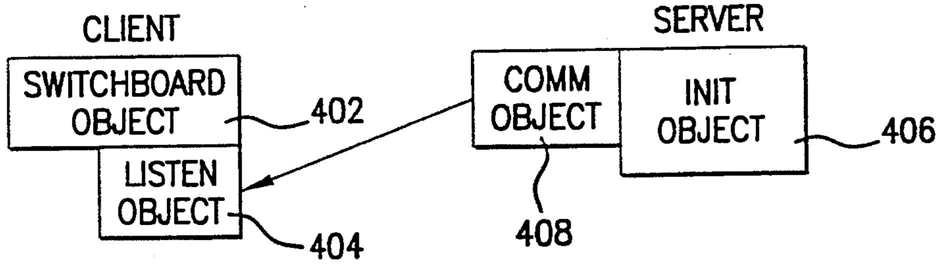


FIG. 4D

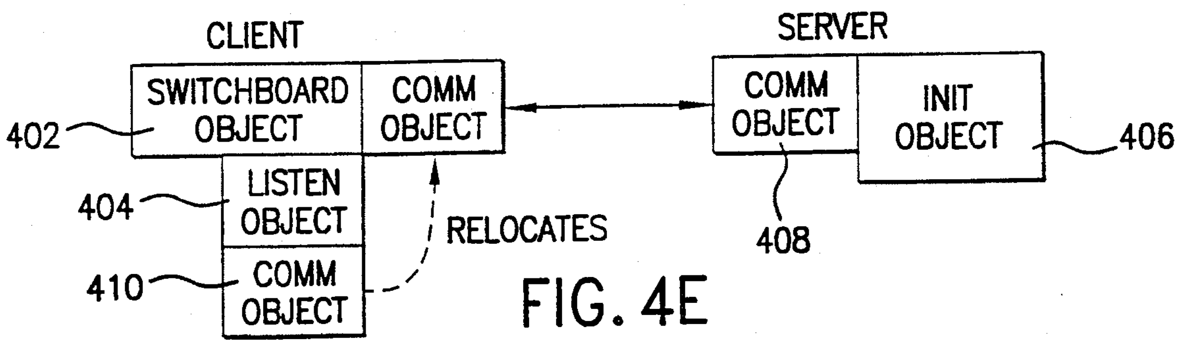


FIG. 4E

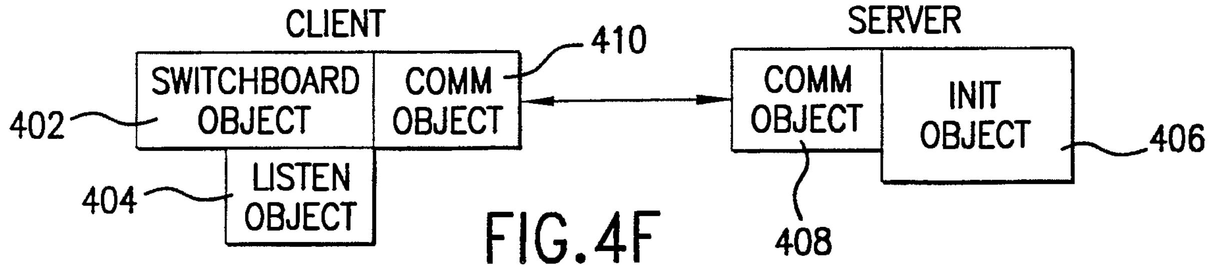


FIG.4F

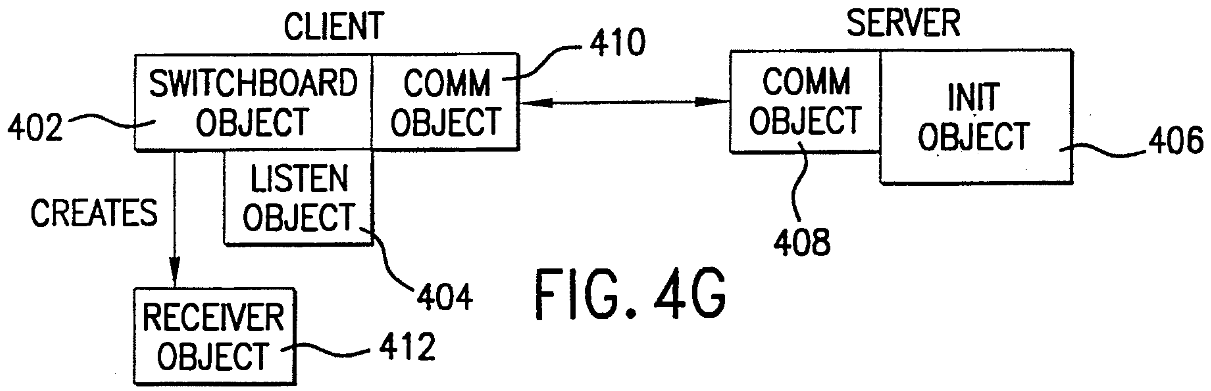


FIG. 4G

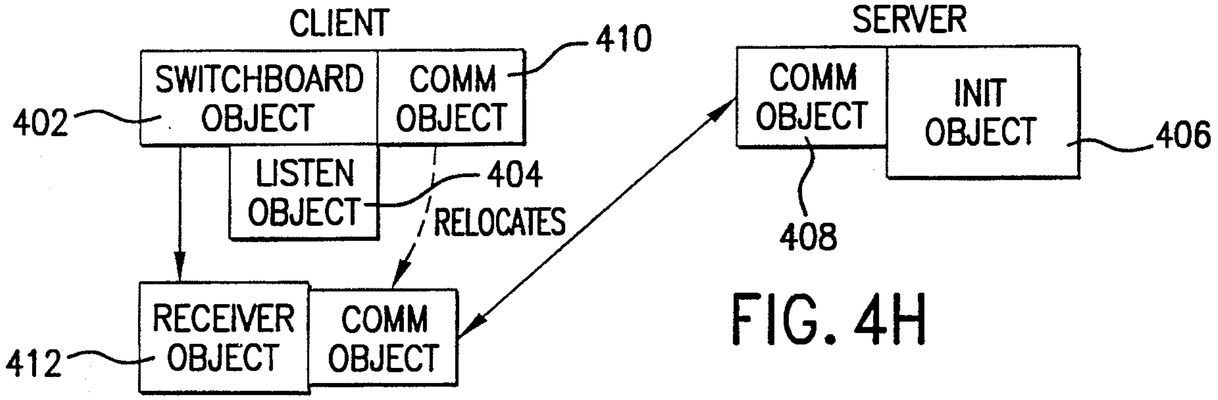


FIG. 4H

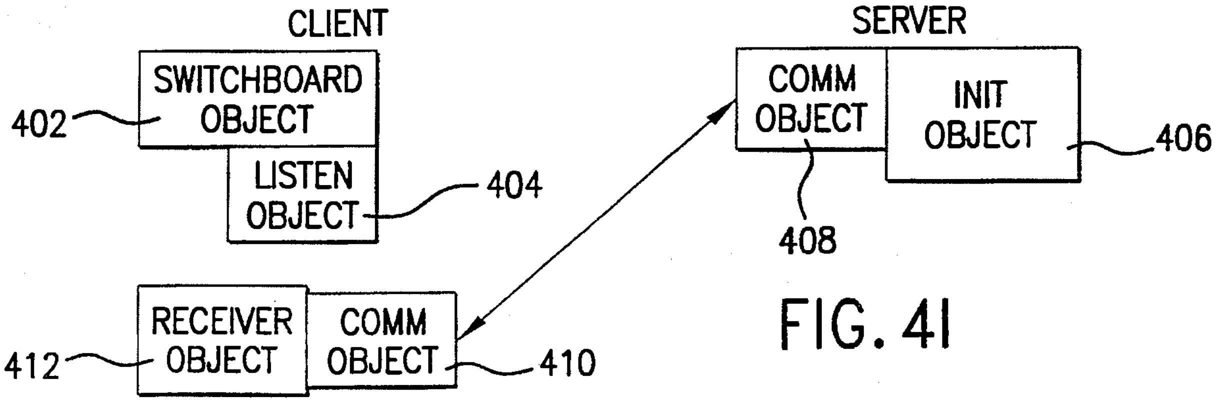


FIG. 4I

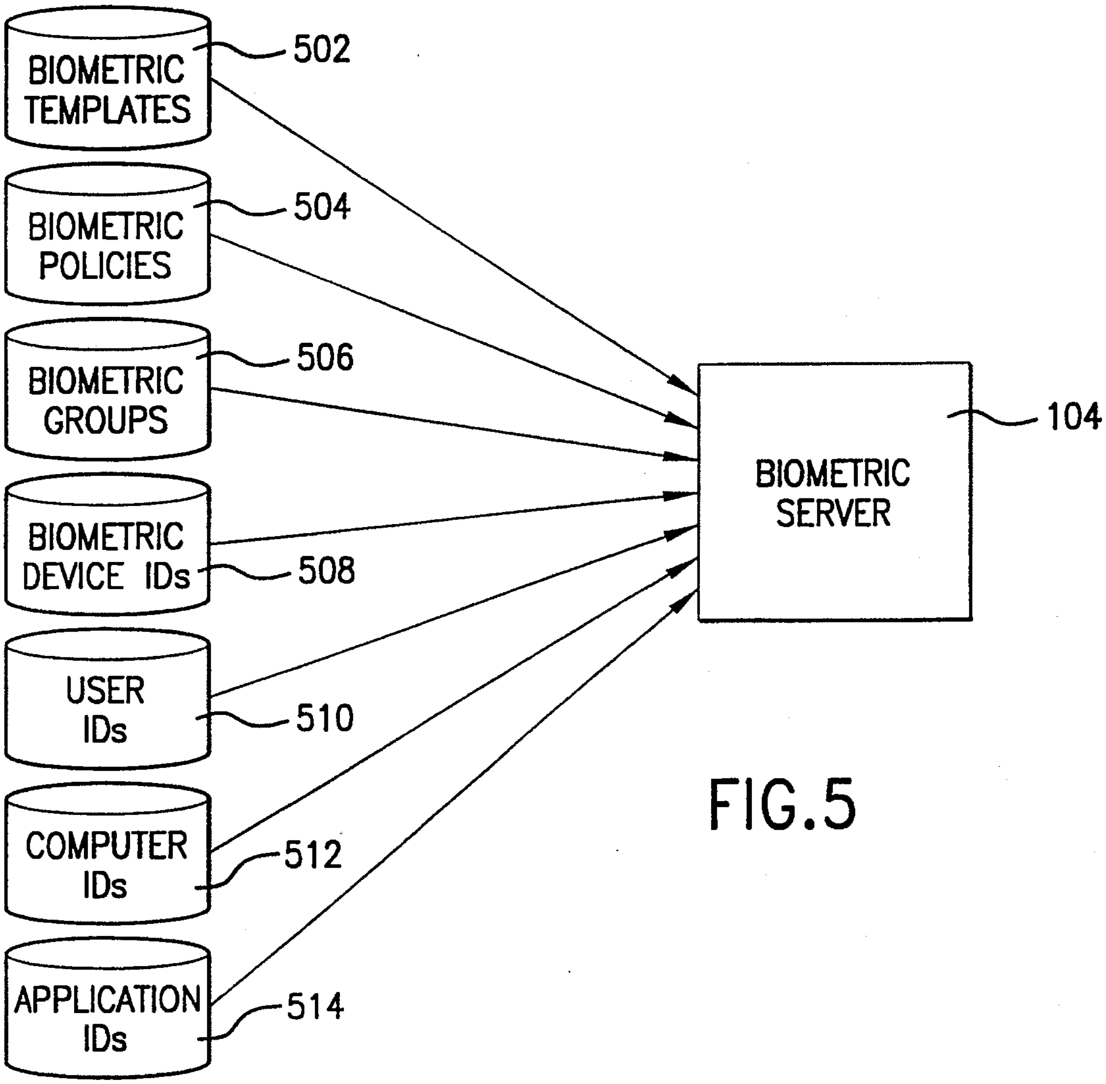

BIOMETRIC TEMPLATES
502
BIOMETRIC POLICIES
504
BIOMETRIC GROUPS
506
BIOMETRIC DEVICE IDs
508
USER IDs
510
COMPUTER IDs
512
APPLICATION IDs
514
BIOMETRIC SERVER
104

FIG.5

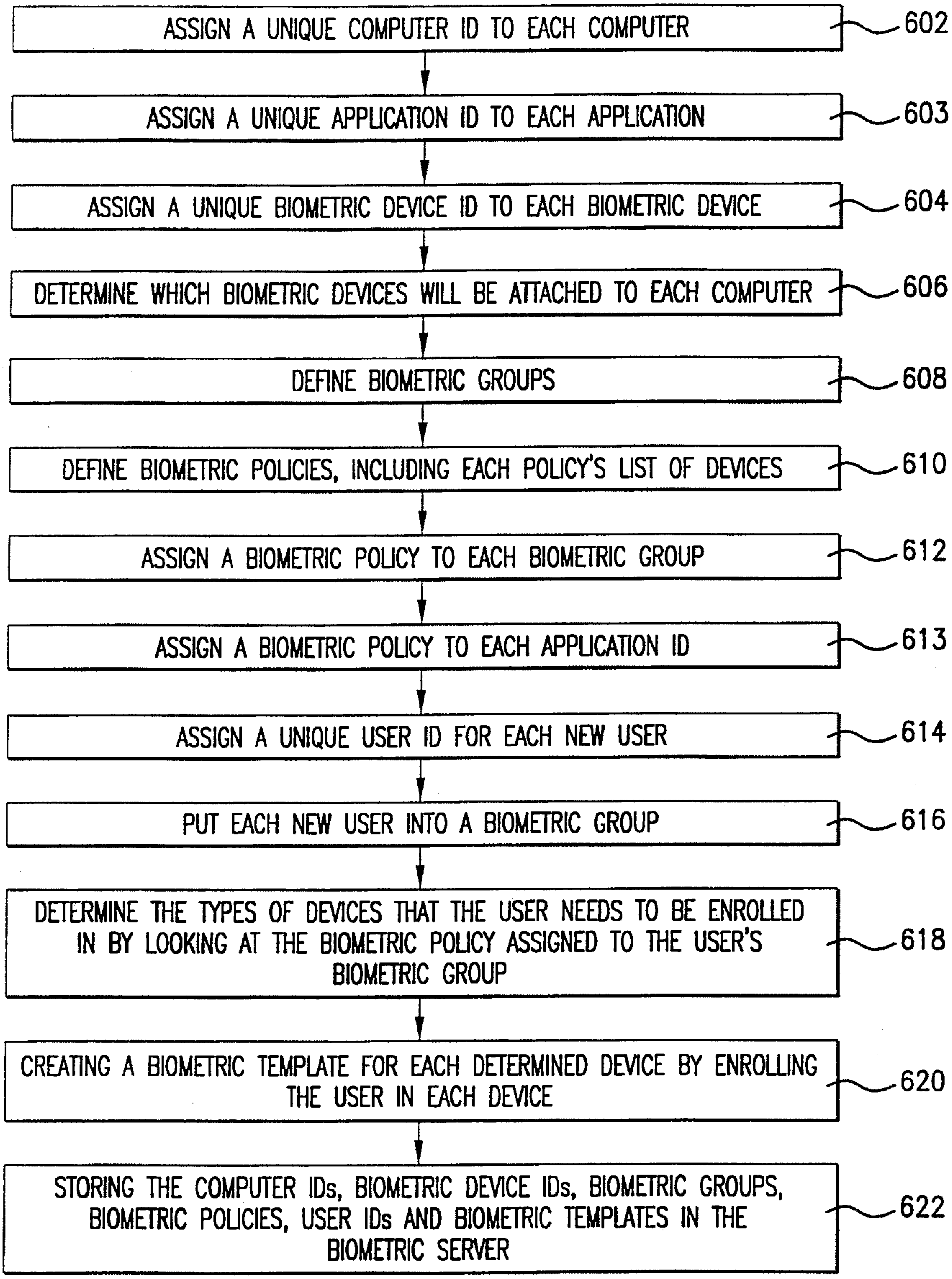

ASSIGN A UNIQUE COMPUTER ID TO EACH COMPUTER
602
ASSIGN A UNIQUE APPLICATION ID TO EACH APPLICATION
603
ASSIGN A UNIQUE BIOMETRIC DEVICE ID TO EACH BIOMETRIC DEVICE
604
DETERMINE WHICH BIOMETRIC DEVICES WILL BE ATTACHED TO EACH COMPUTER
606
DEFINE BIOMETRIC GROUPS
608
DEFINE BIOMETRIC POLICIES, INCLUDING EACH POLICY'S LIST OF DEVICES
610
ASSIGN A BIOMETRIC POLICY TO EACH BIOMETRIC GROUP
612
ASSIGN A BIOMETRIC POLICY TO EACH APPLICATION ID
613
ASSIGN A UNIQUE USER ID FOR EACH NEW USER
614
PUT EACH NEW USER INTO A BIOMETRIC GROUP
616
DETERMINE THE TYPES OF DEVICES THAT THE USER NEEDS TO BE ENROLLED IN BY LOOKING AT THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP
618
CREATING A BIOMETRIC TEMPLATE FOR EACH DETERMINED DEVICE BY ENROLLING THE USER IN EACH DEVICE
620
STORING THE COMPUTER IDs, BIOMETRIC DEVICE IDs, BIOMETRIC GROUPS, BIOMETRIC POLICIES, USER IDs AND BIOMETRIC TEMPLATES IN THE BIOMETRIC SERVER
622

FIG.6

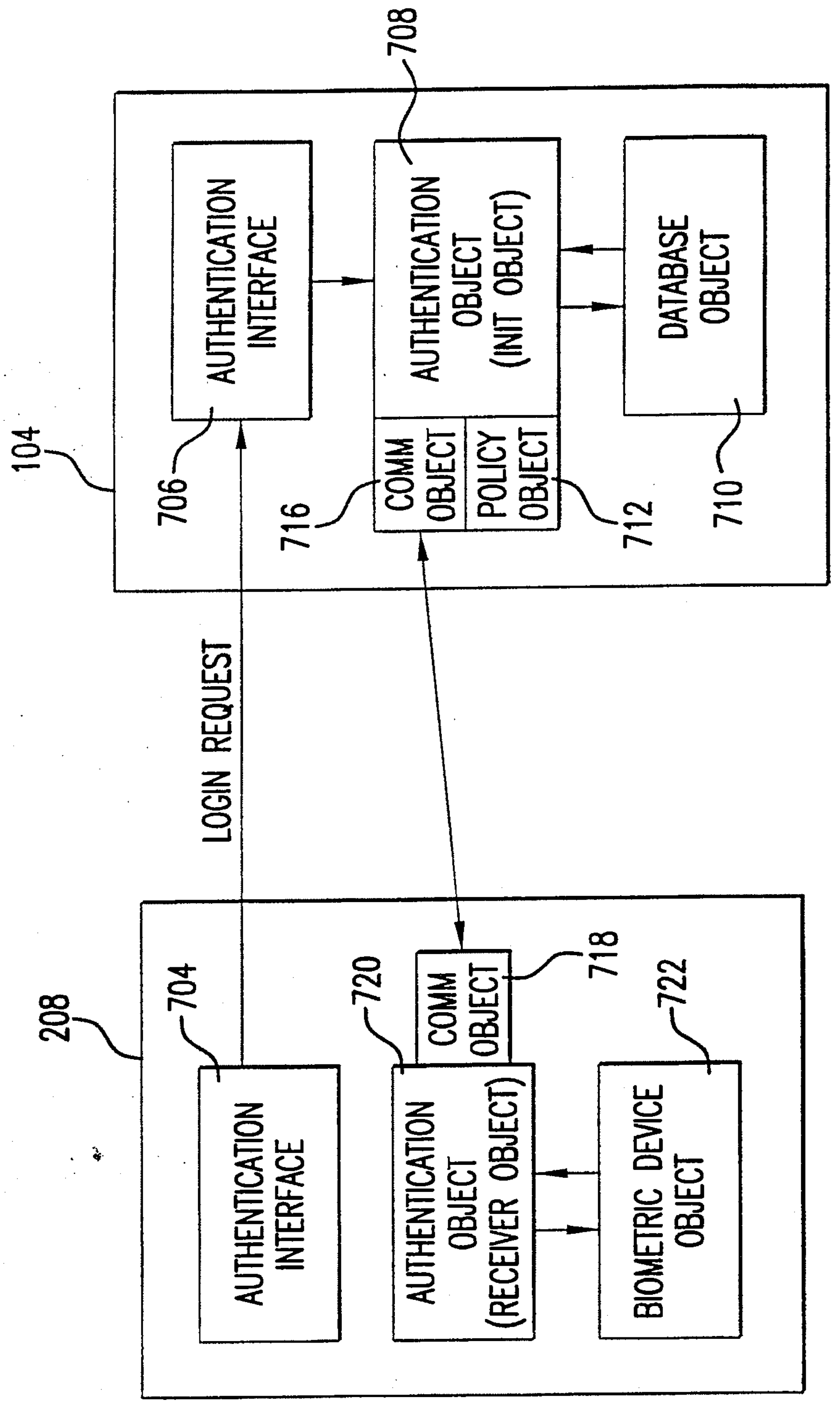

104
AUTHENTICATION INTERFACE
706
AUTHENTICATION OBJECT (INIT OBJECT)
708
COMM OBJECT
716
POLICY OBJECT
712
DATABASE OBJECT
710
LOGIN REQUEST
208
AUTHENTICATION INTERFACE
704
AUTHENTICATION OBJECT (RECEIVER OBJECT)
720
COMM OBJECT
718
BIOMETRIC DEVICE OBJECT
722

FIG.7

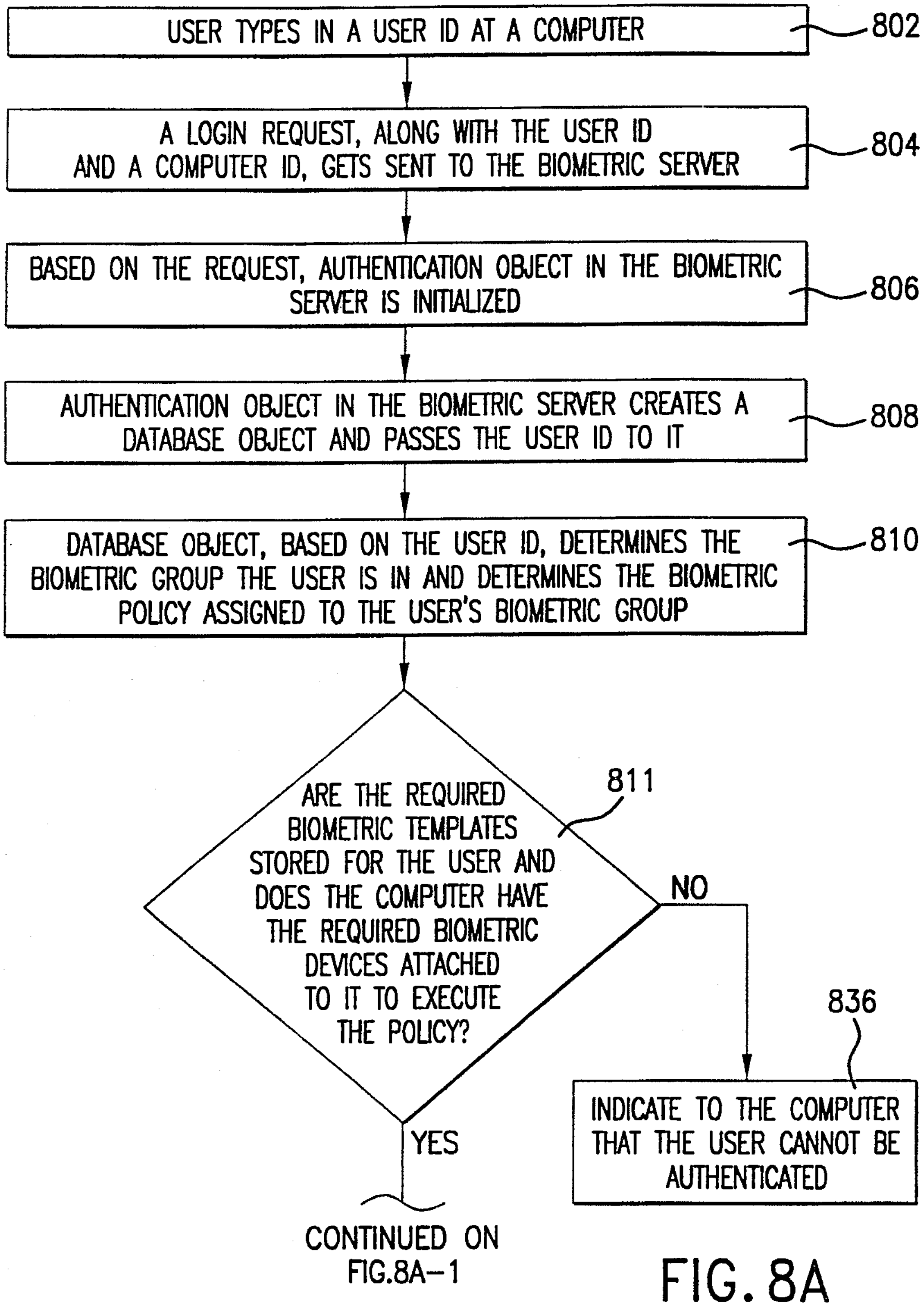

USER TYPES IN A USER ID AT A COMPUTER
802
A LOGIN REQUEST, ALONG WITH THE USER ID AND A COMPUTER ID, GETS SENT TO THE BIOMETRIC SERVER
804
BASED ON THE REQUEST, AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER IS INITIALIZED
806
AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER CREATES A DATABASE OBJECT AND PASSES THE USER ID TO IT
808
DATABASE OBJECT, BASED ON THE USER ID, DETERMINES THE BIOMETRIC GROUP THE USER IS IN AND DETERMINES THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP
810
ARE THE REQUIRED BIOMETRIC TEMPLATES STORED FOR THE USER AND DOES THE COMPUTER HAVE THE REQUIRED BIOMETRIC DEVICES ATTACHED TO IT TO EXECUTE THE POLICY?
811
NO
836
INDICATE TO THE COMPUTER THAT THE USER CANNOT BE AUTHENTICATED
YES
CONTINUED ON FIG.8A-1

FIG. 8A

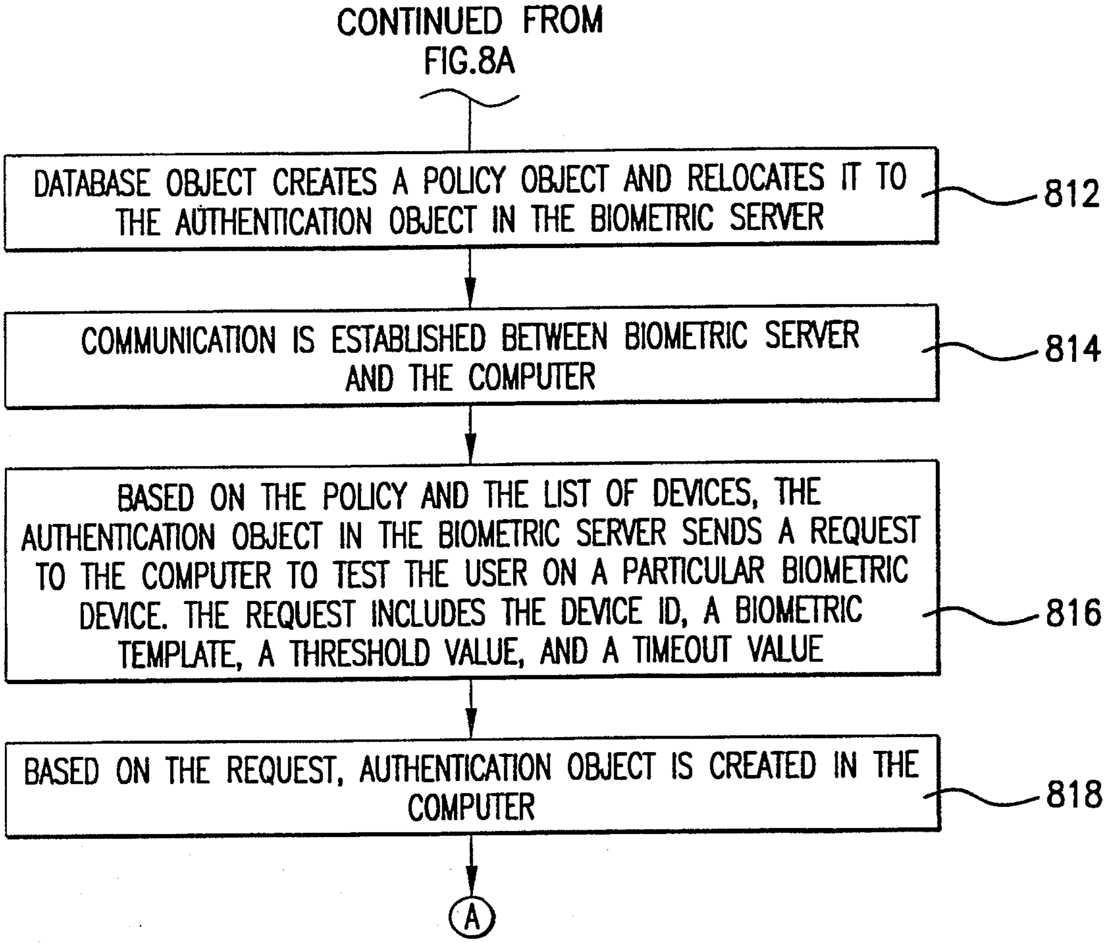

CONTINUED FROM FIG.8A
DATABASE OBJECT CREATES A POLICY OBJECT AND RELOCATES IT TO THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER
812
COMMUNICATION IS ESTABLISHED BETWEEN BIOMETRIC SERVER AND THE COMPUTER
814
BASED ON THE POLICY AND THE LIST OF DEVICES, THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER SENDS A REQUEST TO THE COMPUTER TO TEST THE USER ON A PARTICULAR BIOMETRIC DEVICE. THE REQUEST INCLUDES THE DEVICE ID, A BIOMETRIC TEMPLATE, A THRESHOLD VALUE, AND A TIMEOUT VALUE
816
BASED ON THE REQUEST, AUTHENTICATION OBJECT IS CREATED IN THE COMPUTER
818
A

FIG. 8A-1

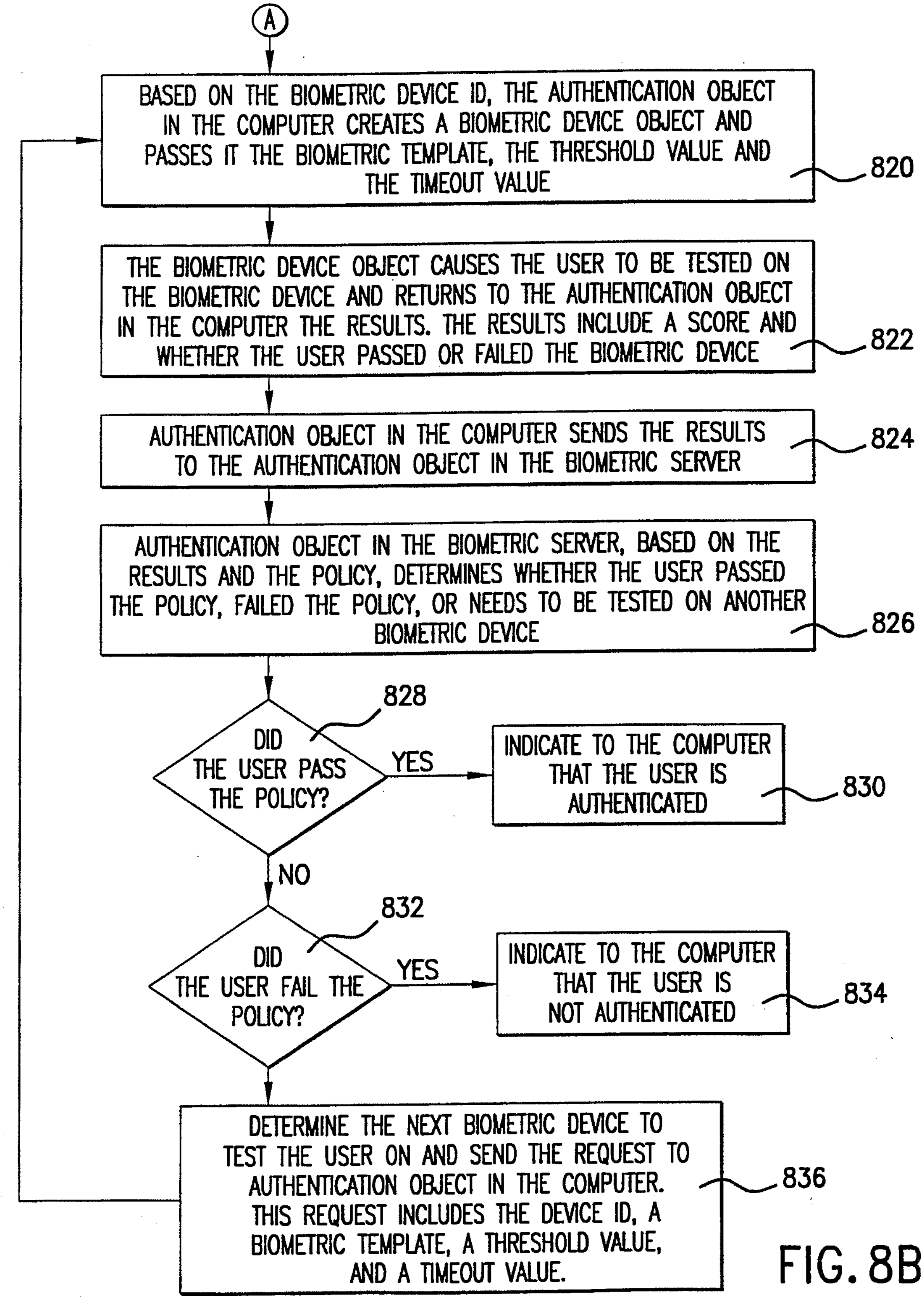

A
BASED ON THE BIOMETRIC DEVICE ID, THE AUTHENTICATION OBJECT IN THE COMPUTER CREATES A BIOMETRIC DEVICE OBJECT AND PASSES IT THE BIOMETRIC TEMPLATE, THE THRESHOLD VALUE AND THE TIMEOUT VALUE
820
THE BIOMETRIC DEVICE OBJECT CAUSES THE USER TO BE TESTED ON THE BIOMETRIC DEVICE AND RETURNS TO THE AUTHENTICATION OBJECT IN THE COMPUTER THE RESULTS. THE RESULTS INCLUDE A SCORE AND WHETHER THE USER PASSED OR FAILED THE BIOMETRIC DEVICE
822
AUTHENTICATION OBJECT IN THE COMPUTER SENDS THE RESULTS TO THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER
824
AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER, BASED ON THE RESULTS AND THE POLICY, DETERMINES WHETHER THE USER PASSED THE POLICY, FAILED THE POLICY, OR NEEDS TO BE TESTED ON ANOTHER BIOMETRIC DEVICE
826
828
DID THE USER PASS THE POLICY?
YES
INDICATE TO THE COMPUTER THAT THE USER IS AUTHENTICATED
830
NO
832
DID THE USER FAIL THE POLICY?
YES
INDICATE TO THE COMPUTER THAT THE USER IS NOT AUTHENTICATED
834
DETERMINE THE NEXT BIOMETRIC DEVICE TO TEST THE USER ON AND SEND THE REQUEST TO AUTHENTICATION OBJECT IN THE COMPUTER. THIS REQUEST INCLUDES THE DEVICE ID, A BIOMETRIC TEMPLATE, A THRESHOLD VALUE, AND A TIMEOUT VALUE.
836

FIG. 8B

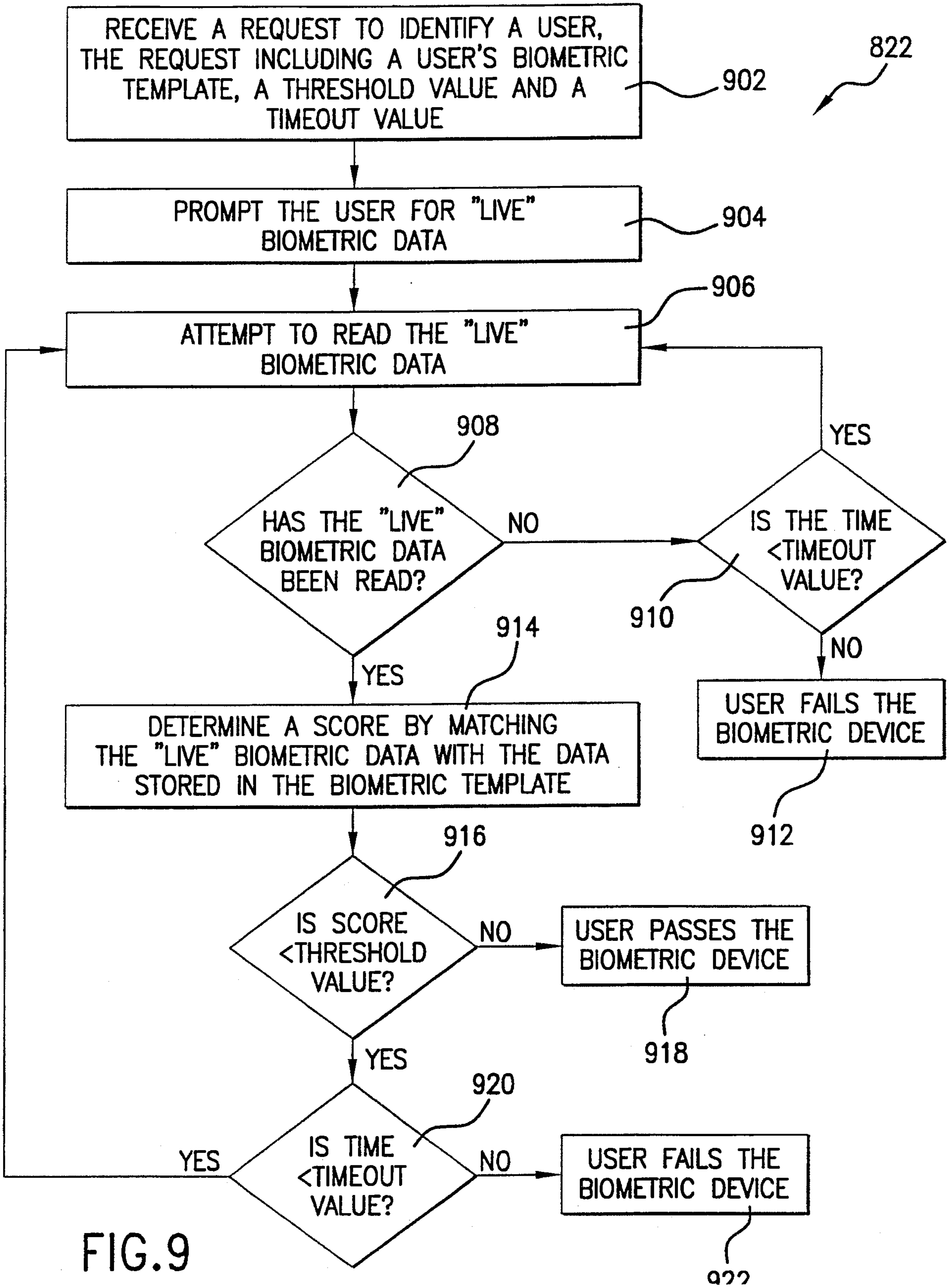

822
RECEIVE A REQUEST TO IDENTIFY A USER, THE REQUEST INCLUDING A USER'S BIOMETRIC TEMPLATE, A THRESHOLD VALUE AND A TIMEOUT VALUE
902
PROMPT THE USER FOR "LIVE" BIOMETRIC DATA
904
ATTEMPT TO READ THE "LIVE" BIOMETRIC DATA
906
HAS THE "LIVE" BIOMETRIC DATA BEEN READ?
908
NO
IS THE TIME <TIMEOUT VALUE?
910
YES
NO
USER FAILS THE BIOMETRIC DEVICE
912
YES
DETERMINE A SCORE BY MATCHING THE "LIVE" BIOMETRIC DATA WITH THE DATA STORED IN THE BIOMETRIC TEMPLATE
914
IS SCORE <THRESHOLD VALUE?
916
NO
USER PASSES THE BIOMETRIC DEVICE
918
YES
IS TIME <TIMEOUT VALUE?
920
YES
NO
USER FAILS THE BIOMETRIC DEVICE
922

FIG.9

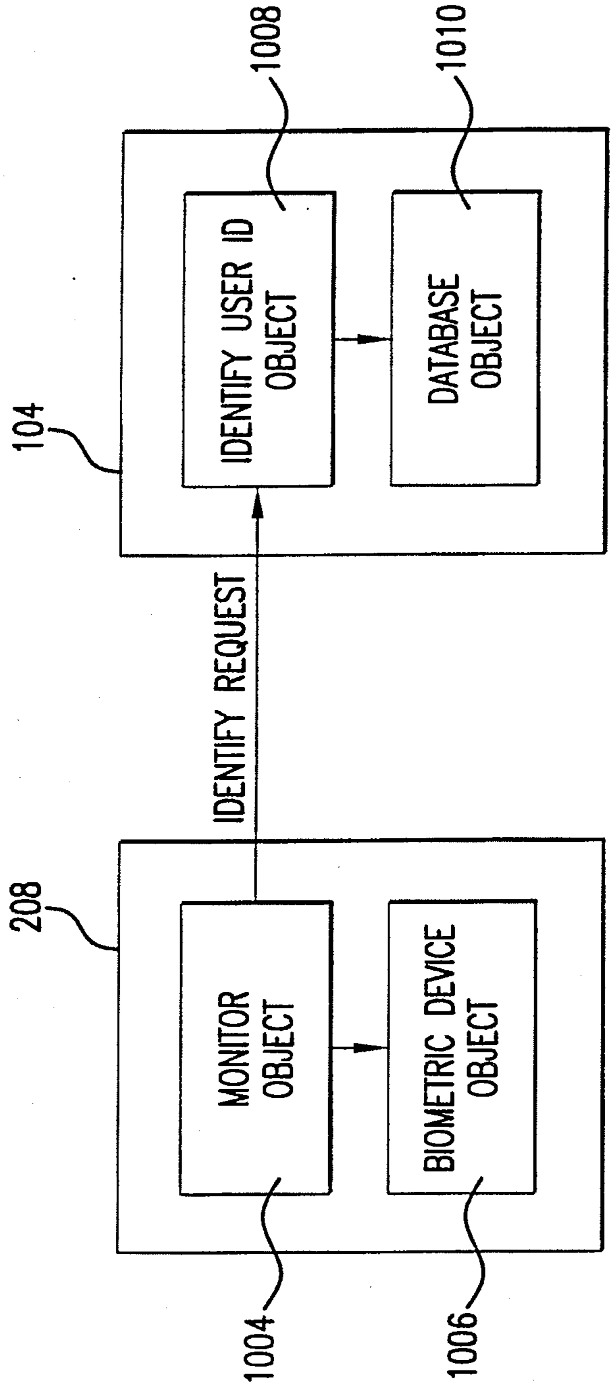

104
1008
1010
IDENTIFY USER ID OBJECT
DATABASE OBJECT
IDENTIFY REQUEST
208
MONITOR OBJECT
BIOMETRIC DEVICE OBJECT
1004
1006

FIG.10

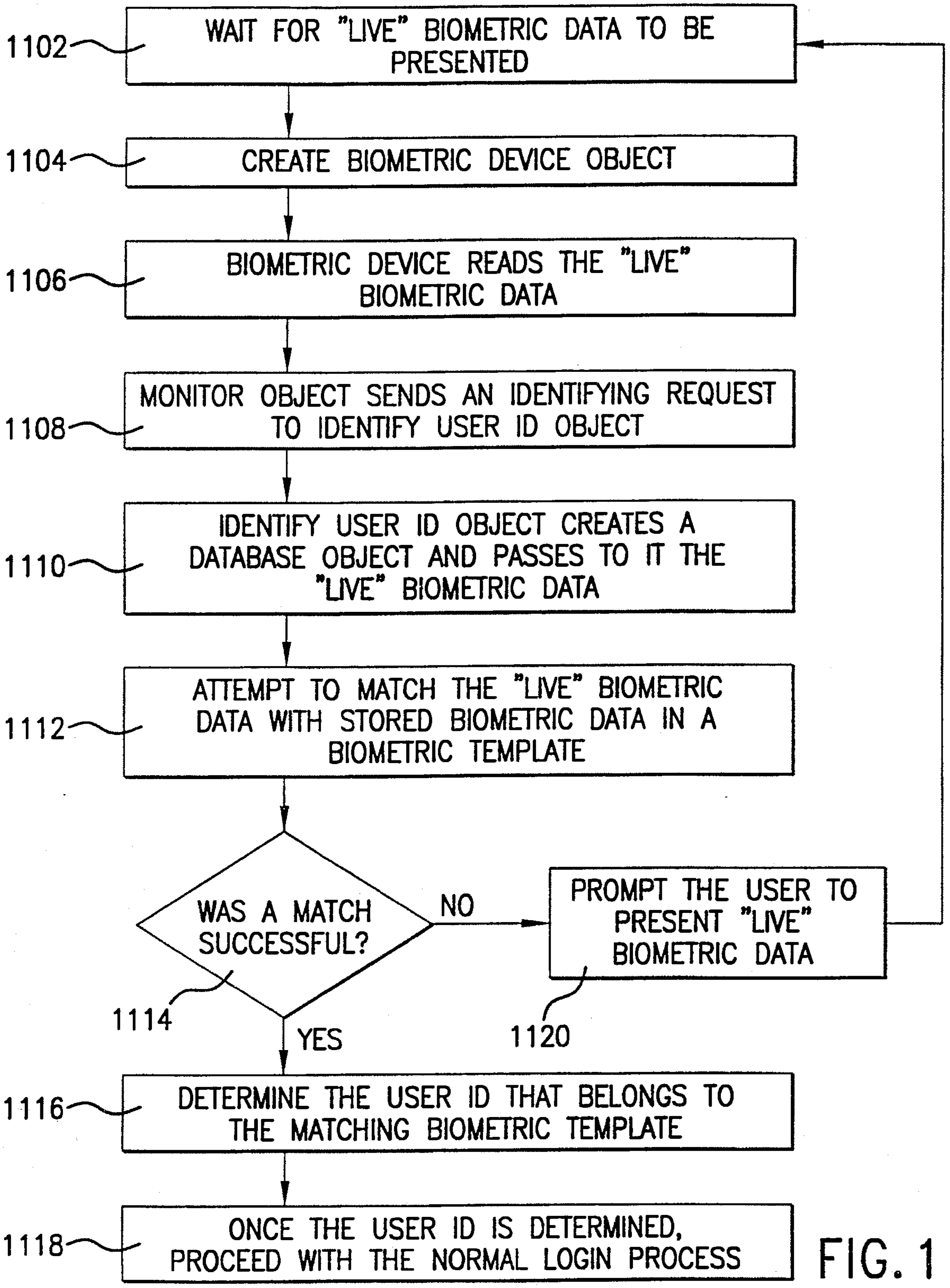

1102
WAIT FOR "LIVE" BIOMETRIC DATA TO BE PRESENTED
1104
CREATE BIOMETRIC DEVICE OBJECT
1106
BIOMETRIC DEVICE READS THE "LIVE" BIOMETRIC DATA
1108
MONITOR OBJECT SENDS AN IDENTIFYING REQUEST TO IDENTIFY USER ID OBJECT
1110
IDENTIFY USER ID OBJECT CREATES A DATABASE OBJECT AND PASSES TO IT THE "LIVE" BIOMETRIC DATA
1112
ATTEMPT TO MATCH THE "LIVE" BIOMETRIC DATA WITH STORED BIOMETRIC DATA IN A BIOMETRIC TEMPLATE
WAS A MATCH SUCCESSFUL?
1114
NO
PROMPT THE USER TO PRESENT "LIVE" BIOMETRIC DATA
1120
YES
1116
DETERMINE THE USER ID THAT BELONGS TO THE MATCHING BIOMETRIC TEMPLATE
1118
ONCE THE USER ID IS DETERMINED, PROCEED WITH THE NORMAL LOGIN PROCESS

FIG. 11

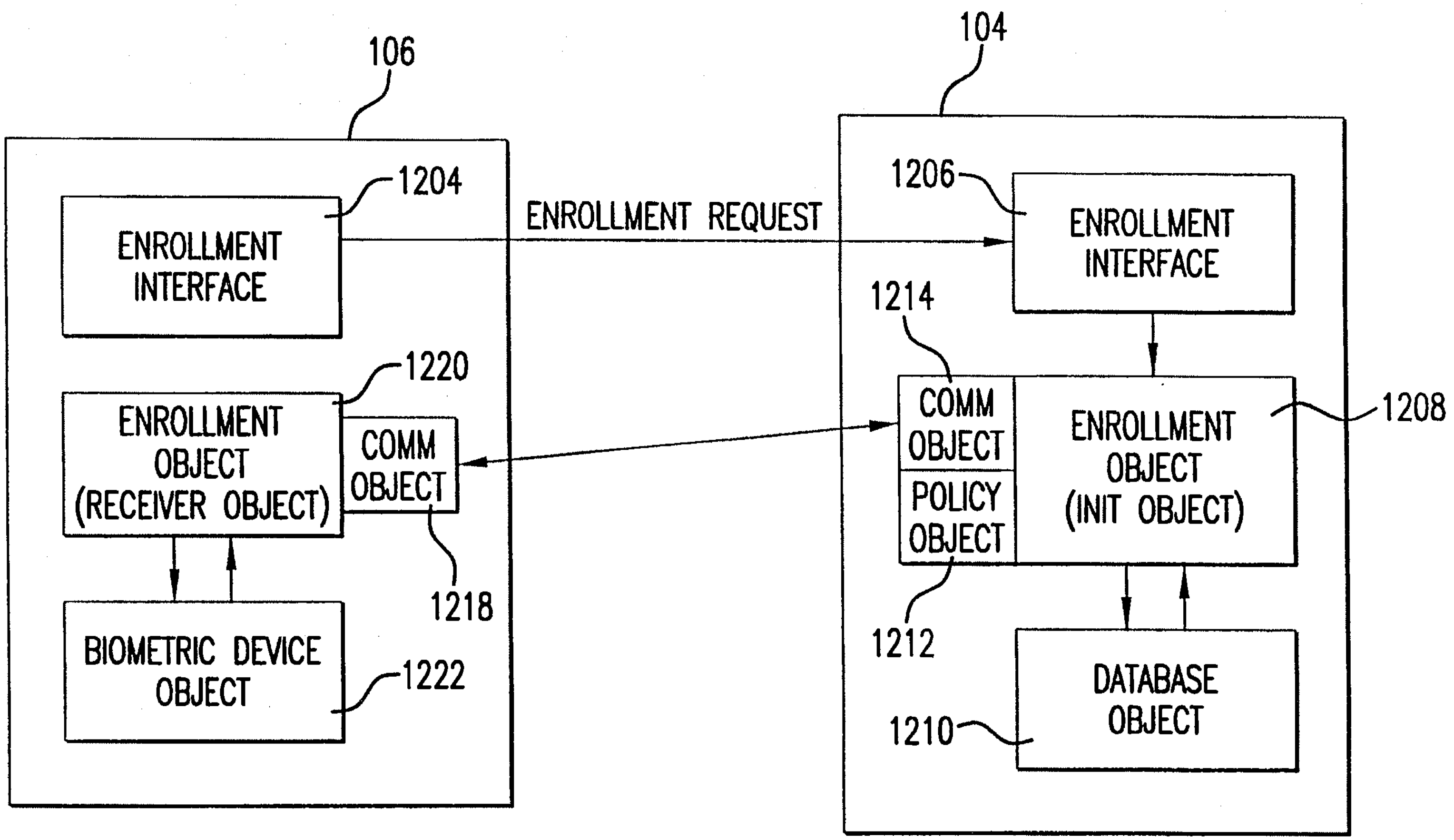

106
1204
ENROLLMENT INTERFACE
ENROLLMENT REQUEST
1220
ENROLLMENT OBJECT (RECEIVER OBJECT)
COMM OBJECT
1218
BIOMETRIC DEVICE OBJECT
1222
104
1206
ENROLLMENT INTERFACE
1214
COMM OBJECT
POLICY OBJECT
1212
ENROLLMENT OBJECT (INIT OBJECT)
1208
DATABASE OBJECT
1210

FIG. 12

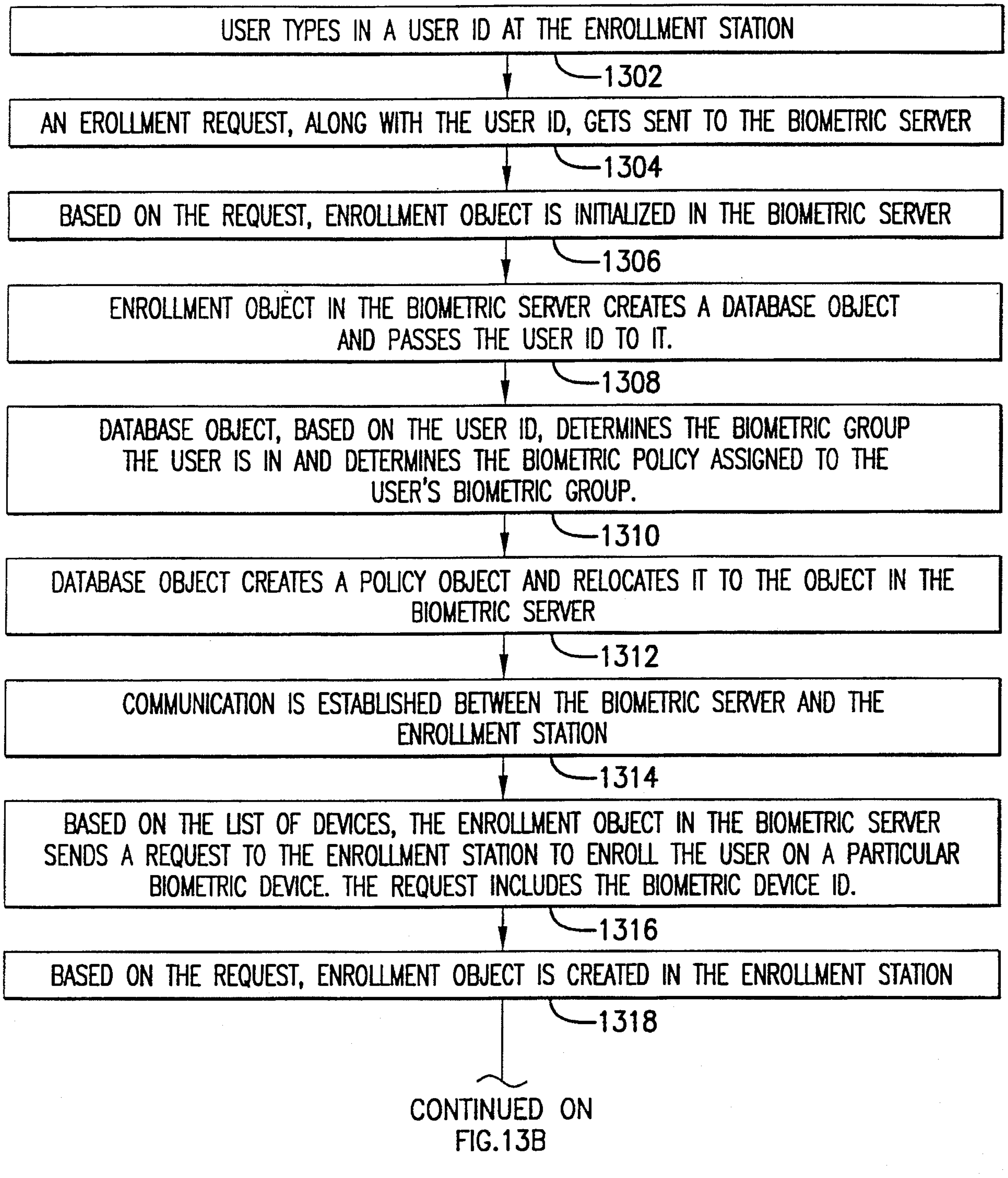

USER TYPES IN A USER ID AT THE ENROLLMENT STATION
1302
AN EROLLMENT REQUEST, ALONG WITH THE USER ID, GETS SENT TO THE BIOMETRIC SERVER
1304
BASED ON THE REQUEST, ENROLLMENT OBJECT IS INITIALIZED IN THE BIOMETRIC SERVER
1306
ENROLLMENT OBJECT IN THE BIOMETRIC SERVER CREATES A DATABASE OBJECT AND PASSES THE USER ID TO IT.
1308
DATABASE OBJECT, BASED ON THE USER ID, DETERMINES THE BIOMETRIC GROUP THE USER IS IN AND DETERMINES THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP.
1310
DATABASE OBJECT CREATES A POLICY OBJECT AND RELOCATES IT TO THE OBJECT IN THE BIOMETRIC SERVER
1312
COMMUNICATION IS ESTABLISHED BETWEEN THE BIOMETRIC SERVER AND THE ENROLLMENT STATION
1314
BASED ON THE LIST OF DEVICES, THE ENROLLMENT OBJECT IN THE BIOMETRIC SERVER SENDS A REQUEST TO THE ENROLLMENT STATION TO ENROLL THE USER ON A PARTICULAR BIOMETRIC DEVICE. THE REQUEST INCLUDES THE BIOMETRIC DEVICE ID.
1316
BASED ON THE REQUEST, ENROLLMENT OBJECT IS CREATED IN THE ENROLLMENT STATION
1318
CONTINUED ON FIG.13B

FIG. 13A

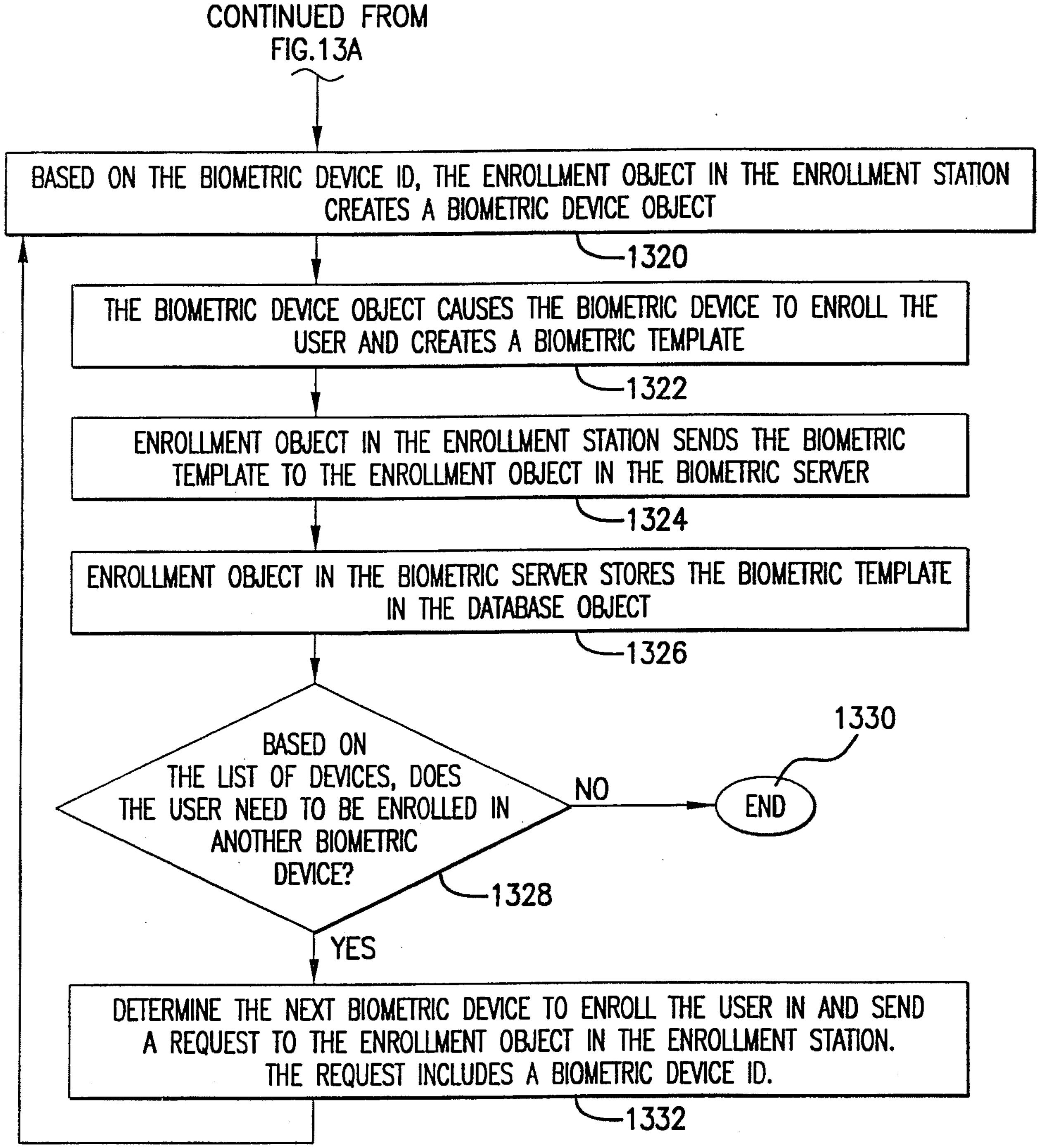
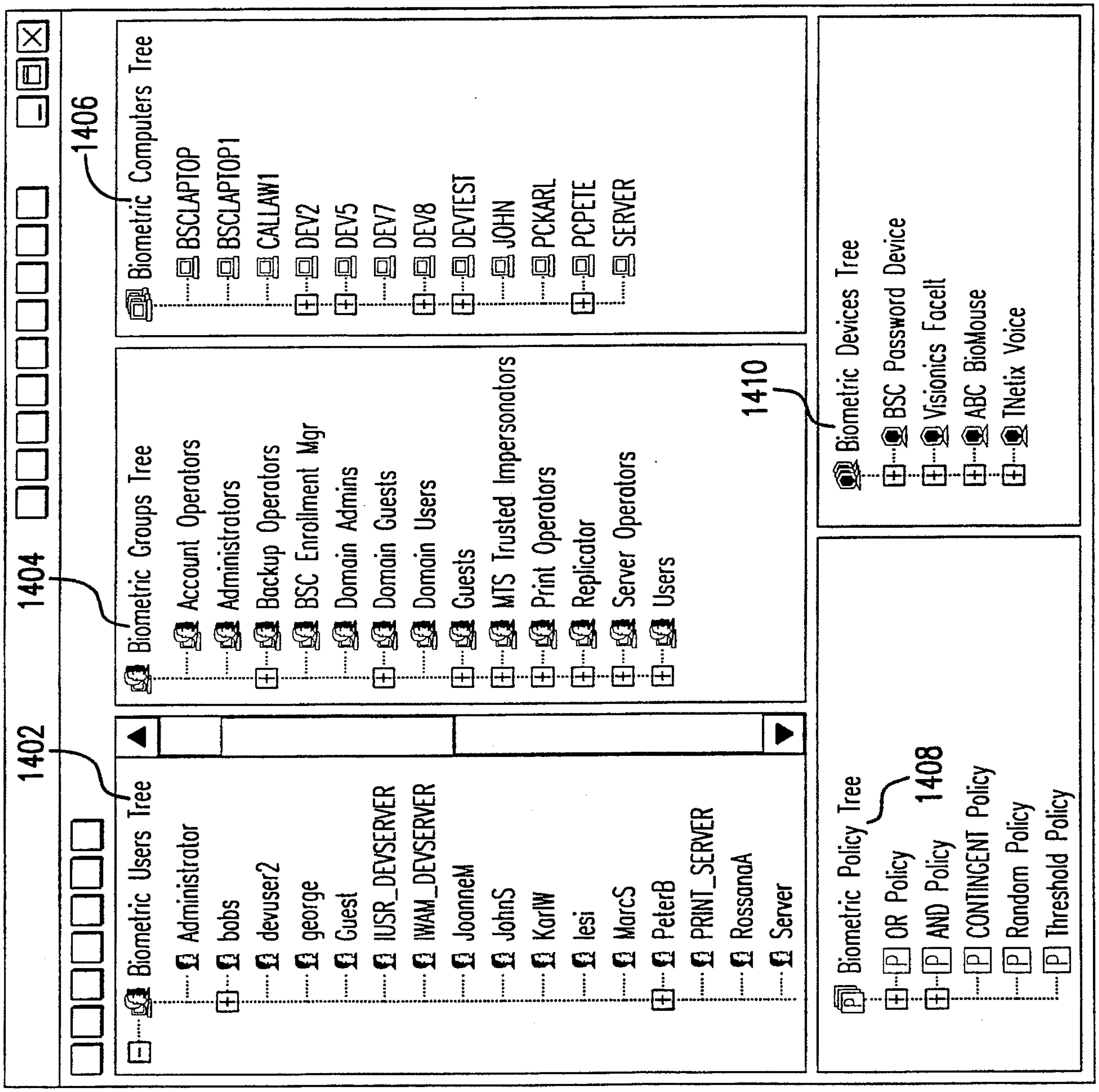

CONTINUED FROM FIG.13A
BASED ON THE BIOMETRIC DEVICE ID, THE ENROLLMENT OBJECT IN THE ENROLLMENT STATION CREATES A BIOMETRIC DEVICE OBJECT
1320
THE BIOMETRIC DEVICE OBJECT CAUSES THE BIOMETRIC DEVICE TO ENROLL THE USER AND CREATES A BIOMETRIC TEMPLATE
1322
ENROLLMENT OBJECT IN THE ENROLLMENT STATION SENDS THE BIOMETRIC TEMPLATE TO THE ENROLLMENT OBJECT IN THE BIOMETRIC SERVER
1324
ENROLLMENT OBJECT IN THE BIOMETRIC SERVER STORES THE BIOMETRIC TEMPLATE IN THE DATABASE OBJECT
1326
BASED ON THE LIST OF DEVICES, DOES THE USER NEED TO BE ENROLLED IN ANOTHER BIOMETRIC DEVICE?
1328
NO
END
1330
YES
DETERMINE THE NEXT BIOMETRIC DEVICE TO ENROLL THE USER IN AND SEND A REQUEST TO THE ENROLLMENT OBJECT IN THE ENROLLMENT STATION. THE REQUEST INCLUDES A BIOMETRIC DEVICE ID.
1332

FIG. 13B



Biometric Users Tree
- Administrator
- bobs
- devuser2
- george
- Guest
- IUSR_DEVSERVER
- IWAM_DEVSERVER
- JoanneM
- JohnS
- KarlW
- lesi
- MarcS
- PeterB
- PRINT_SERVER
- RossanaA
- Server

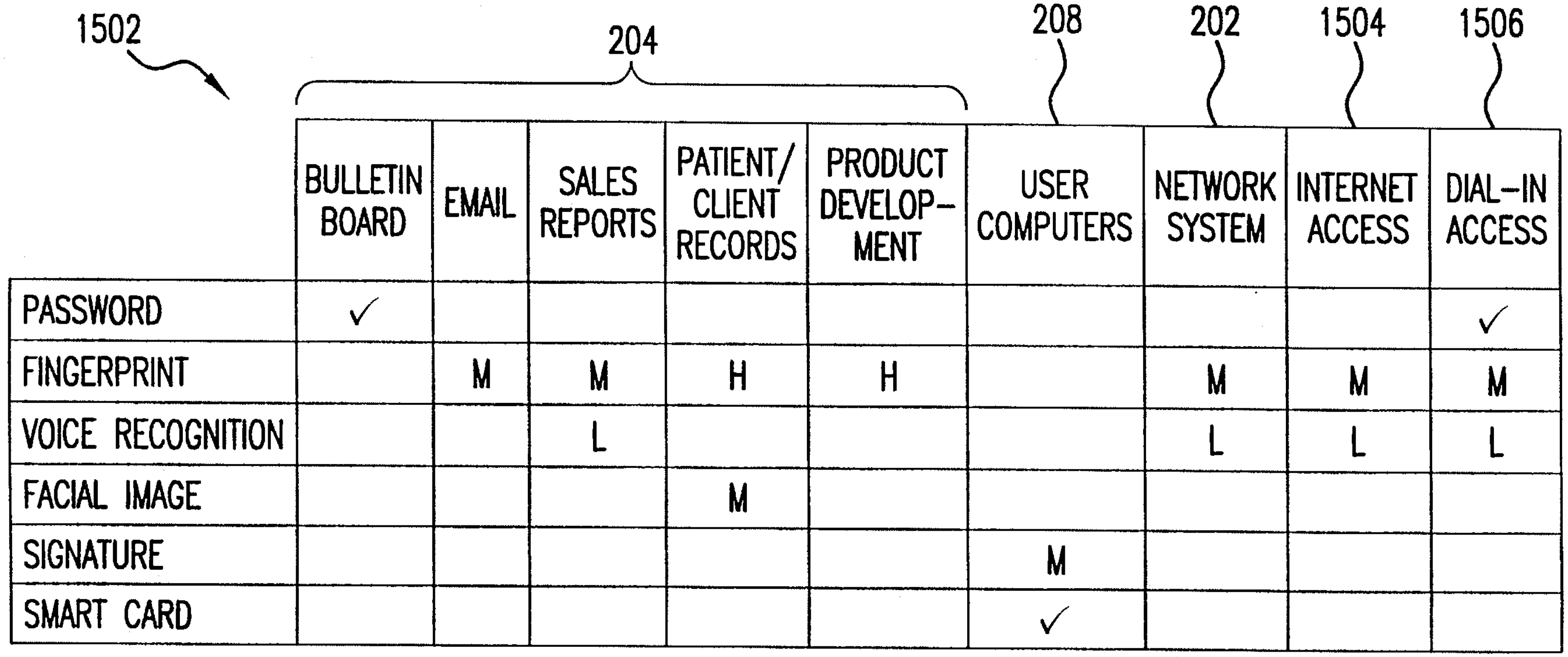
Biometric Groups Tree
- Account Operators
- Administrators
- Backup Operators
- BSC Enrollment Mgr
- Domain Admins
- Domain Guests
- Domain Users
- Guests
- MTS Trusted Impersonators
- Print Operators
- Replicator
- Server Operators
- Users

Biometric Computers Tree
- BSCLAPTOP
- BSCLAPTOP1
- CALLAW1
- DEV2
- DEV5
- DEV7
- DEV8
- DEVTEST
- JOHN
- PCKARL
- PCPETE
- SERVER

Biometric Policy Tree
- OR Policy
- AND Policy
- CONTINGENT Policy
- Random Policy
- Threshold Policy

Biometric Devices Tree
- BSC Password Device
- Visionics FaceIt
- ABC BioMouse
- TNetix Voice

FIG. 14


1502
204
208
202
1504
1506

	BULLETIN BOARD	EMAIL	SALES REPORTS	PATIENT/ CLIENT RECORDS	PRODUCT DEVELOP-MENT	USER COMPUTERS	NETWORK SYSTEM	INTERNET ACCESS	DIAL-IN ACCESS
PASSWORD	✓								✓
FINGERPRINT		M	M	H	H		M	M	M
VOICE RECOGNITION			L				L	L	L
FACIAL IMAGE				M					
SIGNATURE						M			
SMART CARD						✓			

FIG. 15

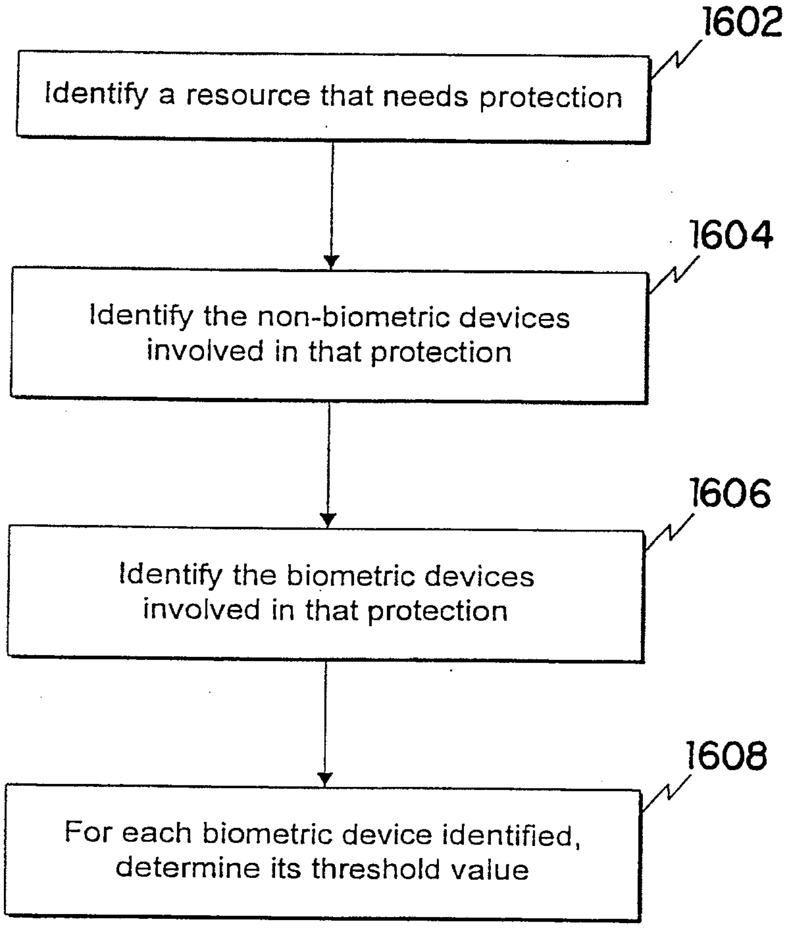

1602
Identify a resource that needs protection
1604
Identify the non-biometric devices involved in that protection
1606
Identify the biometric devices involved in that protection
1608
For each biometric device identified, determine its threshold value

FIG. 16

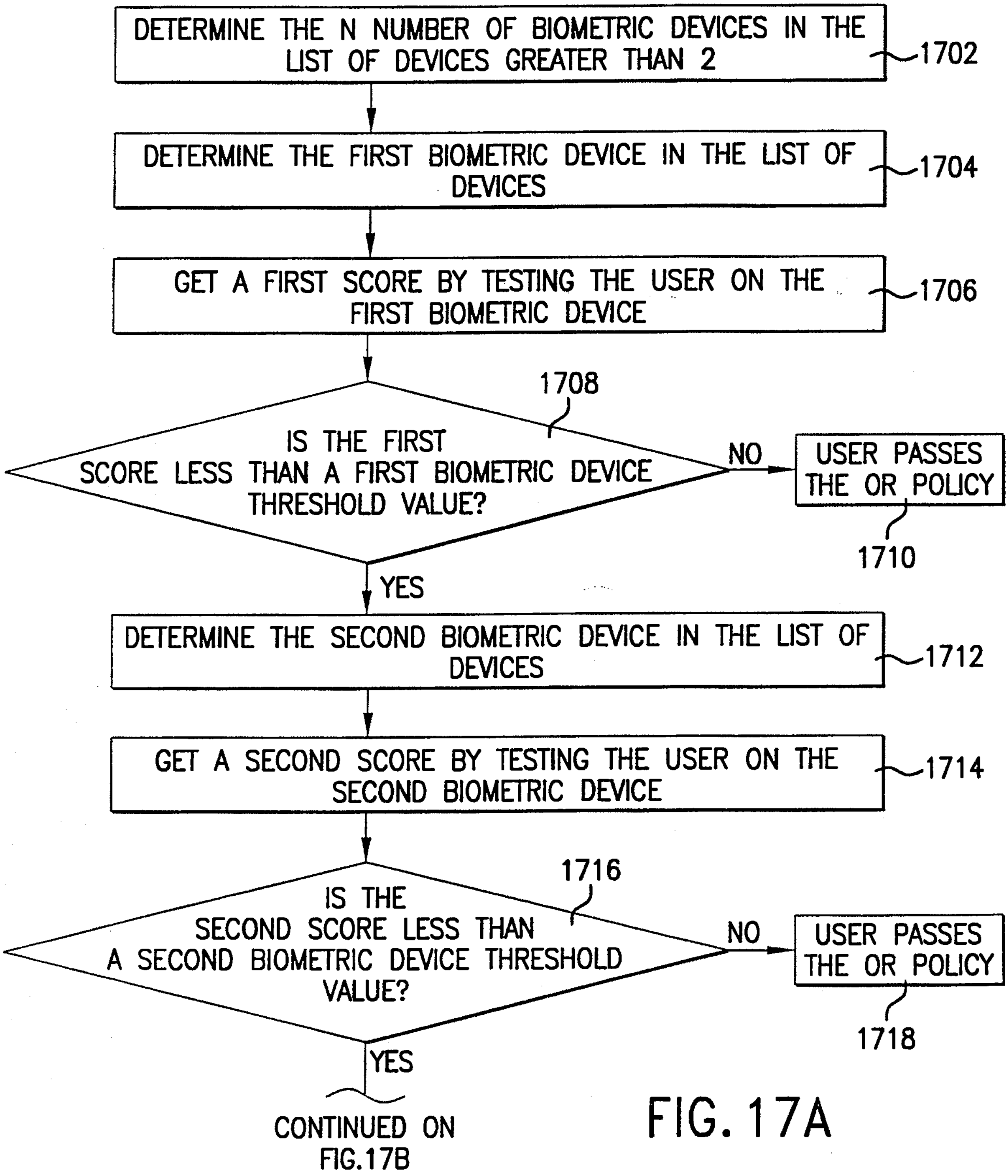

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 2
1702
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
1704
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
1706
1708
IS THE FIRST SCORE LESS THAN A FIRST BIOMETRIC DEVICE THRESHOLD VALUE?
NO
USER PASSES THE OR POLICY
1710
YES
DETERMINE THE SECOND BIOMETRIC DEVICE IN THE LIST OF DEVICES
1712
GET A SECOND SCORE BY TESTING THE USER ON THE SECOND BIOMETRIC DEVICE
1714
1716
IS THE SECOND SCORE LESS THAN A SECOND BIOMETRIC DEVICE THRESHOLD VALUE?
NO
USER PASSES THE OR POLICY
1718
YES
CONTINUED ON FIG.17B

FIG. 17A

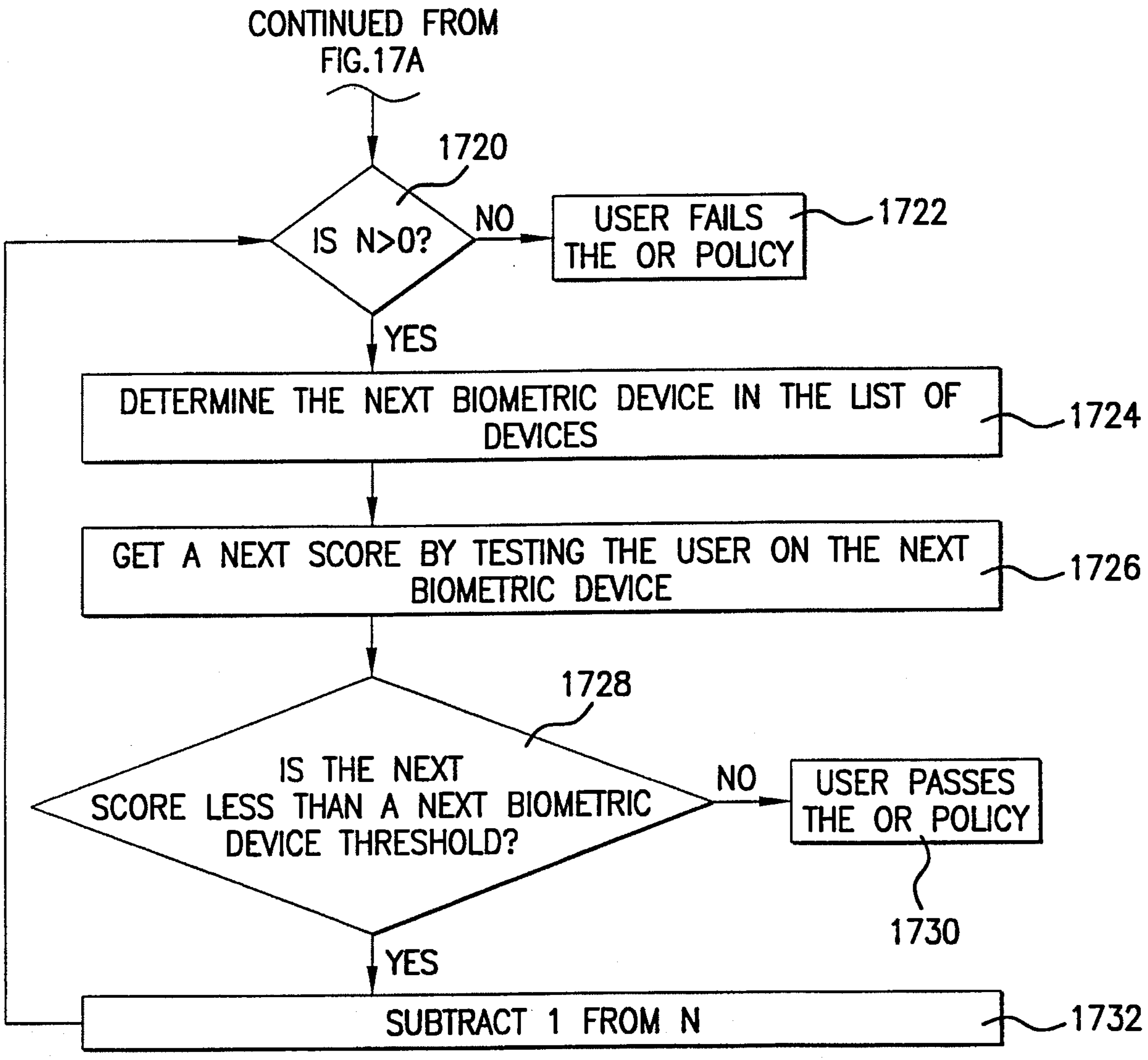

CONTINUED FROM FIG.17A
1720
IS N>0?
NO
USER FAILS THE OR POLICY
1722
YES
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
1724
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
1726
1728
IS THE NEXT SCORE LESS THAN A NEXT BIOMETRIC DEVICE THRESHOLD?
NO
USER PASSES THE OR POLICY
1730
YES
SUBTRACT 1 FROM N
1732

FIG. 17B

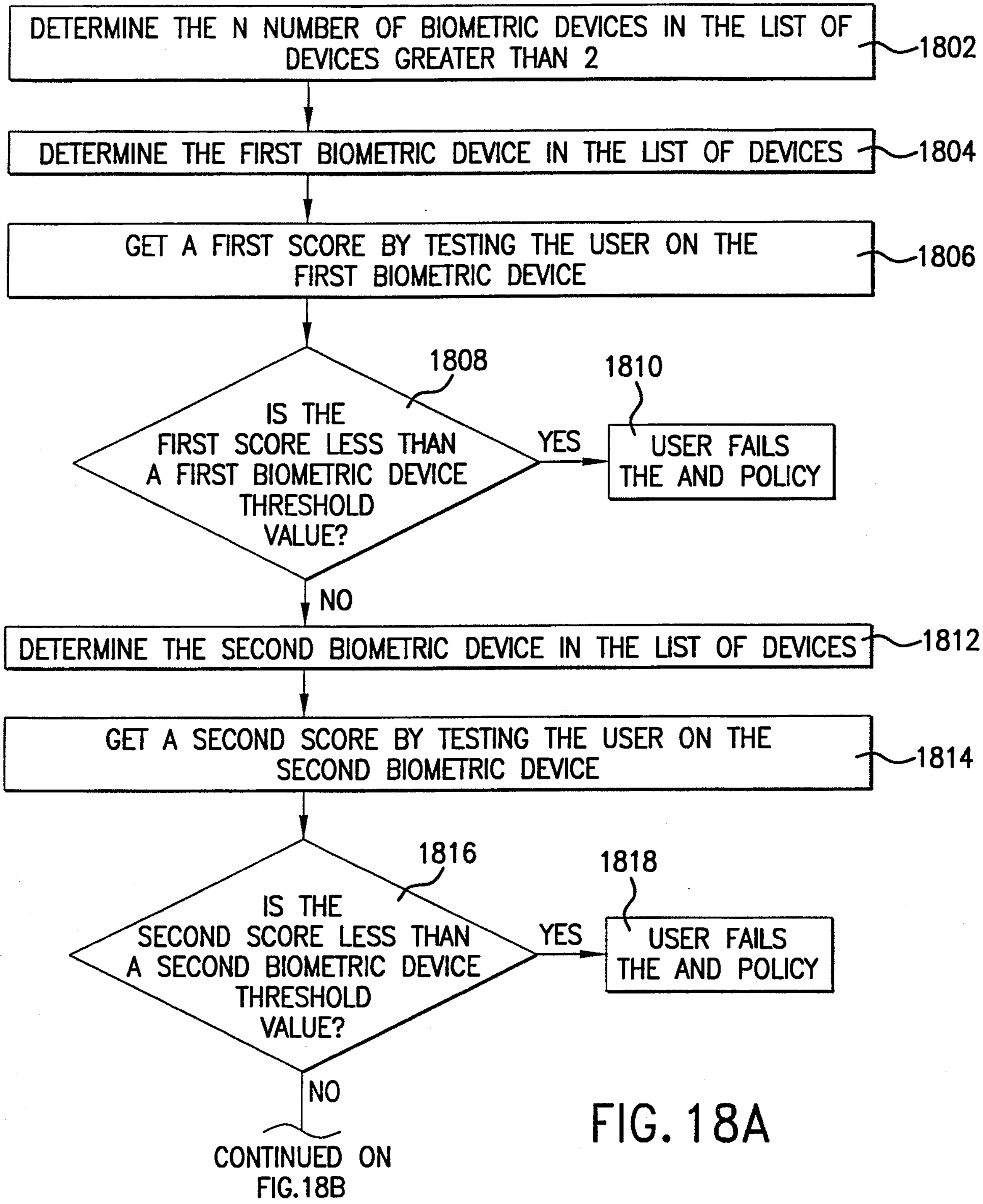

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 2
1802
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
1804
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
1806
1808
IS THE FIRST SCORE LESS THAN A FIRST BIOMETRIC DEVICE THRESHOLD VALUE?
YES
1810
USER FAILS THE AND POLICY
NO
DETERMINE THE SECOND BIOMETRIC DEVICE IN THE LIST OF DEVICES
1812
GET A SECOND SCORE BY TESTING THE USER ON THE SECOND BIOMETRIC DEVICE
1814
1816
IS THE SECOND SCORE LESS THAN A SECOND BIOMETRIC DEVICE THRESHOLD VALUE?
YES
1818
USER FAILS THE AND POLICY
NO
CONTINUED ON FIG.18B

FIG. 18A

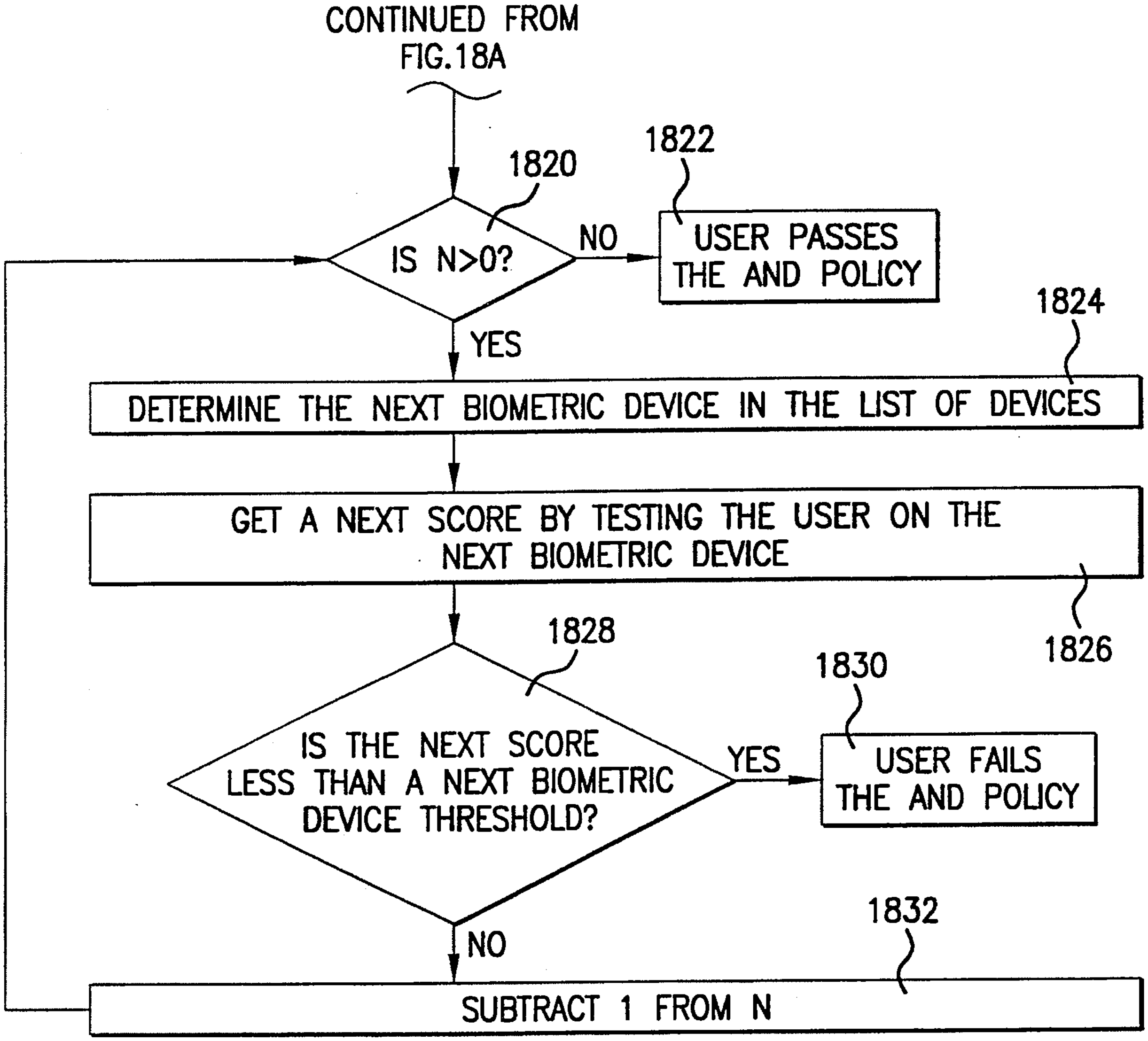

CONTINUED FROM FIG.18A
1820
1822
IS N>0?
NO
USER PASSES THE AND POLICY
1824
YES
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
1826
1828
1830
IS THE NEXT SCORE LESS THAN A NEXT BIOMETRIC DEVICE THRESHOLD?
YES
USER FAILS THE AND POLICY
NO
1832
SUBTRACT 1 FROM N

FIG. 18B

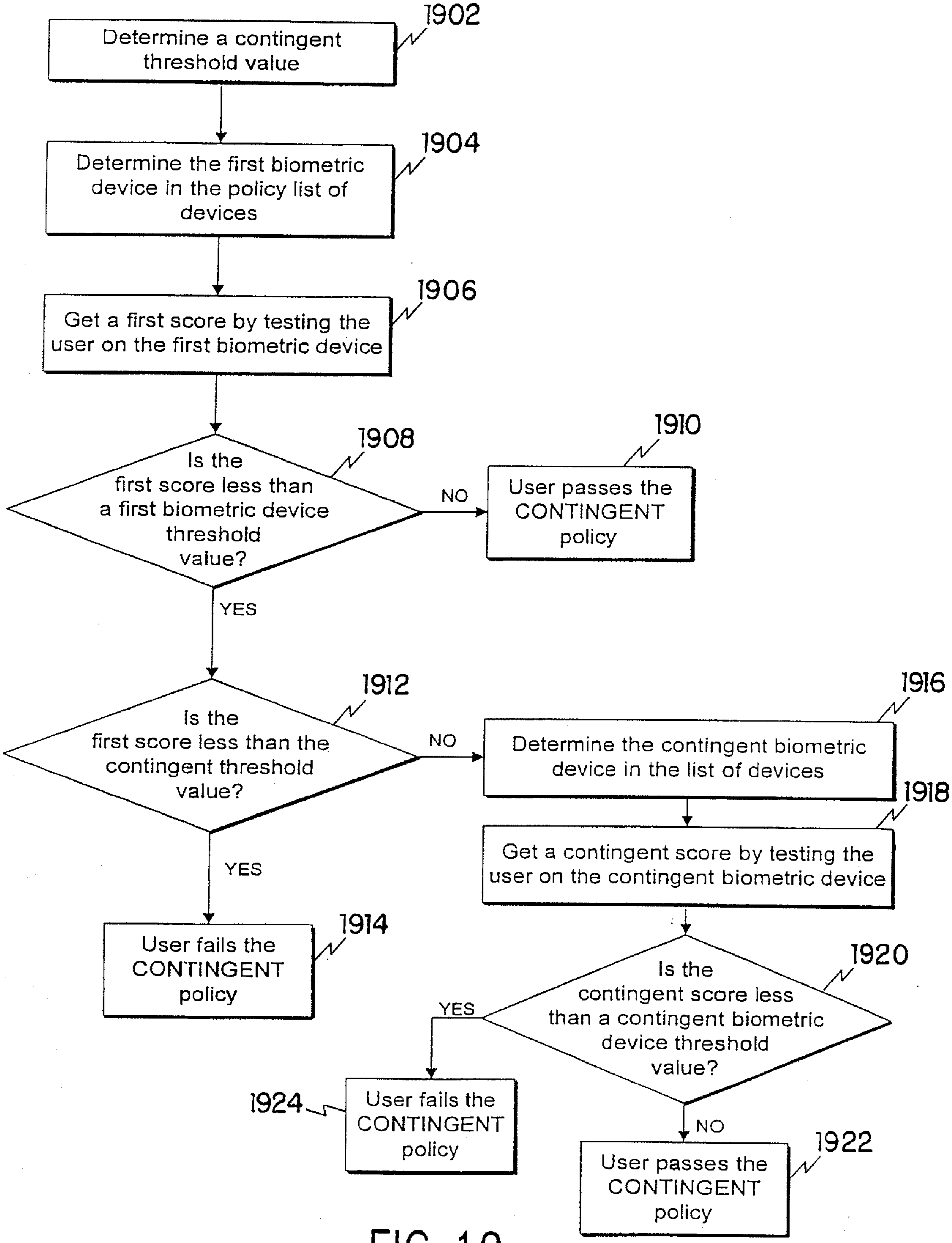

1902
Determine a contingent threshold value
1904
Determine the first biometric device in the policy list of devices
1906
Get a first score by testing the user on the first biometric device
1908
Is the first score less than a first biometric device threshold value?
NO
1910
User passes the CONTINGENT policy
YES
1912
Is the first score less than the contingent threshold value?
NO
1916
Determine the contingent biometric device in the list of devices
1918
Get a contingent score by testing the user on the contingent biometric device
YES
1914
User fails the CONTINGENT policy
1920
Is the contingent score less than a contingent biometric device threshold value?
YES
1924
User fails the CONTINGENT policy
NO
1922
User passes the CONTINGENT policy

FIG. 19

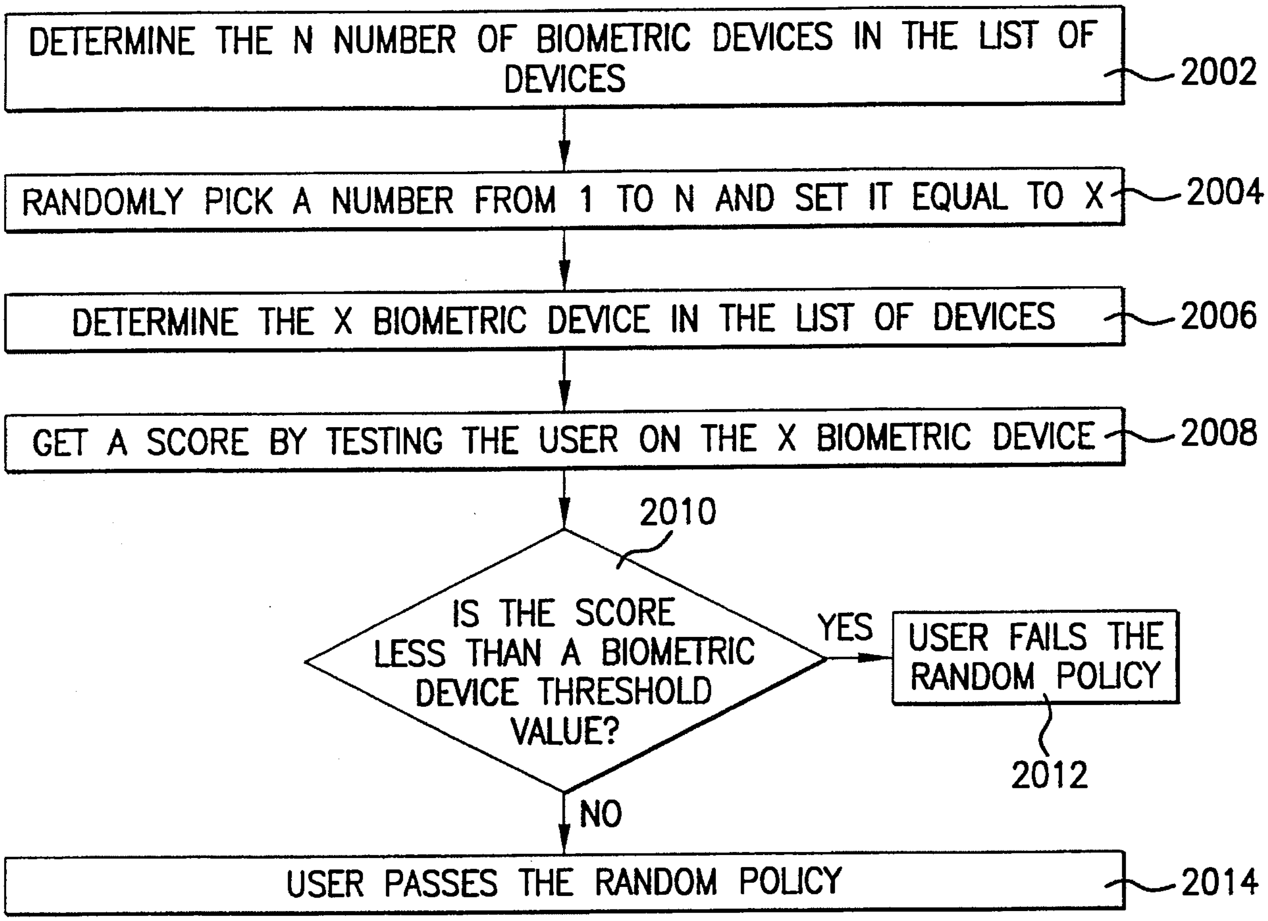

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES
2002
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2004
DETERMINE THE X BIOMETRIC DEVICE IN THE LIST OF DEVICES
2006
GET A SCORE BY TESTING THE USER ON THE X BIOMETRIC DEVICE
2008
2010
IS THE SCORE LESS THAN A BIOMETRIC DEVICE THRESHOLD VALUE?
YES
USER FAILS THE RANDOM POLICY
2012
NO
USER PASSES THE RANDOM POLICY
2014

FIG. 20

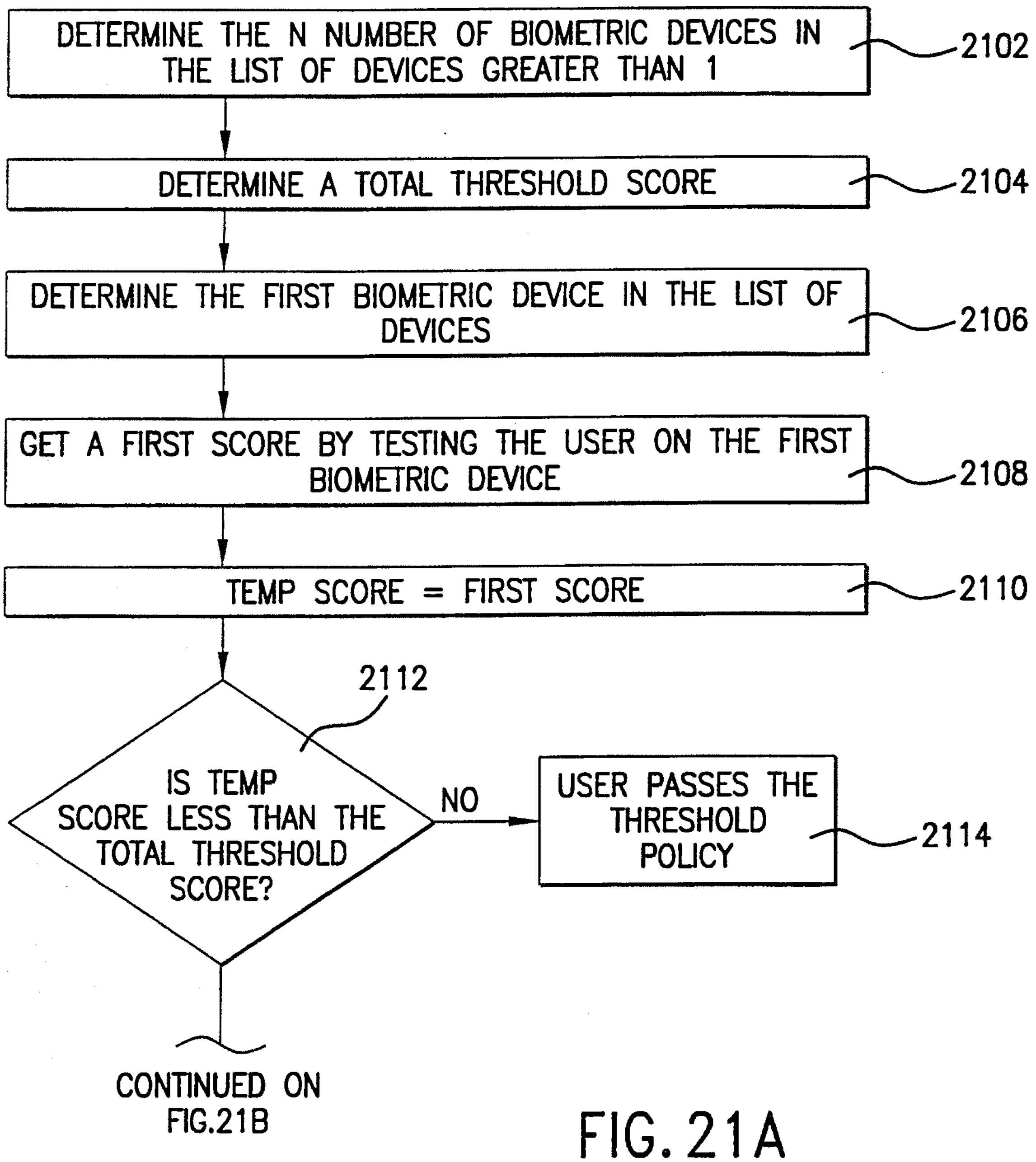

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 1
2102
DETERMINE A TOTAL THRESHOLD SCORE
2104
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
2106
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
2108
TEMP SCORE = FIRST SCORE
2110
2112
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY
2114
CONTINUED ON FIG.21B

FIG. 21A

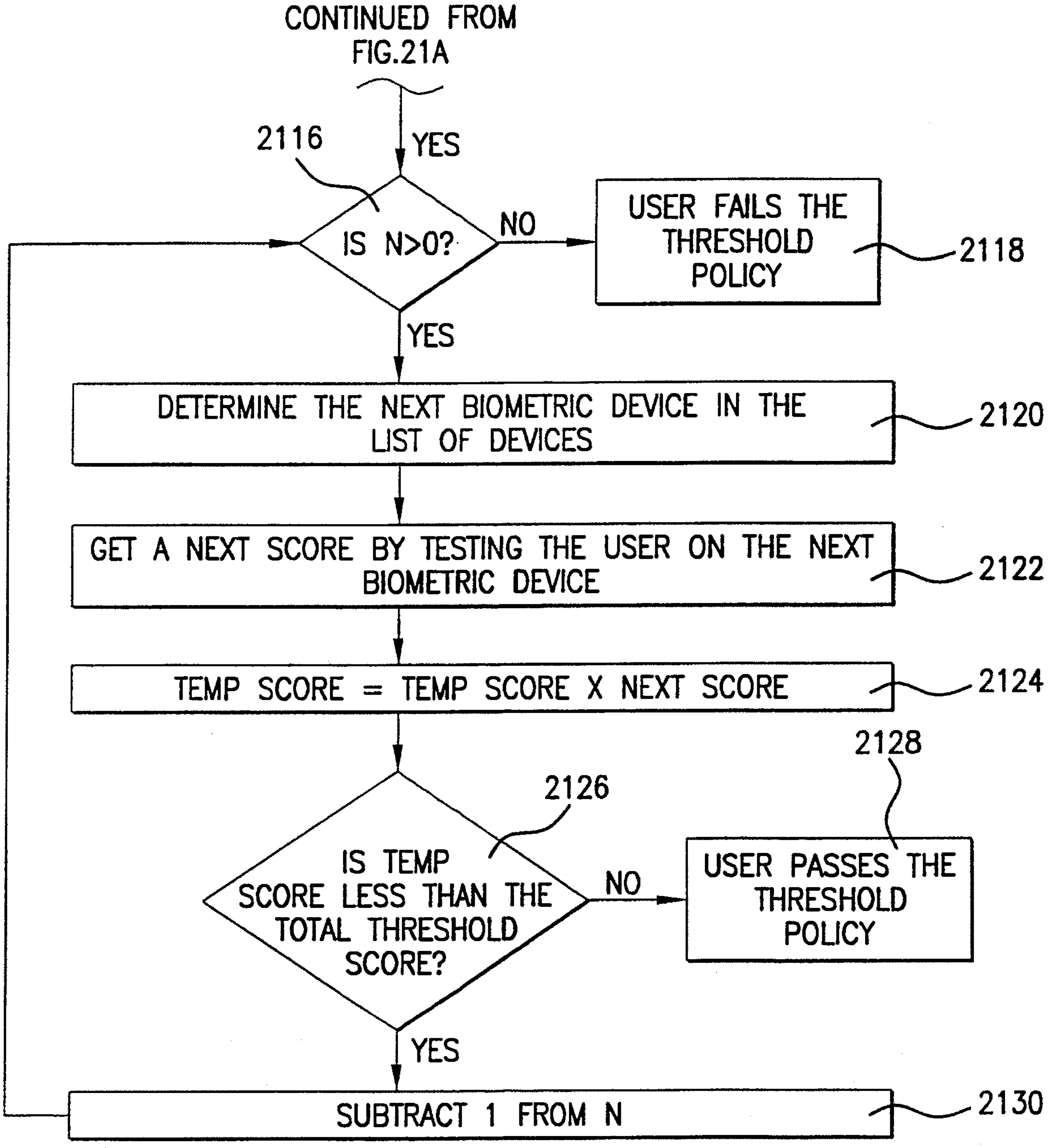

CONTINUED FROM FIG.21A
YES
2116
IS N>0?
NO
USER FAILS THE THRESHOLD POLICY
2118
YES
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
2120
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
2122
TEMP SCORE = TEMP SCORE X NEXT SCORE
2124
2128
2126
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY
YES
SUBTRACT 1 FROM N
2130

FIG. 21B

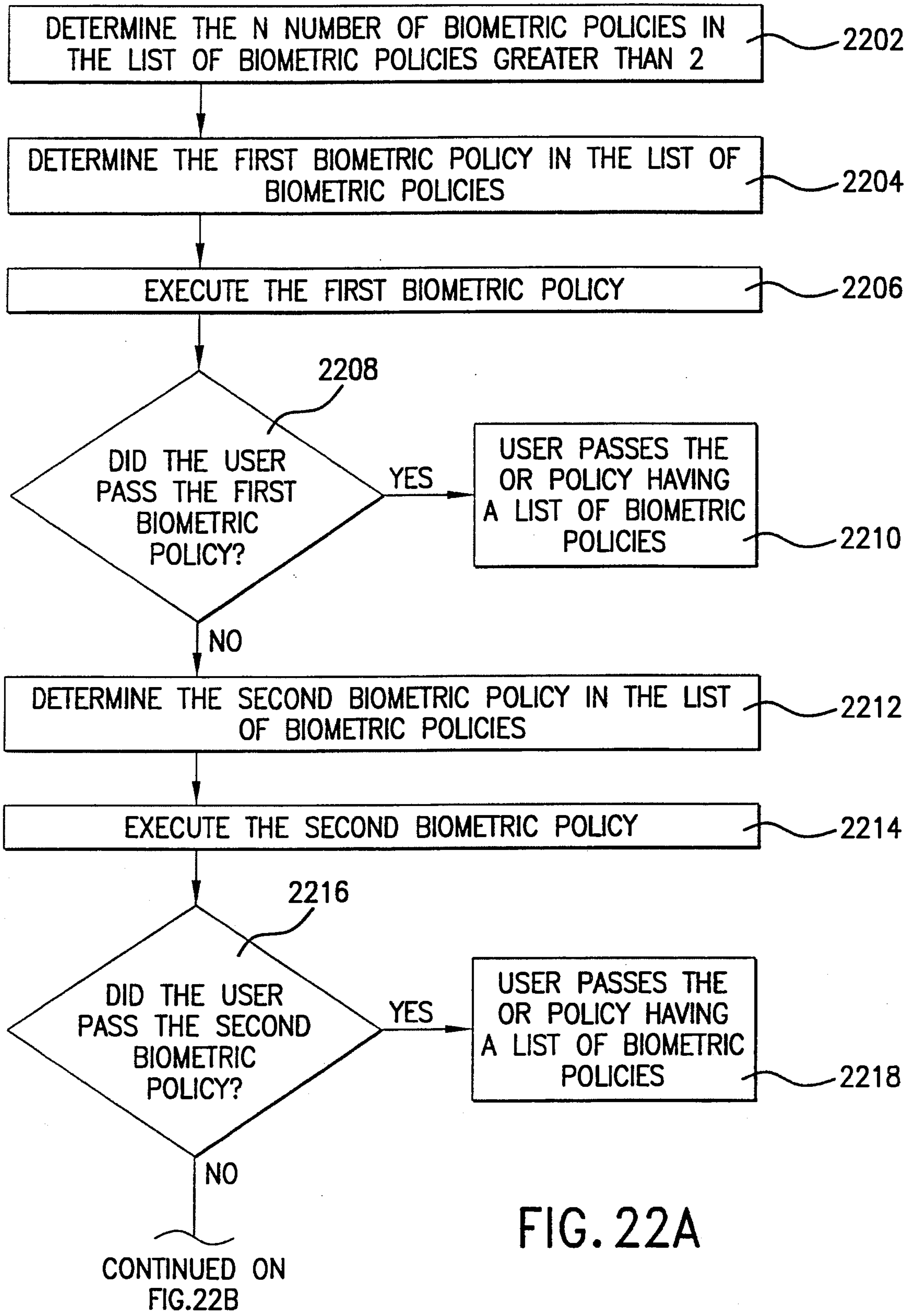

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 2
2202
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2204
EXECUTE THE FIRST BIOMETRIC POLICY
2206
2208
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2210
NO
DETERMINE THE SECOND BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2212
EXECUTE THE SECOND BIOMETRIC POLICY
2214
2216
DID THE USER PASS THE SECOND BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2218
NO
CONTINUED ON FIG.22B

FIG. 22A

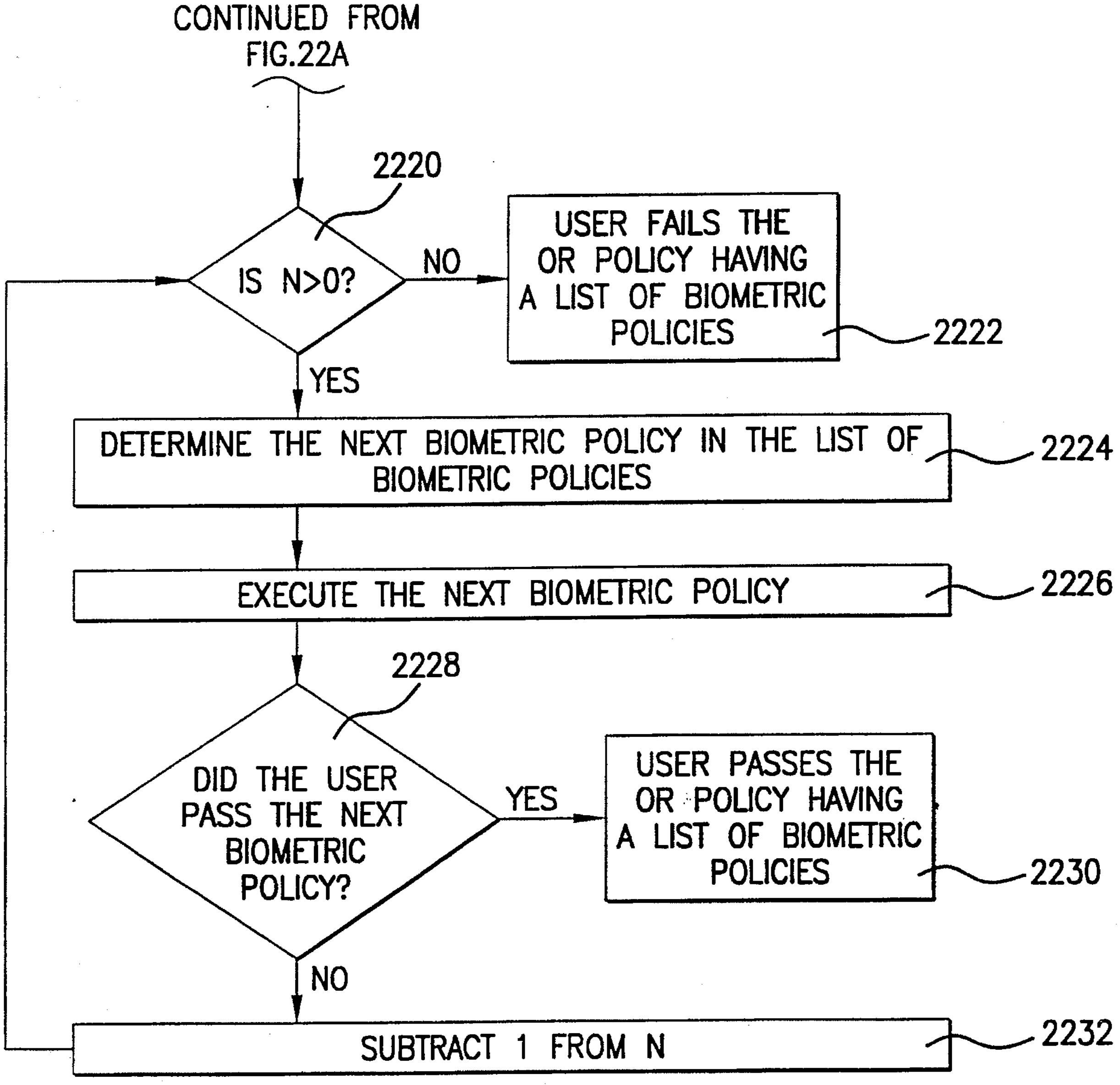

CONTINUED FROM FIG.22A
2220
IS N>0?
NO
USER FAILS THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2222
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2224
EXECUTE THE NEXT BIOMETRIC POLICY
2226
2228
DID THE USER PASS THE NEXT BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2230
NO
SUBTRACT 1 FROM N
2232

FIG. 22B

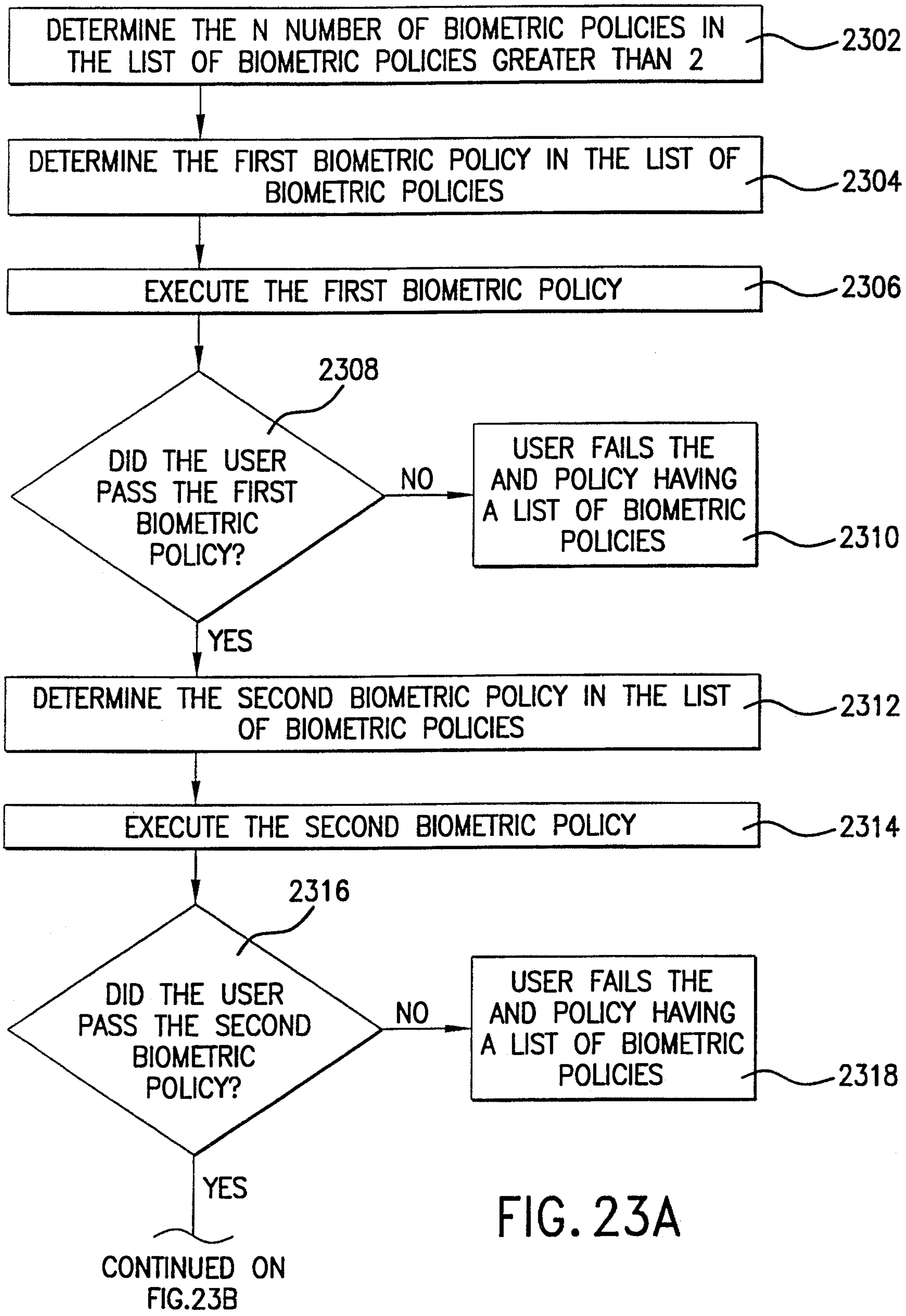

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 2
2302
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2304
EXECUTE THE FIRST BIOMETRIC POLICY
2306
2308
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2310
YES
DETERMINE THE SECOND BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2312
EXECUTE THE SECOND BIOMETRIC POLICY
2314
2316
DID THE USER PASS THE SECOND BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2318
YES
CONTINUED ON FIG.23B

FIG. 23A

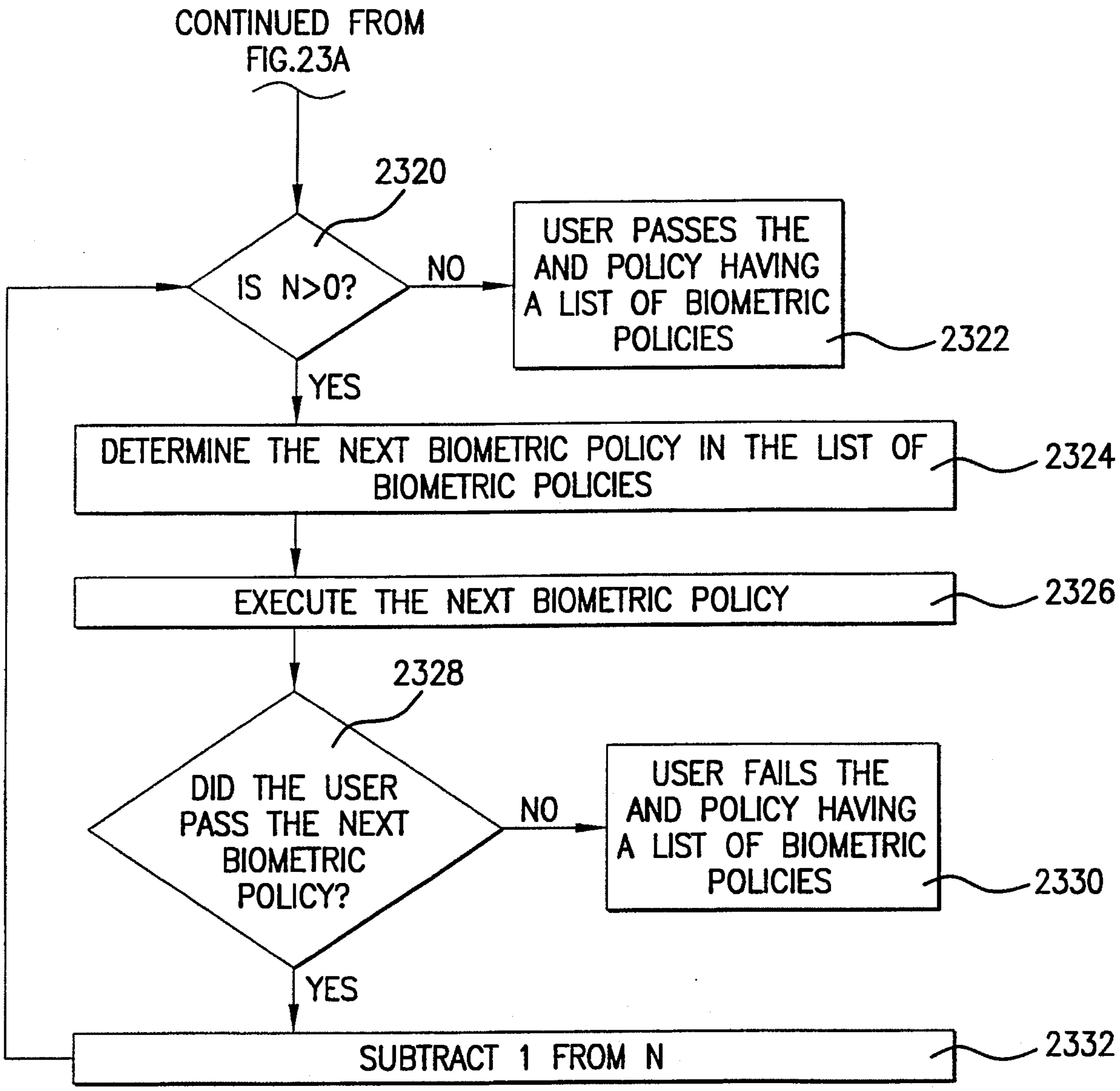

CONTINUED FROM FIG.23A
2320
IS N>0?
NO
USER PASSES THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2322
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2324
EXECUTE THE NEXT BIOMETRIC POLICY
2326
2328
DID THE USER PASS THE NEXT BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2330
YES
SUBTRACT 1 FROM N
2332

FIG. 23B

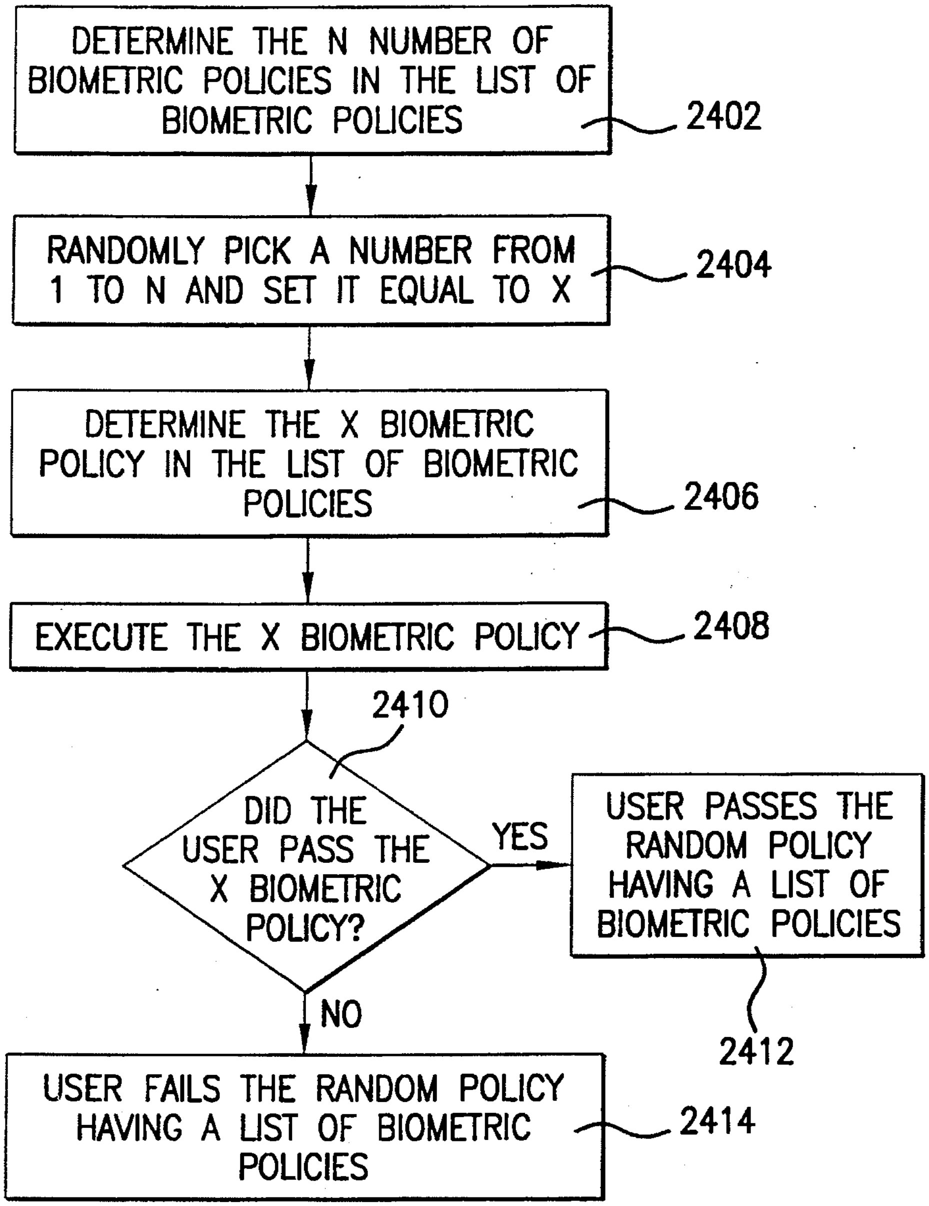
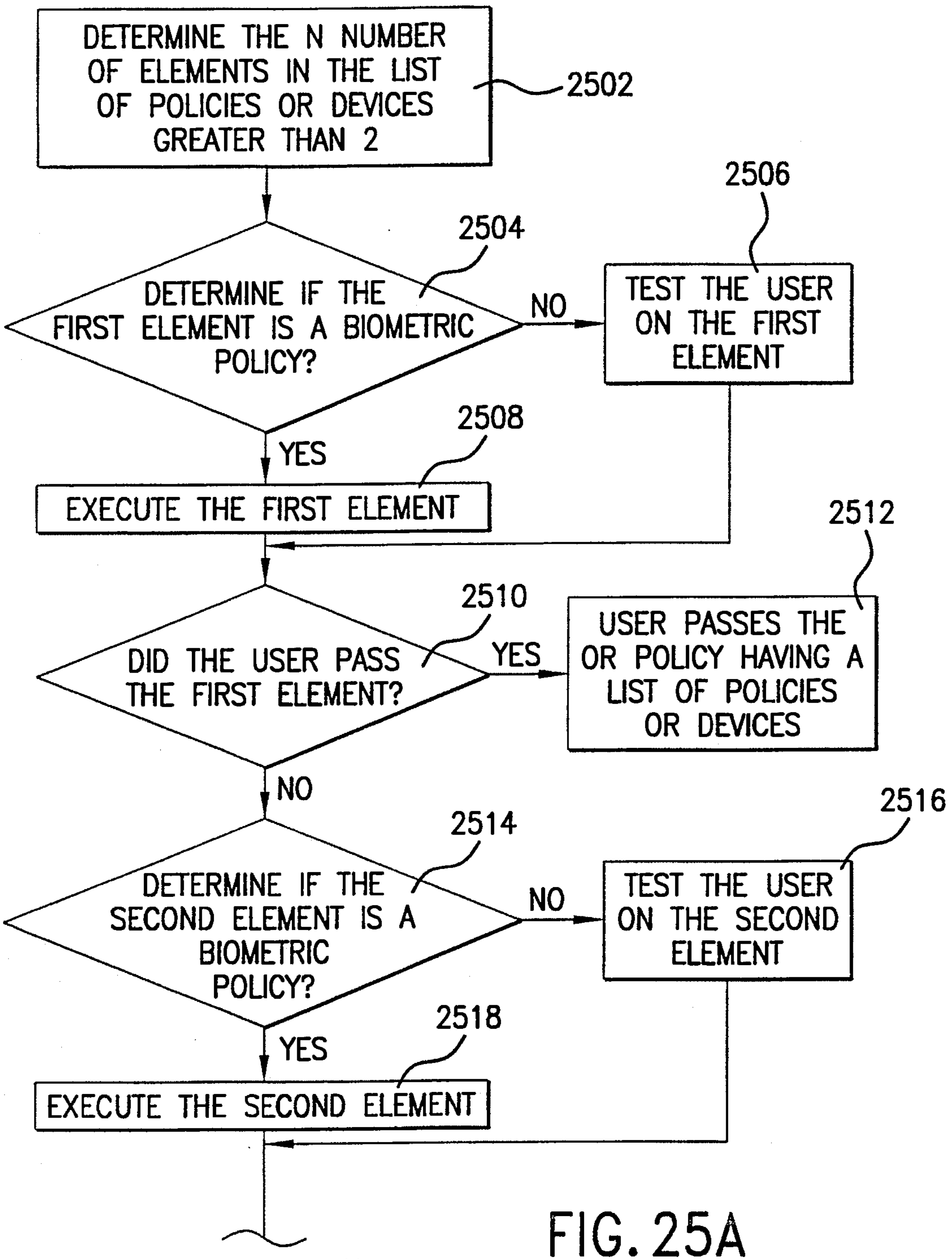

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES
2402
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2404
DETERMINE THE X BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2406
EXECUTE THE X BIOMETRIC POLICY
2408
2410
DID THE USER PASS THE X BIOMETRIC POLICY?
YES
USER PASSES THE RANDOM POLICY HAVING A LIST OF BIOMETRIC POLICIES
2412
NO
USER FAILS THE RANDOM POLICY HAVING A LIST OF BIOMETRIC POLICIES
2414

FIG. 24


DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 2
2502
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
2504
NO
TEST THE USER ON THE FIRST ELEMENT
2506
YES
EXECUTE THE FIRST ELEMENT
2508
DID THE USER PASS THE FIRST ELEMENT?
2510
YES
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
2512
NO
DETERMINE IF THE SECOND ELEMENT IS A BIOMETRIC POLICY?
2514
NO
TEST THE USER ON THE SECOND ELEMENT
2516
YES
EXECUTE THE SECOND ELEMENT
2518

CONTINUED ON FIG.25B

FIG. 25A

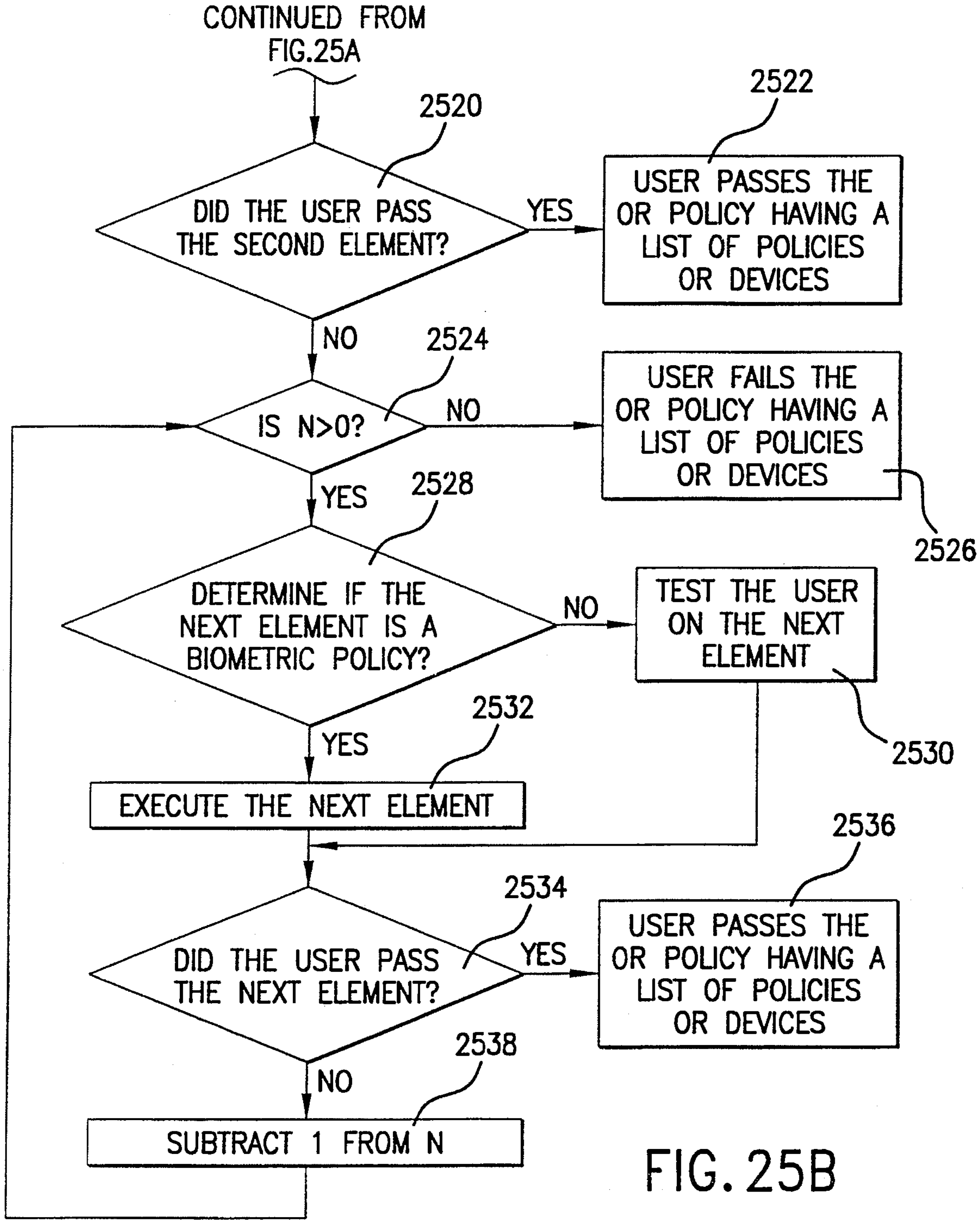

CONTINUED FROM FIG.25A
2520
DID THE USER PASS THE SECOND ELEMENT?
YES
2522
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
2524
IS N>0?
NO
USER FAILS THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
2526
YES
2528
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE NEXT ELEMENT
2530
YES
2532
EXECUTE THE NEXT ELEMENT
2536
2534
DID THE USER PASS THE NEXT ELEMENT?
YES
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
2538
SUBTRACT 1 FROM N

FIG. 25B

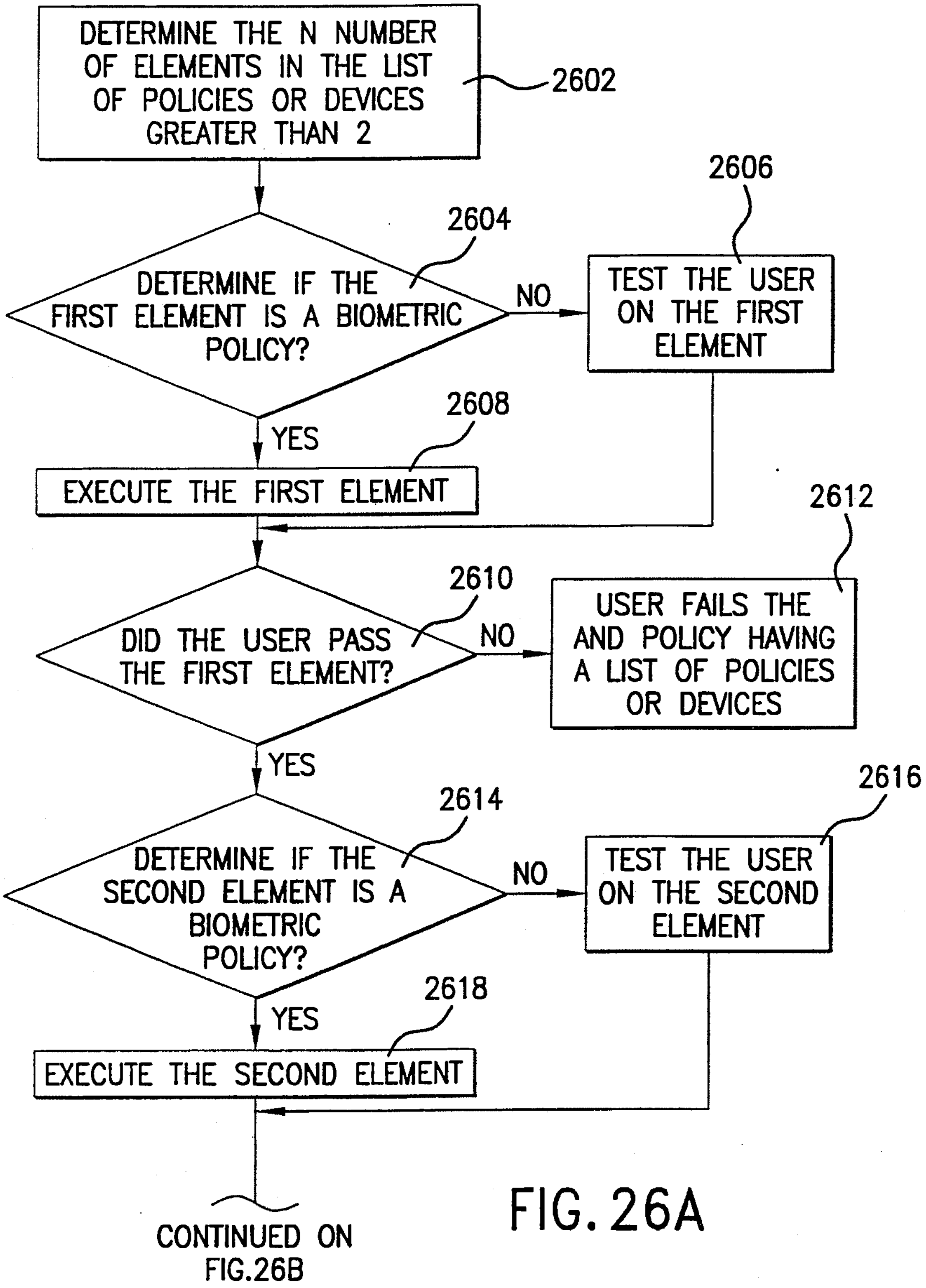

DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 2
2602
2604
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
NO
2606
TEST THE USER ON THE FIRST ELEMENT
YES
2608
EXECUTE THE FIRST ELEMENT
2610
DID THE USER PASS THE FIRST ELEMENT?
NO
2612
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
YES
2614
DETERMINE IF THE SECOND ELEMENT IS A BIOMETRIC POLICY?
NO
2616
TEST THE USER ON THE SECOND ELEMENT
YES
2618
EXECUTE THE SECOND ELEMENT
CONTINUED ON FIG.26B

FIG. 26A

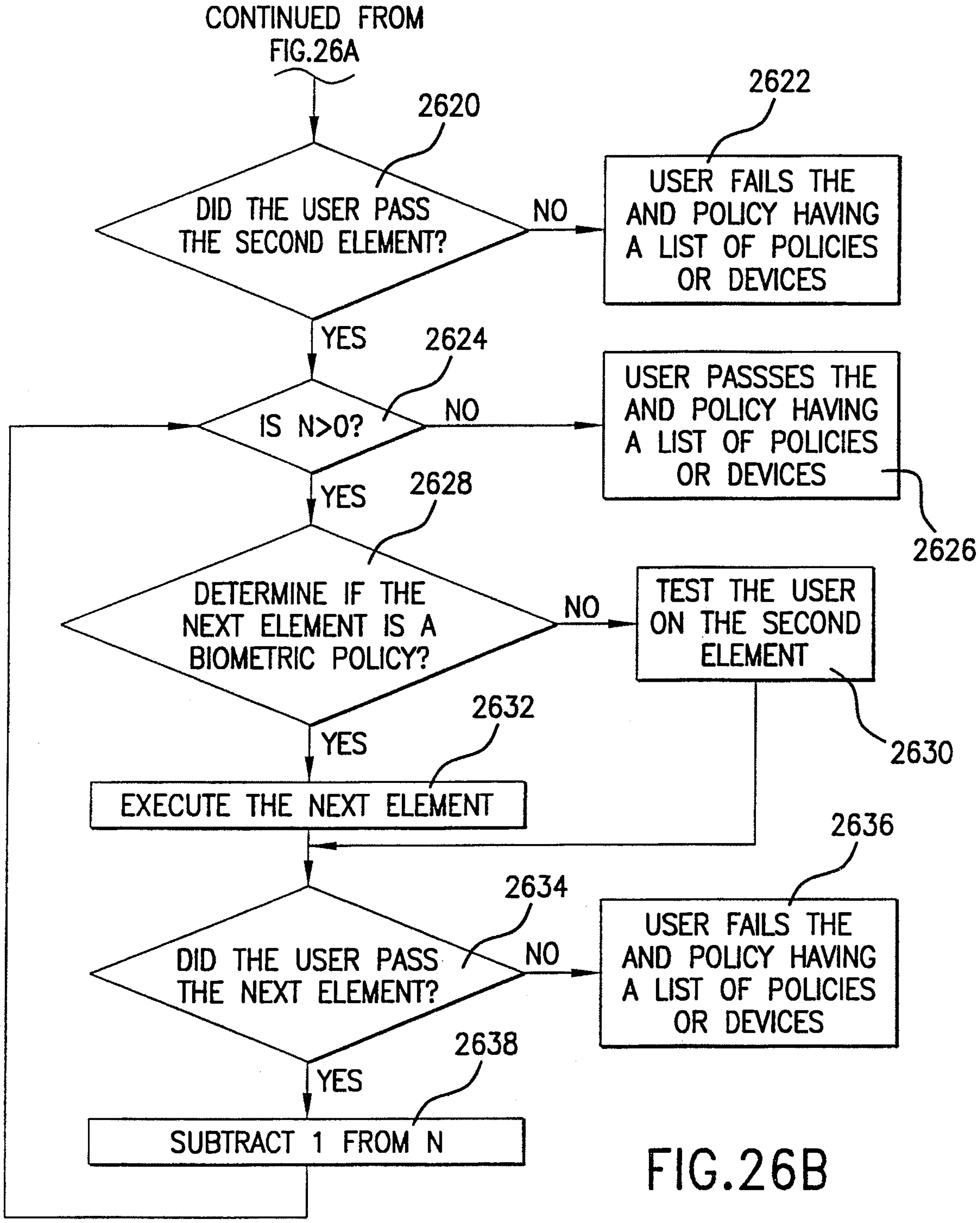

CONTINUED FROM FIG.26A
2620
DID THE USER PASS THE SECOND ELEMENT?
NO
2622
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
YES
2624
IS N>0?
NO
USER PASSSES THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
2626
YES
2628
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE SECOND ELEMENT
2630
YES
2632
EXECUTE THE NEXT ELEMENT
2636
2634
DID THE USER PASS THE NEXT ELEMENT?
NO
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
YES
2638
SUBTRACT 1 FROM N

FIG.26B

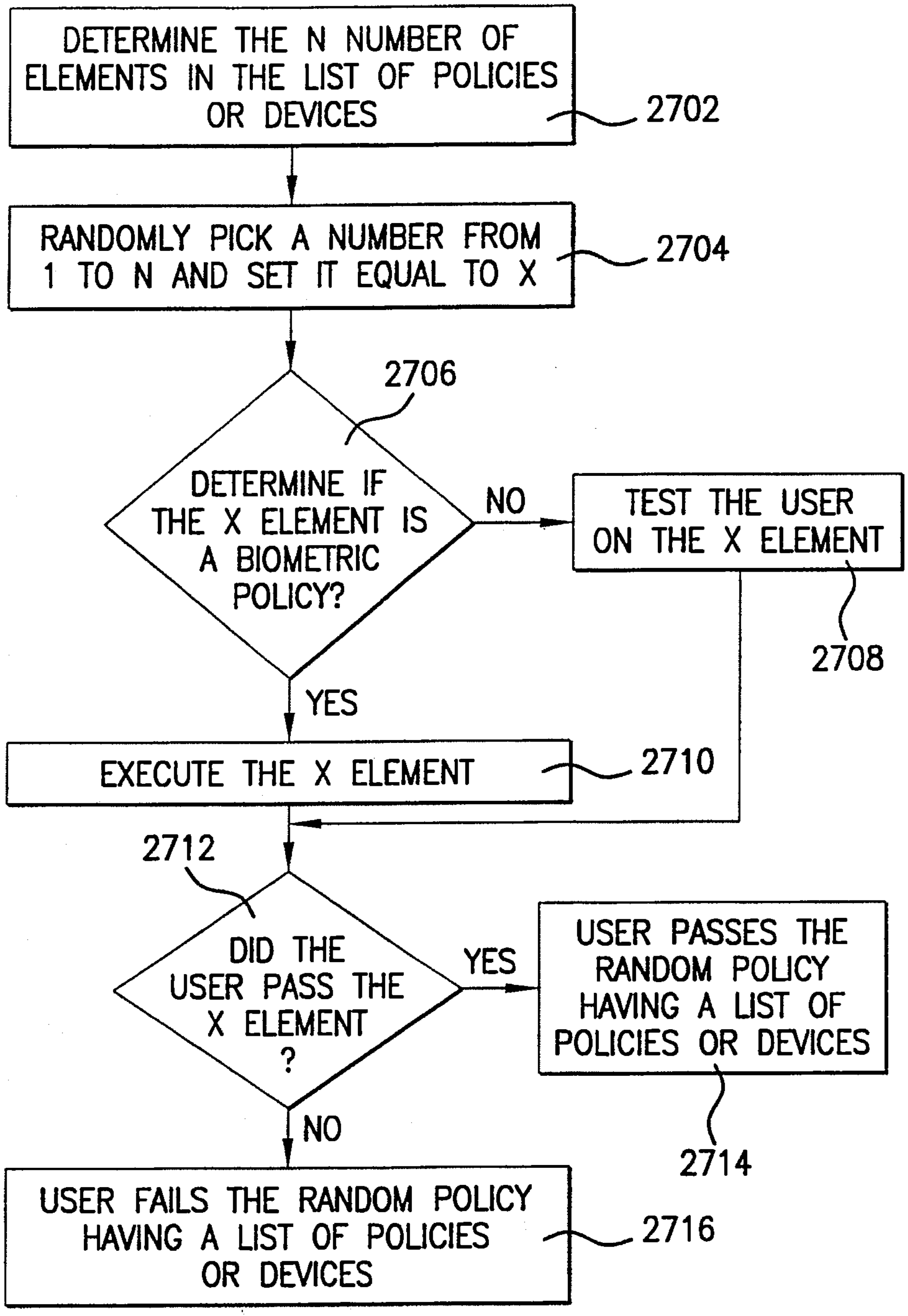

DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES
2702
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2704
2706
DETERMINE IF THE X ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE X ELEMENT
2708
YES
EXECUTE THE X ELEMENT
2710
2712
DID THE USER PASS THE X ELEMENT ?
YES
USER PASSES THE RANDOM POLICY HAVING A LIST OF POLICIES OR DEVICES
2714
NO
USER FAILS THE RANDOM POLICY HAVING A LIST OF POLICIES OR DEVICES
2716

FIG. 27

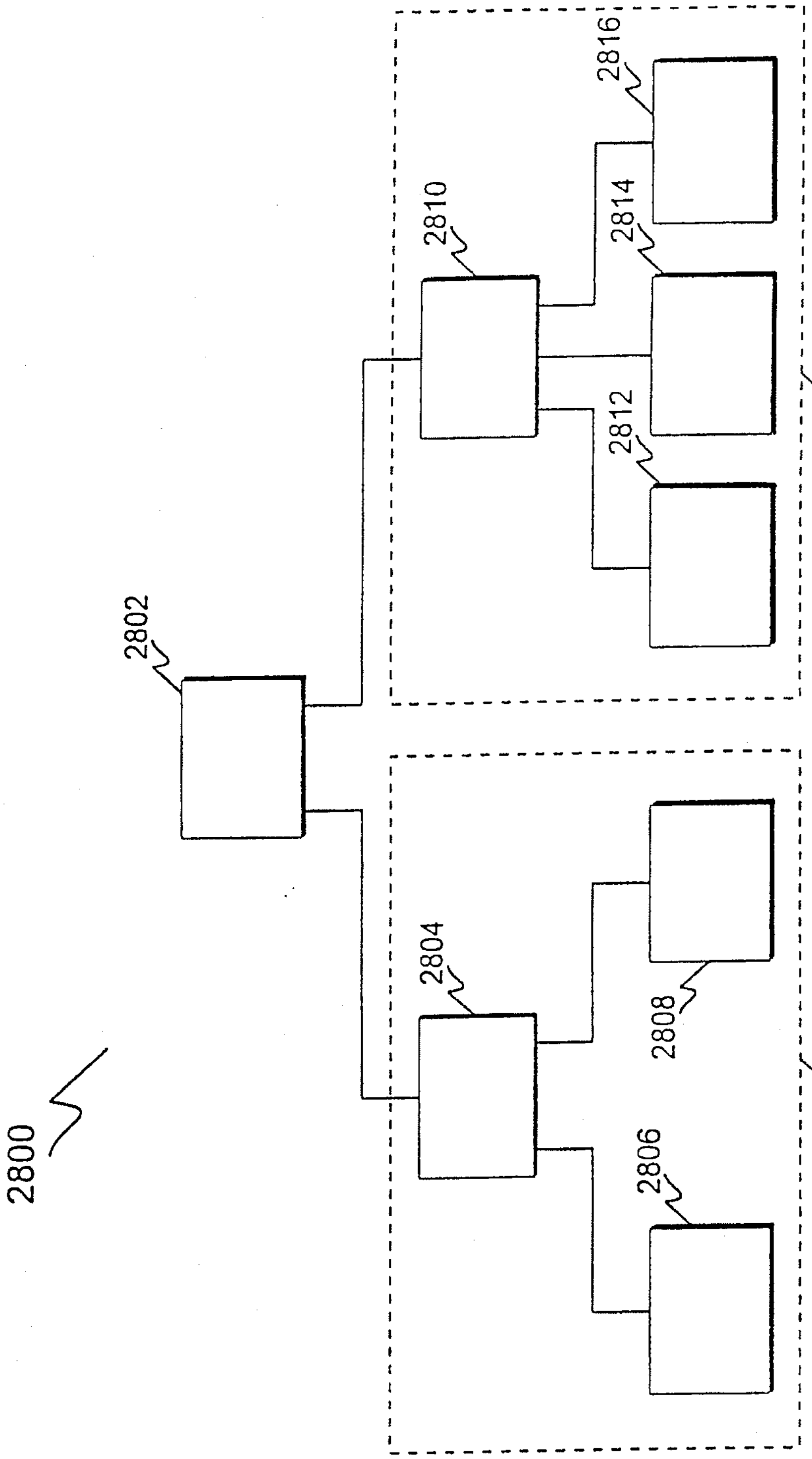


FIG. 28

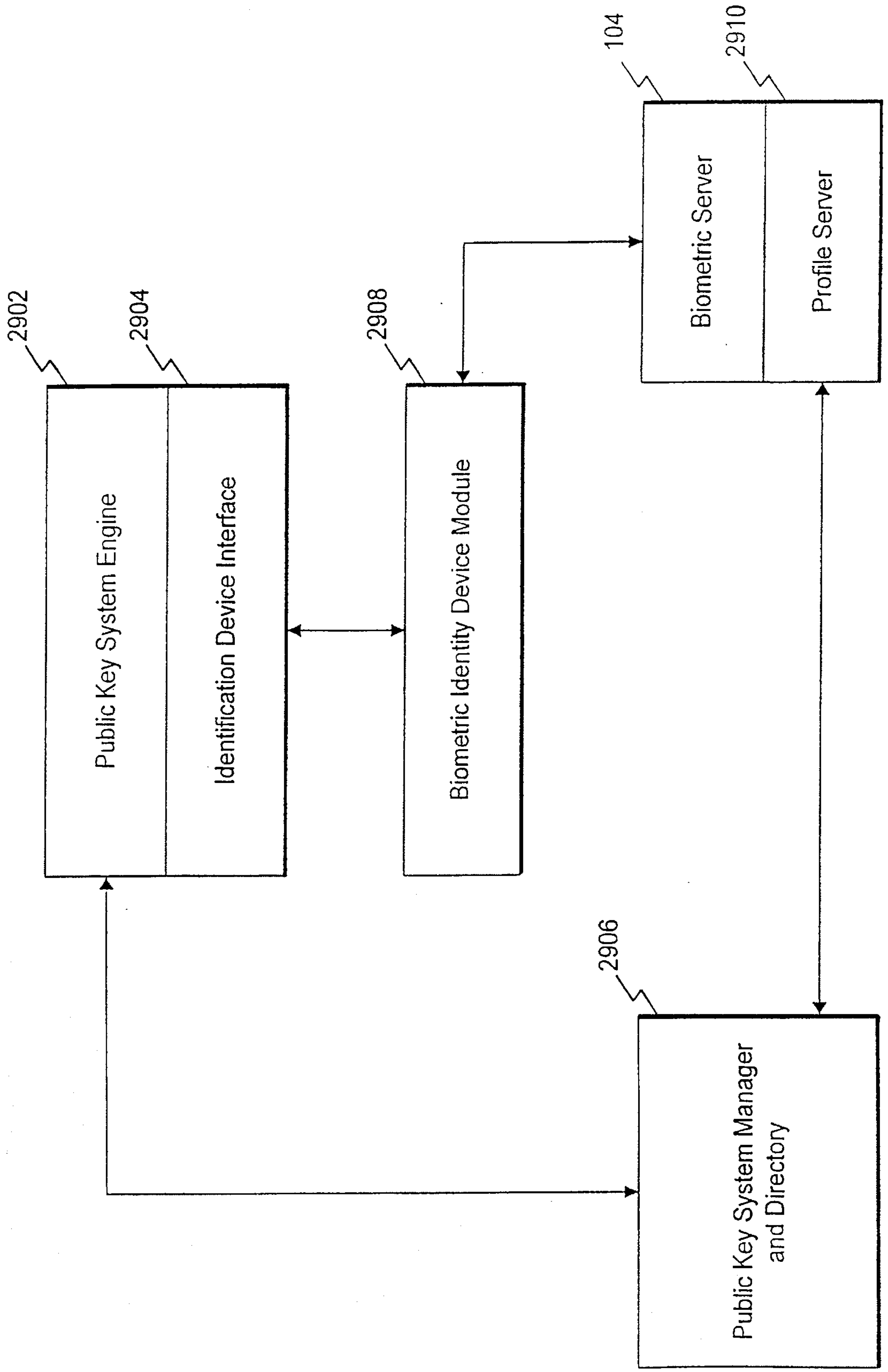

104
2910
Biometric Server
Profile Server
2902
2904
Public Key System Engine
Identification Device Interface
2908
Biometric Identity Device Module
2906
Public Key System Manager and Directory

FIG. 29

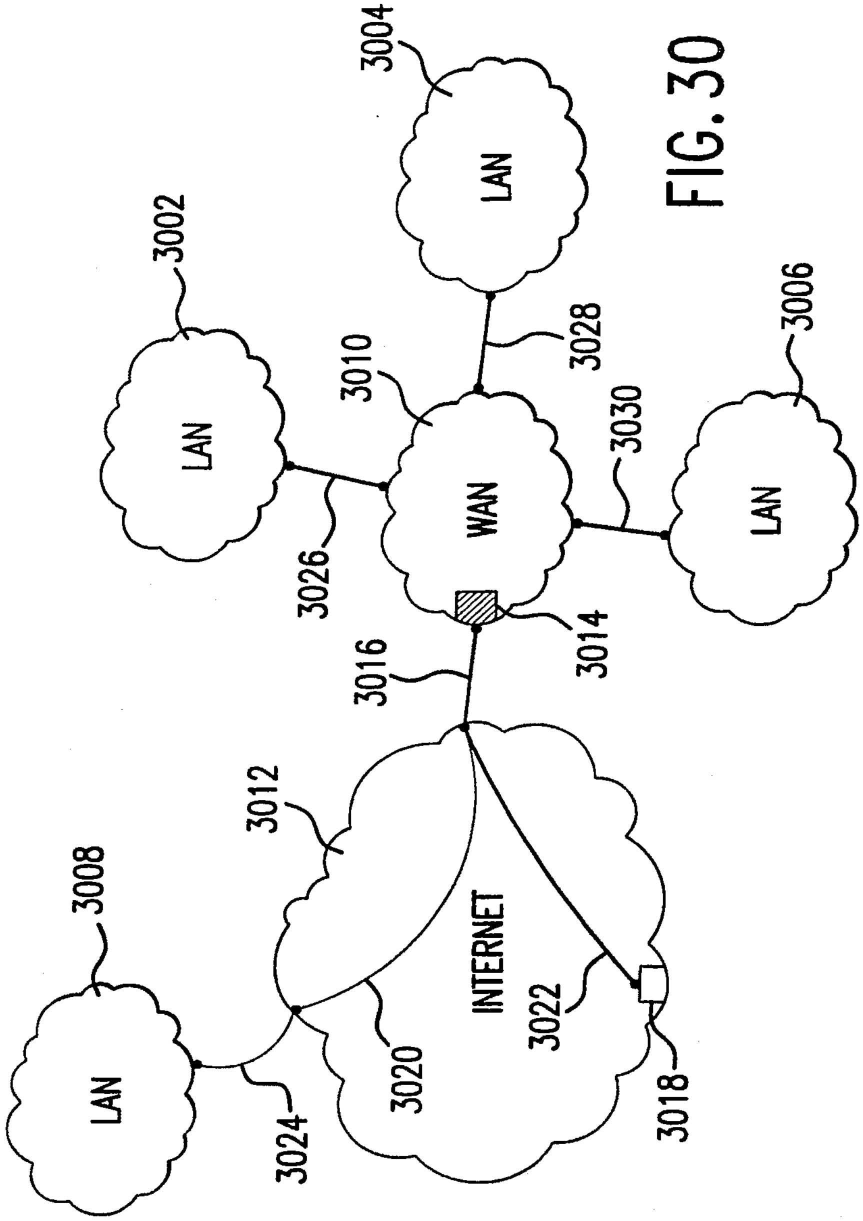

3004
LAN
3002
LAN
3010
WAN
3028
3030
3006
LAN
3026
3014
3016
3012
3008
LAN
INTERNET
3022
3020
3018
3024

FIG. 30

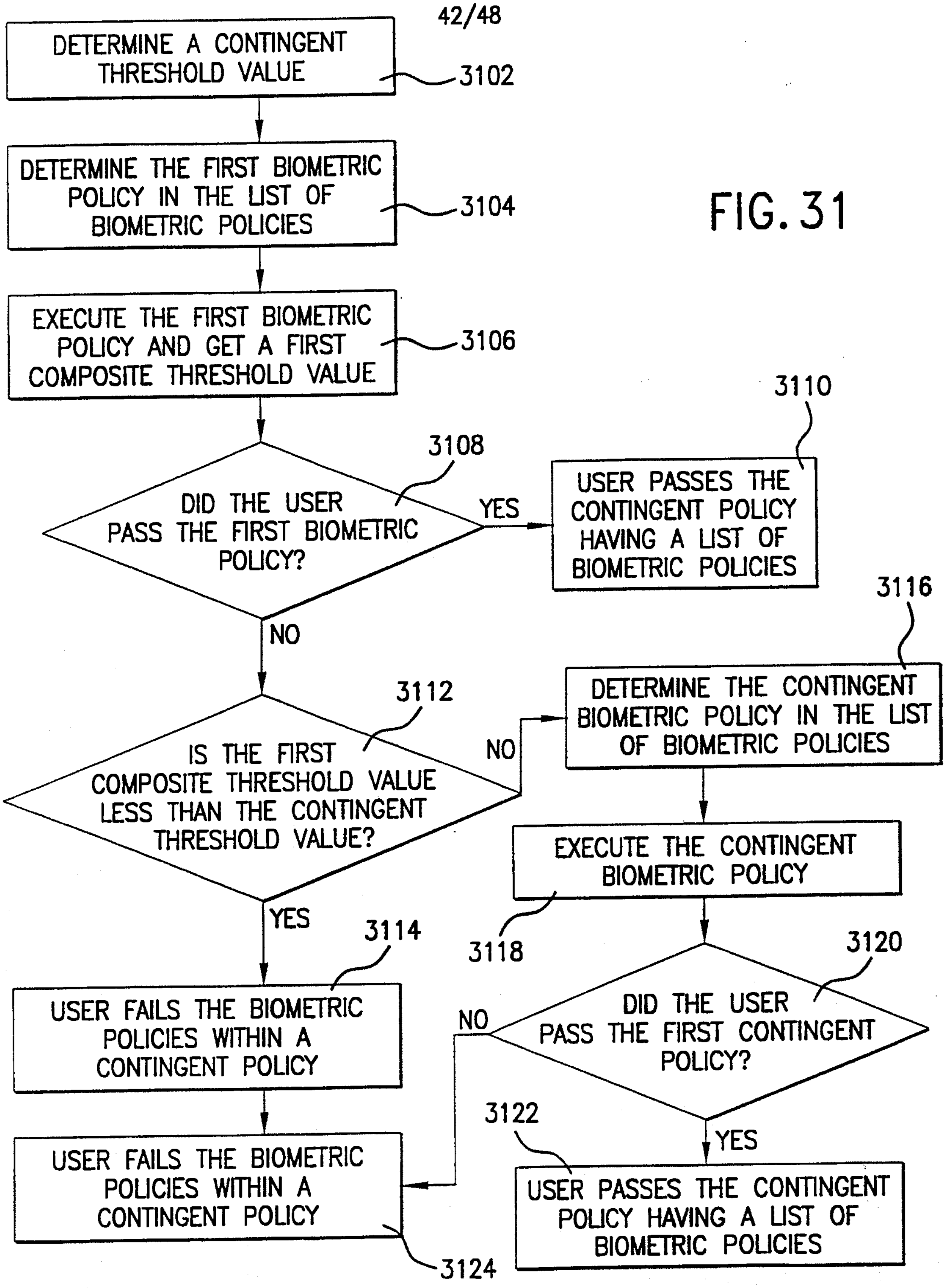

DETERMINE A CONTINGENT THRESHOLD VALUE
3102
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3104
EXECUTE THE FIRST BIOMETRIC POLICY AND GET A FIRST COMPOSITE THRESHOLD VALUE
3106
3108
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
YES
3110
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF BIOMETRIC POLICIES
NO
3112
IS THE FIRST COMPOSITE THRESHOLD VALUE LESS THAN THE CONTINGENT THRESHOLD VALUE?
NO
3116
DETERMINE THE CONTINGENT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
EXECUTE THE CONTINGENT BIOMETRIC POLICY
3118
YES
3114
USER FAILS THE BIOMETRIC POLICIES WITHIN A CONTINGENT POLICY
3120
DID THE USER PASS THE FIRST CONTINGENT POLICY?
NO
YES
3122
USER FAILS THE BIOMETRIC POLICIES WITHIN A CONTINGENT POLICY
3124
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF BIOMETRIC POLICIES

FIG. 31

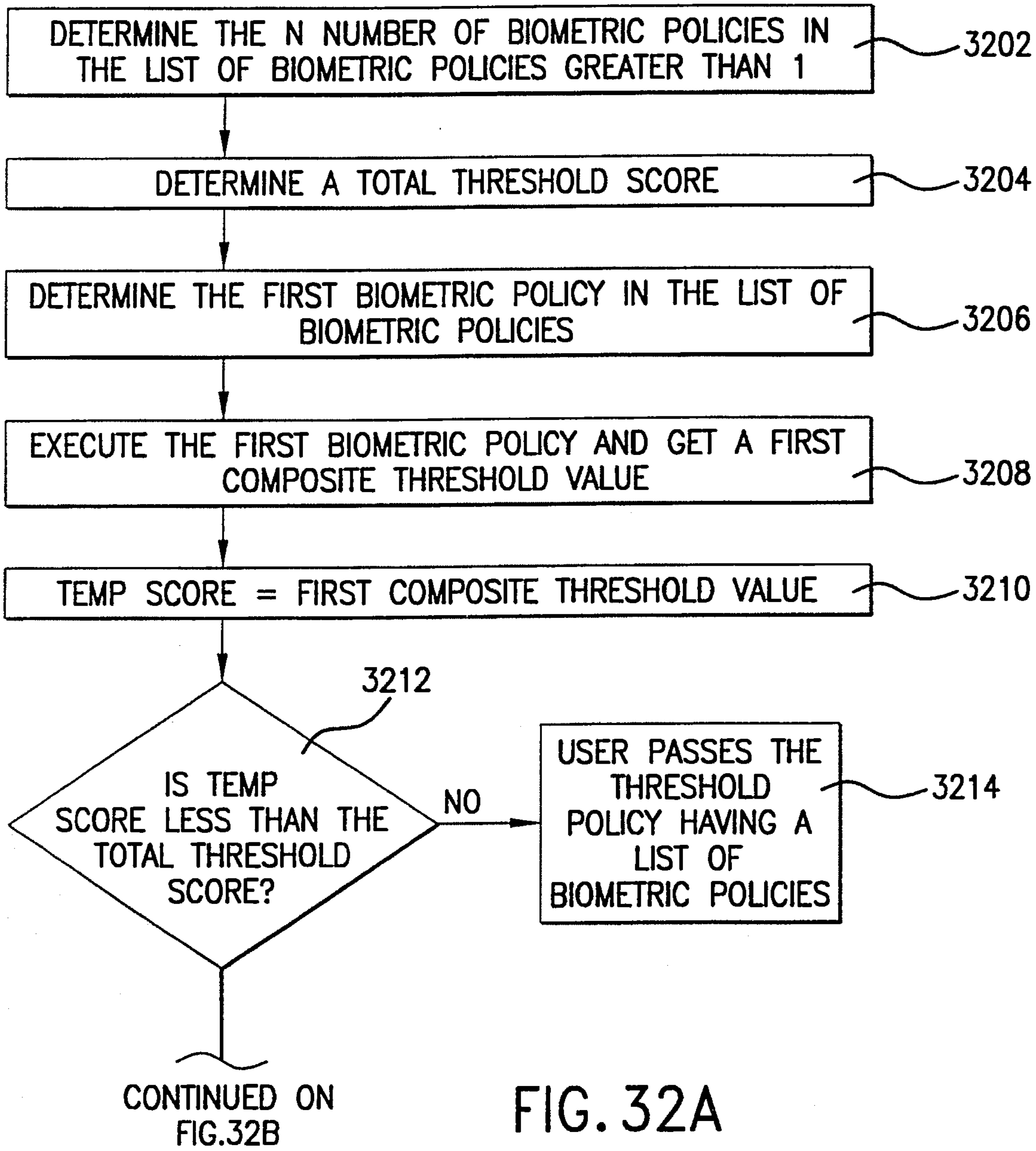

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 1
3202
DETERMINE A TOTAL THRESHOLD SCORE
3204
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3206
EXECUTE THE FIRST BIOMETRIC POLICY AND GET A FIRST COMPOSITE THRESHOLD VALUE
3208
TEMP SCORE = FIRST COMPOSITE THRESHOLD VALUE
3210
3212
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
3214
CONTINUED ON FIG.32B

FIG. 32A

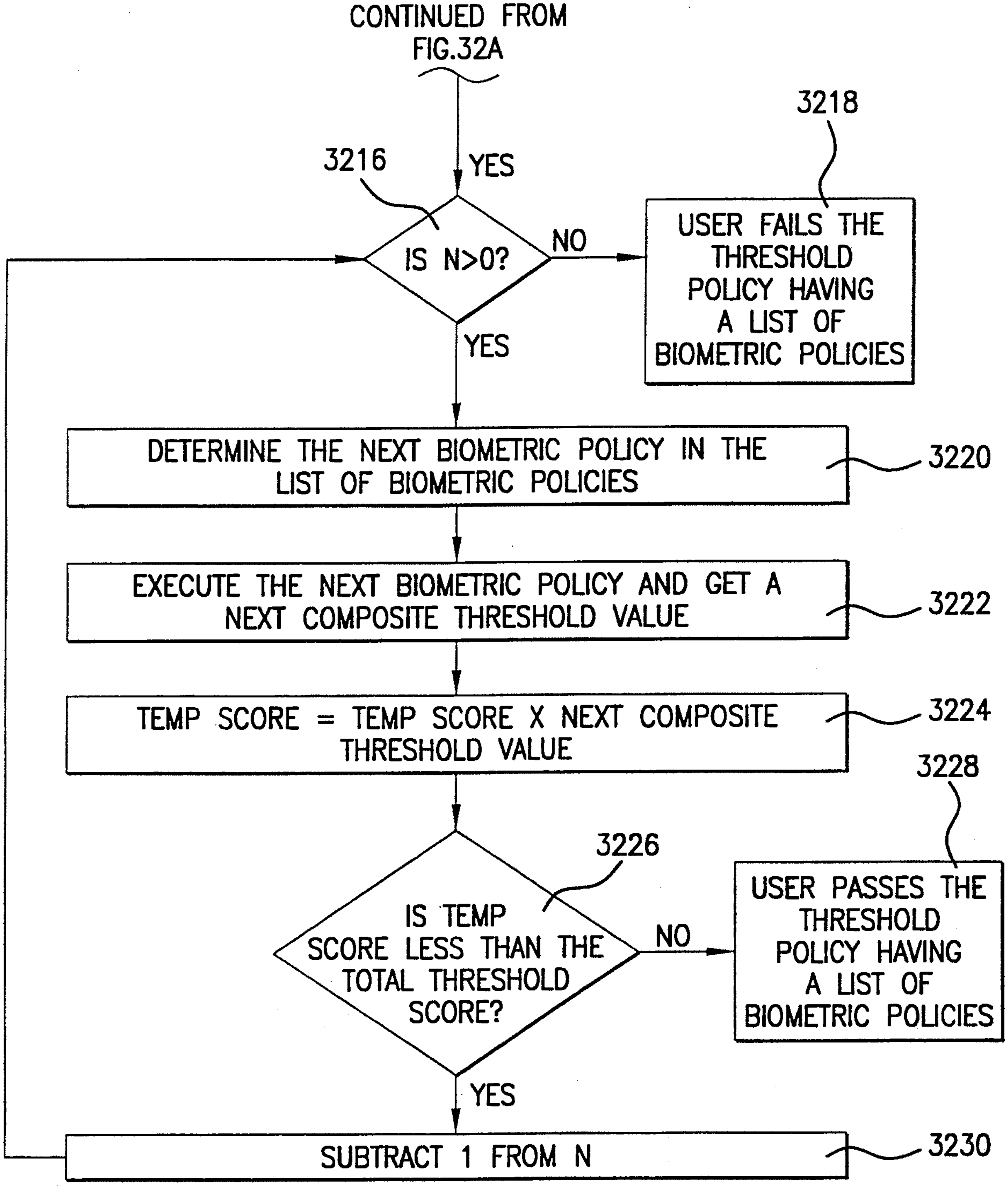

CONTINUED FROM FIG.32A
YES
3216
IS N>0?
NO
3218
USER FAILS THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3220
EXECUTE THE NEXT BIOMETRIC POLICY AND GET A NEXT COMPOSITE THRESHOLD VALUE
3222
TEMP SCORE = TEMP SCORE X NEXT COMPOSITE THRESHOLD VALUE
3224
3228
3226
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
YES
SUBTRACT 1 FROM N
3230

FIG. 32B

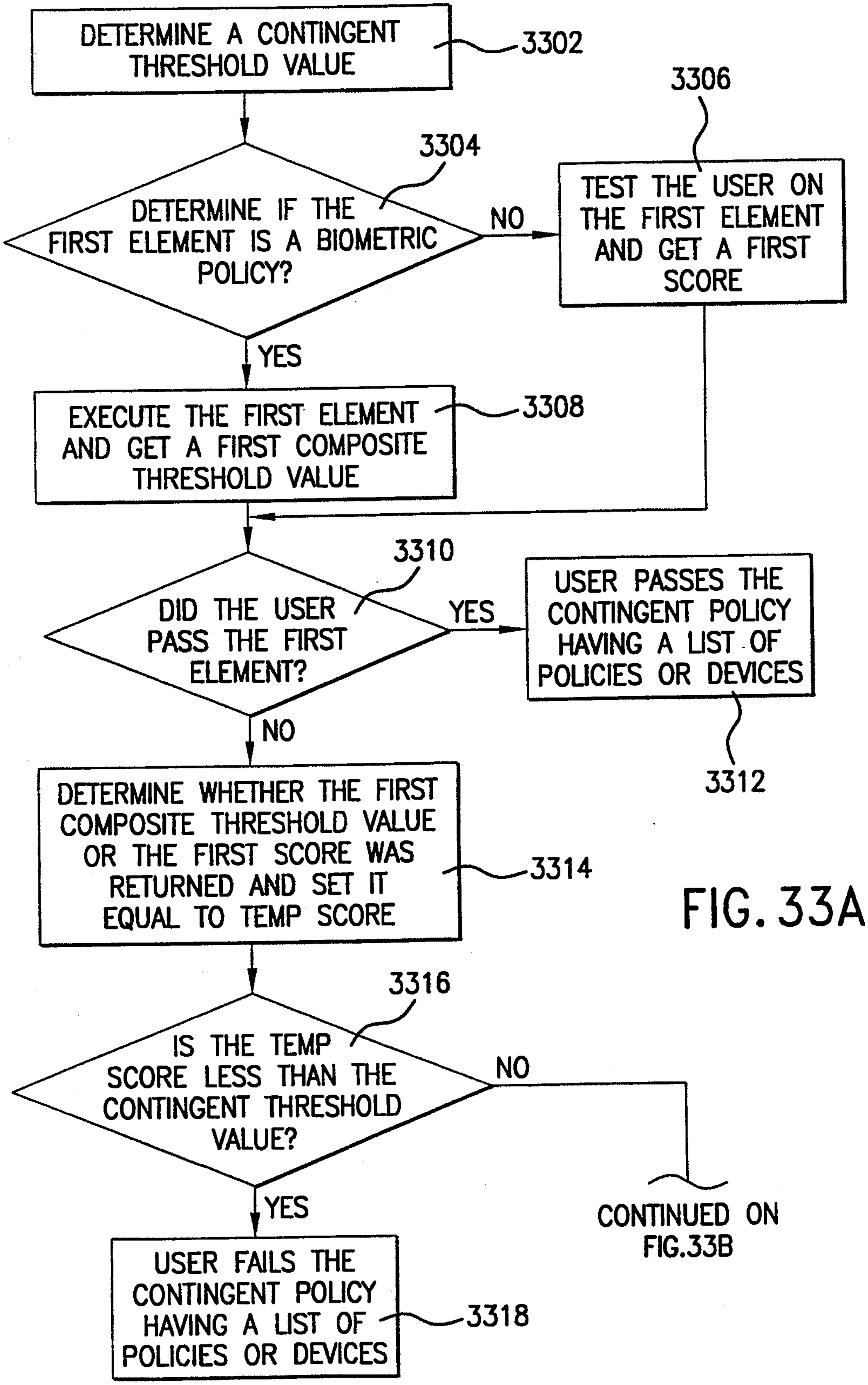

DETERMINE A CONTINGENT THRESHOLD VALUE
3302
3306
3304
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE FIRST ELEMENT AND GET A FIRST SCORE
YES
EXECUTE THE FIRST ELEMENT AND GET A FIRST COMPOSITE THRESHOLD VALUE
3308
3310
DID THE USER PASS THE FIRST ELEMENT?
YES
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
3312
DETERMINE WHETHER THE FIRST COMPOSITE THRESHOLD VALUE OR THE FIRST SCORE WAS RETURNED AND SET IT EQUAL TO TEMP SCORE
3314
3316
IS THE TEMP SCORE LESS THAN THE CONTINGENT THRESHOLD VALUE?
NO
YES
CONTINUED ON FIG.33B
USER FAILS THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
3318

FIG. 33A

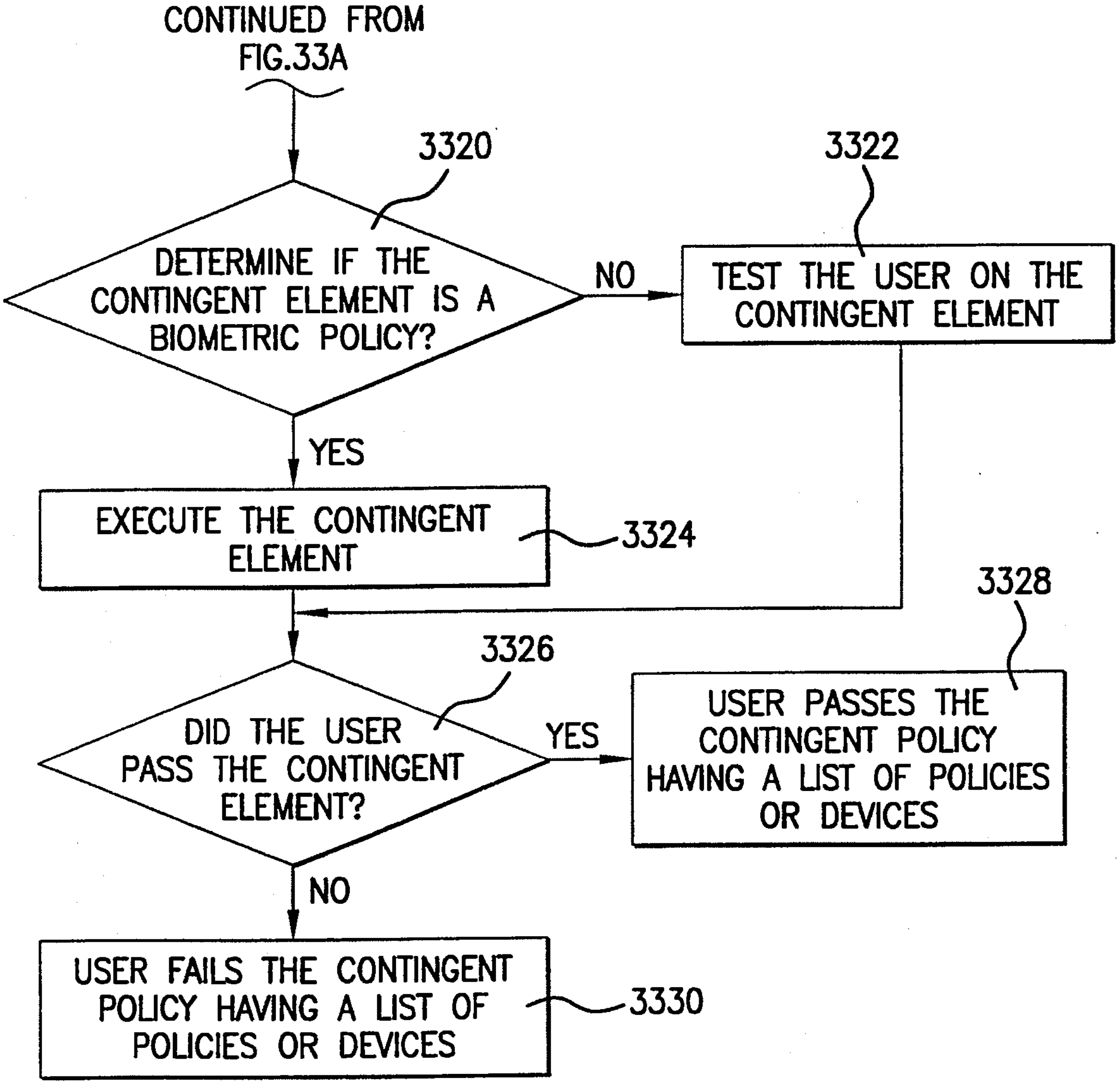

CONTINUED FROM FIG.33A
3320
DETERMINE IF THE CONTINGENT ELEMENT IS A BIOMETRIC POLICY?
NO
3322
TEST THE USER ON THE CONTINGENT ELEMENT
YES
EXECUTE THE CONTINGENT ELEMENT
3324
3328
3326
DID THE USER PASS THE CONTINGENT ELEMENT?
YES
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
USER FAILS THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
3330

FIG. 33B

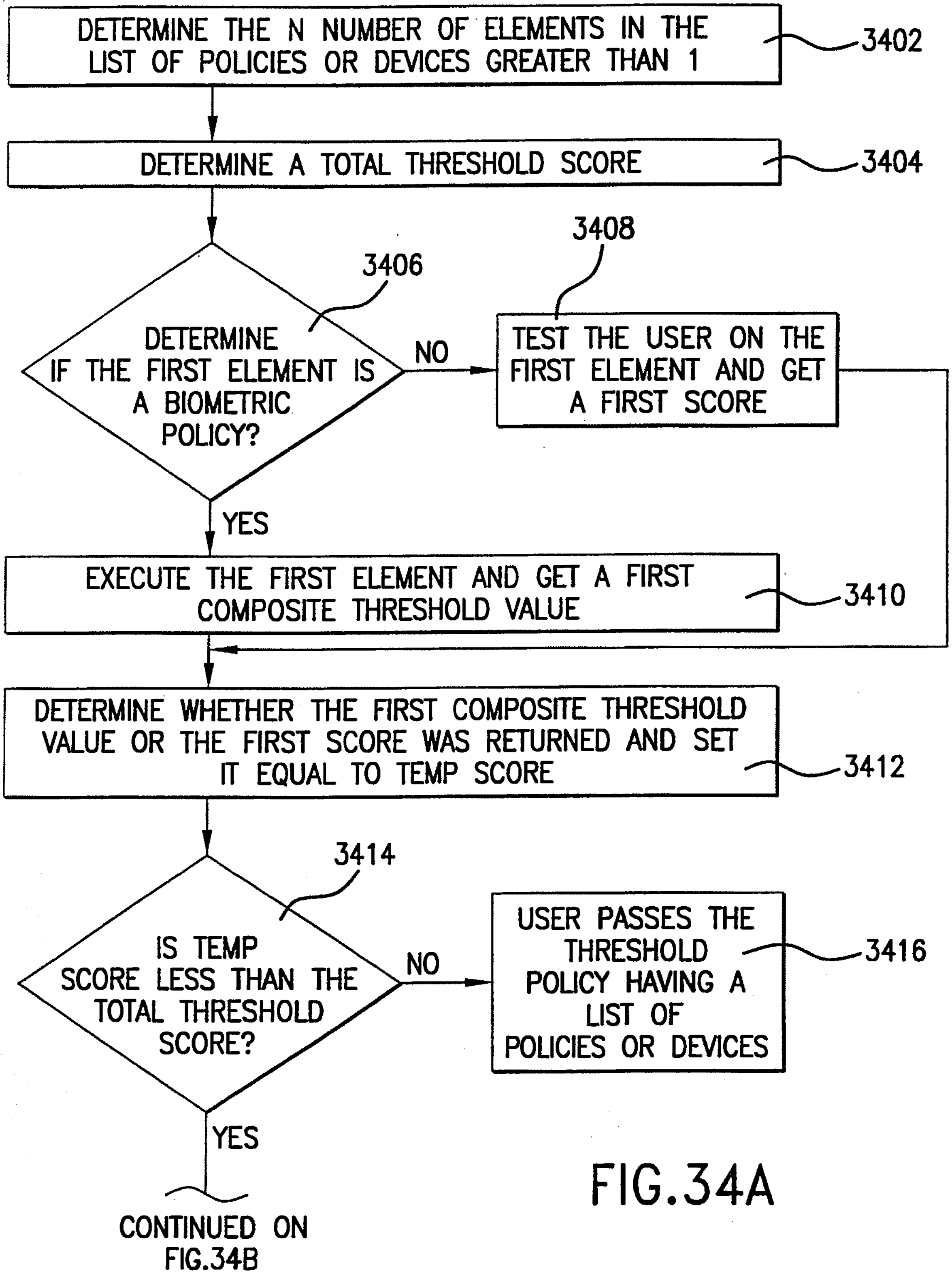

DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 1
3402
DETERMINE A TOTAL THRESHOLD SCORE
3404
3406
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
NO
3408
TEST THE USER ON THE FIRST ELEMENT AND GET A FIRST SCORE
YES
EXECUTE THE FIRST ELEMENT AND GET A FIRST COMPOSITE THRESHOLD VALUE
3410
DETERMINE WHETHER THE FIRST COMPOSITE THRESHOLD VALUE OR THE FIRST SCORE WAS RETURNED AND SET IT EQUAL TO TEMP SCORE
3412
3414
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3416
YES
CONTINUED ON FIG.34B

FIG.34A

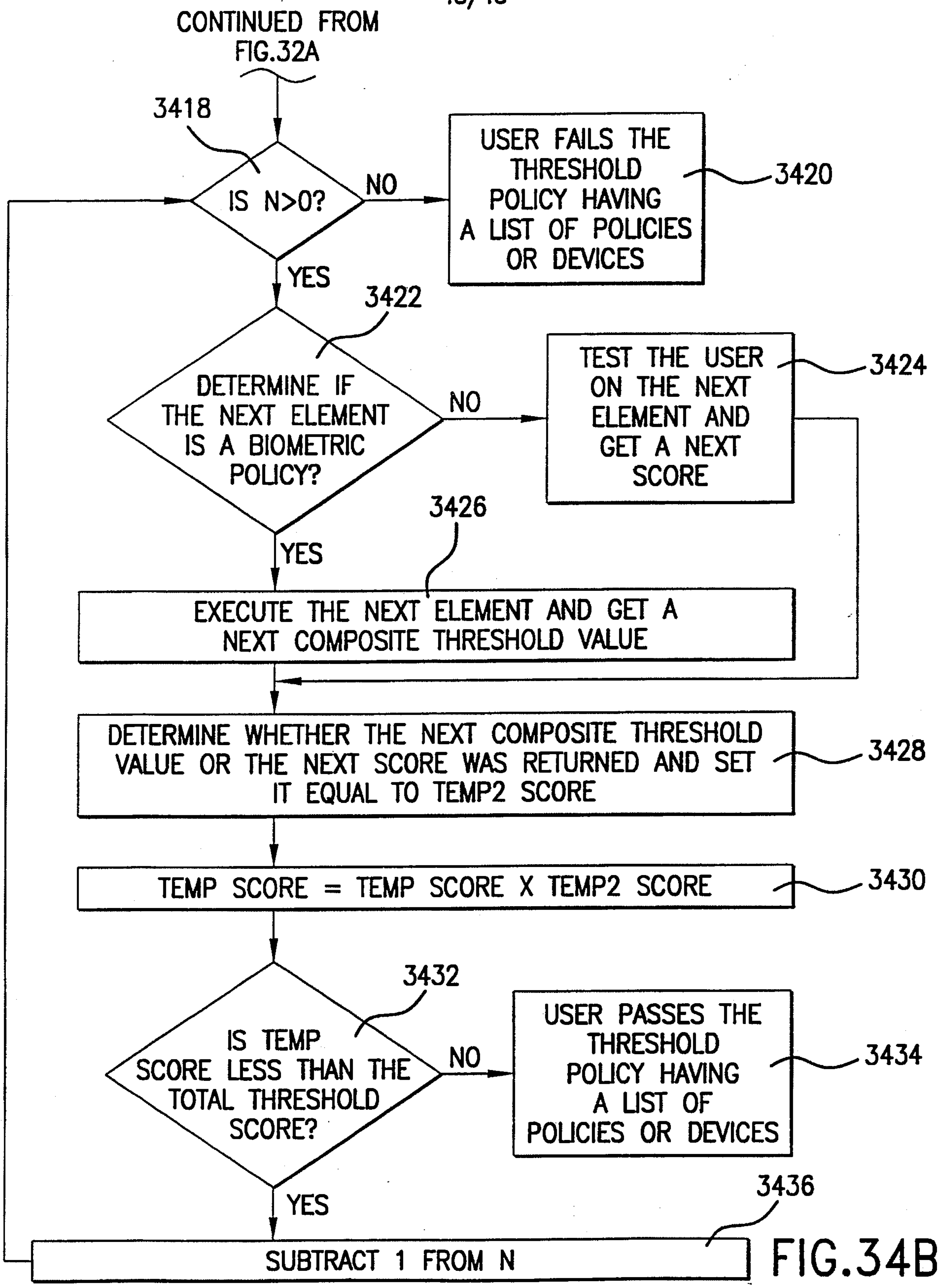

CONTINUED FROM FIG.32A
3418
IS N>0?
NO
USER FAILS THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3420
YES
3422
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE NEXT ELEMENT AND GET A NEXT SCORE
3424
3426
YES
EXECUTE THE NEXT ELEMENT AND GET A NEXT COMPOSITE THRESHOLD VALUE
DETERMINE WHETHER THE NEXT COMPOSITE THRESHOLD VALUE OR THE NEXT SCORE WAS RETURNED AND SET IT EQUAL TO TEMP2 SCORE
3428
TEMP SCORE = TEMP SCORE X TEMP2 SCORE
3430
3432
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3434
YES
3436
SUBTRACT 1 FROM N

FIG.34B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05722

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 9/00
US CL : 713/200, 201, 202, 186; 709/229; 380/3, 4,
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202, 186; 709/229; 380/3, 4,

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

none

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

none

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim N
Y	US 5,615,277 A (HOFFMAN) 25 MARCH 1997, col 1, lines 13-64, col 2, lines 8-38, col 3, lines 1-47.	1-49
Y	US 5,594,806 A (COLBERT) 14 JANUARY 1997, col 1, lines 16-43, col 2, lines 10-54, col 3, lines 28-57, col 4, lines 6-48.	1-49

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 20 APRIL 2000	Date of mailing of the international search report 19 JUN 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BEAUSOLEIL ROBERT W. Jr. Joni Hi Telephone No. (703) 305-3987

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
A63F 9/22, G06F 19/00

A1

(11) International Publication Number: **WO 98/08581**

(43) International Publication Date: 5 March 1998 (05.03.98)

(21) International Application Number: PCT/US97/08072

(22) International Filing Date: 7 May 1997 (07.05.97)

(30) Priority Data:
08/643,827 7 May 1996 (07.05.96) US

(71)(72) Applicant and Inventor: BARCELOU, David, M . [US/US]; 720 New Galena Road, Chalfont, PA 18914 (US).

(74) Agents: SHAMOS, Michael, I. et al.; Webb Ziesenheim Bruening Logsdon Orkin & Hanson, P.C., 700 Koppers Building, 436 Seventh Avenue, Pittsburgh, PA 15219-1818 (US).

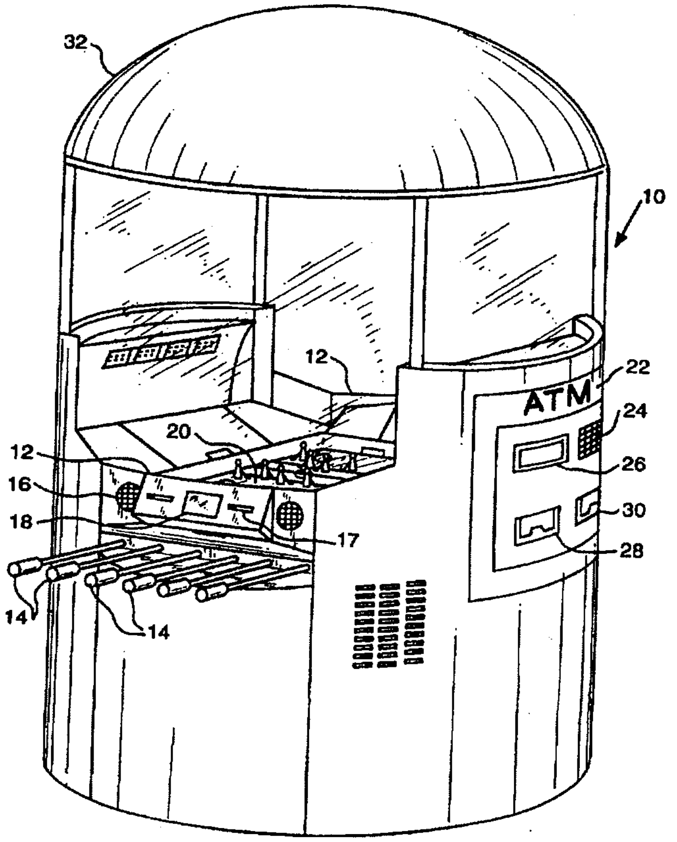
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AUTOMATED LEAGUE AND TOURNAMENT DEVICE

(57) Abstract

A sport or skill game device in which equipment (22) for accepting and dispensing currency, preferably of more than one type (both actual cash and encoded credit, for example), is provided in close proximity with and in electronic connection to one or more of any of a number of sport or skill game devices (14, 20) for play by two or more players. The device contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among two or more entrants whose entry fees and currency pay outs (to the winners) are tendered and distributed as part of the overall operation of the device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

AUTOMATED LEAGUE AND TOURNAMENT DEVICE

Field of the Invention

The invention adapts multiple aspects of entertainment technology and other technologies to sport and skill games and/or devices.

Background of the Invention

Entertainment technology has evolved beyond recognition in a mere ten or fifteen years. New motion pictures are released into complicated and ever more calculated schemes of sequential availability to commercial theaters, rental operations and home theaters--the latter of which can bear startling resemblance to the former. Audio recordings known as "enhanced CDS" offer not only audio but multimedia video replication, and personal computers and televisions and their networks are individually evolving so that soon they may well be virtually indistinguishable. A wide array of online information and interaction tempts us, moreover, from opportunities as unsophisticated as the online equivalent of a group of teenagers sharing a party telephone line to those inherent in ineffable data banks pertaining to satellite photography, medicine and genetic engineering, just to name a few.

Beneath the most enhanced entertainment technology lies a troubling and largely unrecognized assumption, however. With some but minor exceptions, cutting edge entertainment technology is predicated upon the belief that its consumers prefer a largely passive role while the technological dazzle occupies the stage. Multimedia CD jukeboxes are a good example of this phenomenon--a pub or restaurant in which such a machine is installed is overtaken by a genial Wizard of Oz in which social activities, other than the tendering of adequate currency to the welcome sorcerer, take on secondary importance.

This is not to say that the entertainment industry requires passive participation--quite the contrary--just that the concomitant technology generally does. For example, the Karaoke machine in which prerecorded (or sequenced) orchestrations may be augmented by live vocals is at this writing barely taken seriously as an embodiment of entertainment technology, and customarily it is subjected to lighthearted scorn. Even with the newest theme park amusements the "ride" is generally passive. "Hot buttons" on click screens or touchscreens in multimedia interactive applications never seem to deliver the promised autonomy and volition with which such systems entice new users. On the other hand, where true active entertainment participation is maximized the technology tends to be minimal at this writing, such as is evident from the undying popularity of traditional pool or pinball competitions, or in electronic darts and their leagues, or old fashioned amusement park autobahns where the driver can actually (heavens!) steer the car. Consumers of up-to-the-minute elaborate entertainment technology are not today supposed to impose themselves too visibly, or too actively, into the mechanations of their experience.

Quite apart from the entertainment technology industries, sport and skill game leagues of all kinds are gaining in popularity in various settings. The aforementioned electronic darts leagues are immensely popular across a wide socioeconomic spectrum, and other games of skill organized into fee-for-entry leagues include but are not limited to chess, bowling, pool, miniature soccer, miniature hockey, and pinball and video games of skill. These leagues are operated separately from legal and less-than-legal gambling channels, such as those having to do with video poker, because the leagues sponsor games of skill only and proceeds are thus not distributed on the basis of chance. These leagues tend to be surprisingly conventional in their organization, solicitation, seasonal entry, execution and end-of season payout, possibly because the same individuals who value active participation in their leisure pursuits likewise tend to take an active role in the hands-on administration of traditionally organized amusement game and sports leagues.

Accordingly, a need remains for an improvement in entertainment technology in which some or all aspects of that technology, as well as other technologies, are redesigned directly to embrace participatory activities such as those of a sport or skill game league rather than merely the passive participation typical of entertainment technology heretofore.

Summary of the Invention

In order to meet this need, the present invention is a sport or skill game device in which an amalgam of various technologies cooperate to facilitate an active sport or skill game between two players or among three or more players, usually organized into leagues. The device necessarily includes equipment for accepting and dispensing currency, preferably of more than one type (both actual cash and digital cash in the form of encodable credit, for example), in close proximity with and in electronic connection to one or more of any of a number of sport or skill game devices such as may be used for electronic darts, minature hockey, chess, miniature bowling, pinball, video games of skill or virtually any other game of skill in either full sized or miniaturized versions. Preferably, the device includes multimedia enhancements such as controllably cheering crowds and context specific video displays. Moreover, the device necessarily contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among 2 or more entrants whose entry fees and currency payouts (to the winners) are tendered and distributed as part of the overall operation of the device.

The device may occupy a single location, with equipment to allow play by two or more players, or may embody a network of individual game kiosks under centralized control. The device may offer additional optional services including, but not limited to, jukebox activation, full automated teller function, vending of various retail goods and services such as mail order catalogue purchases, sporting and cultural event tickets, cruise or airline tickets, dating services, stock trading or other investment services or even direct vending of foods, beverages, publications, esoterica, etc.

Brief Description of the Drawings

Figure 1 is a perspective view of a first embodiment of the invention;

Figures 2a and 2b are schematic diagrams showing the elements of the first embodiment and a second embodiment of the invention;

Figure 3 is a schematic diagram of a third embodiment of the invention;

Figure 4 is a side elevational view of a control panel according to a fourth embodiment of the invention;

Figure 5 is a side elevational view of the same mechanics as shown in Figure 4, but with the control panel removed;

Figure 6 is a plan view of the game playing field shown in Figure 1;

Figure 7 is a schematic diagram of a fifth embodiment of the invention; and

Figure 8 is a schematic diagram of a sixth embodiment of the invention.

Detailed Description of the Invention

The present invention is a sport or skill game device in which an amalgam of various technologies cooperate to solicit, to organize and to administer an active sport or skill game between two players or among three or more players, with larger numbers usually being organized into leagues. The device may occupy a single location, with equipment to allow play by two or more players, or may embody a network of individual games under centralized control.

The inventive sports league device necessarily includes equipment for accepting and dispensing currency, preferably of more than one type (both actual cash and at least one form of digital currency such as encodable credit, for example), in close proximity with and in electronic connection to any of a number of sport or skill game devices such as may be used for electronic darts, miniature hockey, chess, miniature bowling, pinball, video games of skill or virtually any other game of skill in either full sized or miniaturized versions. Preferably, the device includes multimedia enhancements such as controllably cheering crowds and pertinent video displays. Moreover, the device necessarily contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among two or more entrants whose entry fees and currency payouts (to the winners) are tendered and distributed as part of the overall operation of the device.

The device may offer additional optional services including, but not limited to, jukebox activation, full automated teller function, direct vending of foods, beverages, publications and other retail items or remote vending of various retail goods and services such as mail order catalogue purchases or restaurant take-out orders, online service access, sporting and cultural event tickets, cruise or airline tickets, telephone or other smart card encoding, dating services, stock trading or other investment or banking services, health assessment and treatment services, pharmacy services including drug interaction databases, government benefits administration such as food stamps or Medicaid, or insurance brokerage. Other services are limited only by the imagination.

By convention throughout this specification, the "device" refers to the sport or skill game system as a whole, notwithstanding the varying nature of the device as an individual kiosk, such as is shown in Figure 1, or local area networks or wide area networks for multiple station league play with or without the additional functions of retail kiosks for direct or remote vending. The invention and the device, for the purposes of this specification, are thus synonymous.

The present device is used to solicit, to enroll, to govern play and to pay the winner of any one or more of a number of games of skill. A description of the details of how to govern games between two people or league tournament competitions is largely omitted here, because the underlying administrative procedures are both well known and variable regarding aspects such as entry fees, playoff progression and other aspects of tournament administration. However, the present device preferably includes equipment to allow for one or more of the following entertainment technology enhancements to tournament play, including but not limited to:

a) sound and/or motion sensors to initiate attract mode displays on device video display(s) and from audio speakers;

b) audio as well as video instructions and menus;

c) game command interactive touchscreen which also commands selective cheers or taunts from built in speakers, or the national anthem at the start of play, or other light or sound enhancements of game play;

d) juke box provision with operation both independent of and/or interrelated to game play;

e) portrait camera(s) for encoding digital portraits inserted either on players' individual smart cards or as a means of access to a pictorial database;

f) real time video telephone and/or video broadcasting connections between and among local or wide area players or other video networks; printouts of discount coupons, award certificates, player statistics and/or game or tournament results and/or coming tournaments and attractions and schedules.

Enhancements beyond entertainment technology per se have already been listed and include ticket services, dating services, etc. as options. However, the following list helps to illustrate the wide variety of services which can be included: E-M Games of Skill Services; Smart Card Services; Insurance Services; Restaurant Services; Travel Services; Sports Services; Gaming Device Services; Delivery Services; Coupon Services; Introduction Services; Audio Services; News Services; Transportation Services; Utility Services; Physician Services; School Services; Security Services; Building Services; Credit Services; Directory Services; Home Services; Military Services; Personal Services; Automotive Services; Employment Services; Recreational Services; Travelers Check Services; Kids Services; Videogames of Skill Services; Internet Services; Brokerage Services; Government Services; Entertainment Services; Library Services; Catalog Services; Print Services; Diagnostic Services; Chat Services; Video Services; Database Services; Barter Services; Engineering Services; Pharmacy Services; Identification Services; Detective Services; Church Services; Loan Services; Training Services; Buying Services; Recruitment Services; Accounting Services; Photographic Services; Food Services; Radio Services; Credit Services; Theme Park Services; Music Services; Financial Services; Full-line Vending Services; Health Care Services; Remote Access Services; Payment Services; Computer Services; Search Services; Network Services; Subscription Services; Virtual Reality Services; Advertising Services; Rental Services; Programming Services; Beverage Services; Credit/Debit Card Services; Freight Services; Stored Value Card Services; Beauty

Services; Tax Services; Leasing Services; Medical Services; Emergency Services; Publishing Services; Counseling Services; Satellite Services; Screening Services; Real Estate Services; Telephone Services; Ticket Services; Television Services; Dating Services; Information Services; Lottery Services; Software Services; Reservation Services; Communication Services; Intranet Services; Adult Services; Referral Services; Repair Services; Legal Services; Consulting Services; Maintenance Services; Moving Services; Trade Show Services; Design Services; Lodging Services; Mail Services; Fast Food Services; Automated Services; Recording Services; Clothing Services; Wireless Services; Human Services; and Encryption Services.

In a manner similar to the known nature of the league administrative organization, software systems capable of coordinating the combined functions of the present invention are within the skill of the art and do not form a central part of the invention, nor actually do specific video displays and interactive protocols associated therewith (apart from independent proprietary design). For example, the Remote Procedure Call (RPC) model is an industry wide, well tested technology enabling the design and implementation of distributed applications such as the multi-vendor interoperability intrinsic to the present device. The RPC service enables the local game or sport player to invoke a remote procedure as if it were local to the calling process (a remote procedure is a procedure located in an address space separate from the calling code). Ordinarily, the present device will be coordinated according to the RPC model, generally using TCP/IP support protocol computerized systems and known smart card encoding/decoding, database, directory, currency transfer, alternative error recovery and security systems in Local Area Network (LAN), frequently in conjunction with Wide Area Network (WAN), configurations. The invention inheres in the novel interactive combination of several separate technologies as described above, and not in the specifics of the man-machine interface protocols which govern either individual transactions or the overall device.

The above generalized disclosure of the invention is illustrated further by means of the six embodiments specifically illustrated in Figures 1-8, which embodiments are not exhaustive of the various ways the present invention may be implemented.

Referring now to Figure 1, a kiosk 10 is shown in perspective in which two play stations 12 are fitted with play controls 14, a smart card reader/encoder 16, a credit card reader 17, and a video command touchscreen 18. Play controls 14 govern play on a playing field 20 (the playing field itself is shown in greater detail in Figure 6, below), and scoring is automatically calculated and communicated to a computerized control (not shown) interior to and/or exterior to the kiosk 10. The computerized control connects directly to the smart card reader/encoder 16, the credit card reader 17 and the video command screen 18. On a side of the kiosk 10 generally normal to the two play stations 12, an automated teller machine (ATM) 22 includes typical ATM hardware including a card reader (not shown), keyboard 24, instruction screen 26, bill dispenser 28 and receipt dispenser 30. The playing field 20 is covered by and protected by a penetration resistant dome 32 and a standard ATM/bank security camera 31.

In operation, the kiosk of Figure 1 contains all the hardware necessary to enable a player to stand in front of the play station 12, to place a credit card in the credit card reader 17, and to vend or to add value to a smart card (not shown) via the video command touchscreen and the smart card reader/encoder 16. By continuing to use the video command touchscreen, the player may initiate play of a game of skill embodied in the kiosk with another player (either real or virtual), usually after paying an entry fee. Electronic sensors within the kiosk connected with the accompanying computerized control determine the winner of the game of skill and winner identity can be confirmed via the video command touchscreen. Payout of any cash prize owing to the winner can be directed by the computerized control by encoding a credit on the smart card with which game entry was effected, and at the same time the computerized control may also encode player game statistics on the smart card as well. The winner of the game may then insert his smart card through the card reader of the ATM for the purpose of transacting immediate cash disbursement or, alternatively, may deposit his winnings to an existing bank account or make any other electronic credit transaction he or she wishes--including leaving the winnings on the smart card for payment of further entry fees or other retail transactions.

The above exemplary configuration is subject to wide variation, particularly with respect to the smart card reader/encoder 16 and the credit card reader 17. In modified embodiments these structures may be combined as multifunctional smart card/credit card readers and/or a bill acceptor may be added or substituted.

An important aspect of the present invention is the provision of a game of skill to two or more players. For the purposes of the invention, a "player" may be a computer program capable of operating in lieu of a live player, so that for example a single player using the kiosk of Figure 1 could be given the option, via his touchscreen, of playing a computerized opponent. The opponent may even be mechanical, such as in the cyclical rotation of moving targets in a shooting match game of skill. The provision of the option of a computerized or mechanized opponent does not, however, convert a game of skill to a game of chance (viz. computerized chess opponents who invoke very real chess skills). This is an important distinction to arguable games of skill which are really games of chance, such as video solitaire or other games in which the skill required is primarily that of marshaling the chance or random element. Ordinarily, the skill games and sports contemplated for incorporation in the present device are those which require skills of either eye-hand or eye-motor coordination and/or the intellectual skills necessary to answer or to solve problems of science, trivia or war strategy. Skill games well suited to inclusion within the present device are mechanical hockey, chess, video football and others, whereas games substantially governed by die-rolling or card dealing (and their virtual equivalents) are not what is generally meant by "game of skill."

The separate use of a smart card, first at a play station and later (in the event of winning) at an ATM is not strictly speaking a necessary feature of the present invention--although it can be an extremely practical one. Kiosks such as are shown in Figure 1 will be welcomed in places where heretofore neither fully automated league devices nor ATMs have traditionally been available, such as pubs and bars, restaurants, public waiting areas, game arcades and amusement parks. Anticipated high usage of the kiosks suggests that some individuals will form a queue to use the ATM even while other individuals are using the play stations, so that direct credit of winnings to the player's smart card can be more secure than would an automatic payout to the adjacent ATM--which someone else other than the winner might be using at the time.

In the most preferred embodiment of the invention, the smart card has a greater processing and/or memory capacity than can be encoded in mere bar codes or magnetic stripes, as a result of inclusion of processors and/or computer chips therein. Such "smartest" cards can keep track of the owner's usage--game handicap, statistics and scores, for example. Music preferences and other menus can be stored in such cards.

That said, however, the smart card is not strictly essential to the present invention. The first embodiment of the invention as described in reference to Figure 1 is shown in the schematic diagram of Figure 2a, but Figure 2b illustrates that the smart card itself, as well as the smart card reader/encoder, may be eliminated from the present invention. If smart cards are not used at all, the control function of the present device merely directs payout, to the winner, via the adjacent currency acceptor/disburser. As shown in Figure 2b, players may pay their entry fees to the cash acceptor/disburser and proceed to play at stations 1 and 2, which are in two-way communication with a control (usually computerized), whereupon the control determines the winner and directs payment to the currency acceptor/disburser. Figure 2b shows an optional two-way communication between the play station and the currency acceptor/disburser, to permit the player to control the timing of actual disbursement of the winnings ("Are you ready to receive cash payout now? Y/N," for example).

Figure 2a shows in schematic diagram the invention substantially as described with reference to Figure 1. A device containing two play stations also contains a currency acceptor/disburser, all of which are in two-way communication with a control (usually computerized). Each play station is in two-way communication with a smart card reader/encoder, which may include credit card reading capability. After the players pay their entry fees (either by credit card via the smart card reader/encoder or at the currency acceptor/disburser) and play the game of skill or sport, the control may judge the contest and direct payout to the winner directly to the winner's smart card, via the smart card reader/encoder, after which the player may then use his smart card in a separate transaction at the currency acceptor/disburser. The arrangement of Figure 2a does allow for the possibility that the control means may direct immediate payout via the currency acceptor/disburser, but Figure 2a does not illustrate the player's option of mediating that payout directly, without going through the control.

Notwithstanding the above, it is entirely possible to combine individual smart card usage and multi-station ATM ports and still fall within the scope of the present invention. For example, a player using a smart card could still direct cash disbursement to be made immediately adjacent his play station, if the device is configured to offer cash disbursement in this way. This possibility is discussed further below, in the section which describes Figures 4 and 5. Smart cards may also be encoded with digital portraits of individual players as well as one or more currency accounts and player statistics and/or handicap, as well as current tournament standing if applicable.

A more elaborate, third embodiment of the invention is shown in Figure 3, in which the control function mediates among four play stations each having four adjacent smart card reader/encoder devices. The system also includes two currency acceptor/disburser mechanisms. A device according to the third embodiment of the invention is designed for use in high traffic areas where league competition and/or ATM usage are expected to be high. Although Figures 1-3 refer to two or four play stations, any number of play stations and adjacent smart card and currency handling equipment can be combined along the same organizational schemes--the number of play stations is not critical as long as the present device includes two or more of them.

Despite the practical and commercial appeal of separate provision of play stations and ATM(s), the present invention also embraces the direct combination of one or more play stations with direct cash acceptance and disbursement functions, as shown in Figures 4 and 5. Referring now to Figure 4, a partial side elevational view of a fourth embodiment of the present device is shown, in which a kiosk 40 includes a control panel 42 having a video command touchscreen 44, at least one smart card dispenser 46, a credit card reader 48, stereo speakers 50, a bill (cash) acceptor 52, a bill dispenser 54 and a receipt (printer) dispenser 56. Optionally, one of the smart card dispensers 46 may be recording means for encoding information on media other than smart cards, including but not limited to magnetic recording tape; floppy or removable hard disks or drives; recordable CDS, PC cards or PCMCIA cards and etc. A motion/sound/position sensor 58 is also provided adjacent the video command touchscreen. A player using the control panel 42 thus has all device functions available to him or her in a single location. Entry fees may be paid with credit card, smart card value or cash (or even coin, coin acceptor not shown). Games of skill may be played entirely using the video command touchscreen 44 (although there is no reason why manual controls such as appear in Figure 1 may not be incorporated in the control panel 42). Winnings, if any, may be collected as smart card credits or cash or may even be directed to remote credit locations via the video command touchscreen, if the control feature of the device provides such an option. Video touchscreen commands may activate a juke box internal to the kiosk 40 to play music through the stereo speakers 50 either separate from or in conjunction with game play.

Figure 5 illustrates the control panel 42 of Figure 4 with its cover removed, exposing the underlying mechanical features. A bill dispenser security safe 55 and associated vending hardware is thus positioned adjacent the bill dispenser 54. A bill acceptor mechanism 53 known in the art supports the bill acceptor 52 shown in Figure 4. A smart card safe 47 contains smart card inventory to supply to the smart card dispenser(s) 46. A motion/sound/position device 59 supports the sensor 58. A printer 57 provides receipts or other printed material to the receipt (printer) dispenser 56. Each individual mechanism illustrated in Figures 4 and 5 is known in the art, and the invention combines a number of them in a novel way to achieve a heretofore un-dreamed-of sport league device of almost inestimable ingenuity and consumer appeal.

It is not necessary for a kiosk, such as that shown in Figure 1, actually to include a mechanical skill game therein. A kiosk may simply include a video game of skill via one or more control panels 42 according to Figure 4, or variations thereof as described above. Alternatively, the control panels 42 may be provided as wall mounted stations without a free standing kiosk at all.

Other mechanisms included in the present device but not necessarily novel thereto are the games of skill themselves. Figure 6 provides a plan view of an exemplary playing field for miniature hockey, for inclusion in for example the invention shown in Figure 1, in which the playing field 60 contains a plurality of player gearbox mechanisms 62 for controlling a plurality of electromechanical teamsmen (not shown). Play is conducted by causing the teamsmen mechanically to strike a puck dropped from a puck ejector 64 competitively to score one or more goals into the nets 66, from which the pucks are automatically retrieved by puck tracks 68 back into the puck ejector 64. Computerized control of such a playing field thus requires only addition of counting sensors to the nets 66, to keep track of and to communicate the number of goals scored by each player.

A fifth embodiment of the invention is shown in the schematic diagram of Figure 7. The fifth embodiment differs from the third embodiment in two primary ways: a complete retail kiosk is incorporated into the device instead of simply one or more currency acceptor/disburser means, and sonic detector/loud speaker means provide a number of functions including an "attract" mode to advertise the retail kiosk as well as the game stations. The retail kiosk may be designed for literally any direct or remote vending as discussed earlier in this specification, and may provide endless combinations of point-of-sale purchases including passport application with on-site photography, international phone card dispensing with simultaneous ticket and travel services, accommodations, confirmations and execution of immediate e-mail and facsimile communications with simultaneous customized vending of postcards or personalized aerograms (with or without prepaid postage) for later travel use.

In the device as illustrated in Figures 1-7, the control equipment is generally provided from within a single game site or kiosk, but this is not necessary to the present invention and is not really even preferable. In fact, the most preferred embodiments of the present device are those which accommodate full scale league competitions, and so have at least LAN if not WAN configurations. Referring now to Figure 8, a WAN configuration of the present device is shown in schematic diagram wherein the WAN includes central control of a system of LANs controlled by local servers (according to the computer client/server model). A plurality of game kiosks, such as those shown in other Figures herewith, are controlled by each server, and all servers can be coordinated to administer league play. Network connection with banks, financial institutions and general retail goods and services providers is represented by the box labeled "BANKS." With the system illustrated in Figure 8, skill game or sport league devices according to the invention can administer tournaments throughout a single city, throughout several separate geographic locations or--quite easily--throughout the world.

For the purpose of Figure 8, "game kiosk" should be understood to mean any terminal or play station capable of network interconnection with the disclosed system, some of which may not resemble the subject matter of Figure 1 at all. For example, home participants using a PC or a machine manufactured by companies such as SEGA or NINTENDO may be added to the network with or without a smart card peripheral device therewith.

It is apparent from the above that the inventive concept is susceptible of wide variation without departure from the essential invention as described herewith. For this reason, the invention is only to be considered limited insofar as is set forth in the accompanying claims.

We claim:

1. A league device comprising: game means wherein means are provided for play by at least two players of a game of skill; control means in communication with said game means; and means for accepting and disbursing currency in communication with said control means; whereby administration of league play of two or more players of a game of skill is conducted automatically including acceptance of entry fees and disbursement of any winnings.

2. The league device according to claim 1 wherein said means for accepting and disbursing currency further comprises, in combination, a bill acceptor, a bill dispenser, a credit card reader and a smart card reader.

3. The league device according to claim 1 wherein said game means further includes a video screen for control of said game means.

4. The league device according to claim 1 wherein said game means further includes a video touchscreen for control of said game means and further for control of at least one additional retail transaction means present in association with same game means.

5. The league device according to claim 1 wherein said game means is substantially housed by a kiosk, wherein said control means engages a local area network and further wherein said kiosk houses an automated teller machine.

6. The league device according to claim 1 wherein the device includes at least two kiosks each of which substantially houses at least one of said game means, wherein said control means engages a wide area network, and further houses an automated teller machine.

7. The league device according to claim 1 wherein said game means includes means for playing at least one of the games in the group of skill games consisting of mechanical and electromechanical skill games and video games of skill.

8. The league device according to claim 7 wherein said game means includes at least one video control screen, at least one card reader/encoder and at least one audio speaker.

9. The league device according to claim 8 wherein said game means further includes control means for said at least one audio speaker.

10. The league device according to claim 9 wherein said game means is housed substantially within a kiosk which also contains juke box means and at least one control therefor.

11. The league device according to claim 10 wherein said kiosk further houses means for E-M Games of Skill Services; Smart Card Services; Insurance Services; Restaurant Services; Travel Services; Sports Services; Gaming Device Services; Delivery Services; Coupon Services; Introduction Services; Audio Services; News Services; Transportation Services; Utility Services; Physician Services; School Services; Security Services; Building Services; Credit Services; Directory Services; Home Services; Military Services; Personal Services; Automotive Services; Employment Services; Recreational Services; Travelers Check Services; Kids Services; Videogames of Skill Services; Internet Services; Brokerage Services; Government Services; Entertainment Services; Library Services; Catalog Services; Print Services; Diagnostic Services; Chat Services; Video Services; Database Services;

Barter Services; Engineering Services; Pharmacy Services; Identification Services; Detective Services; Church Services Loan Services; Training Services; Buying Services; Recruitment Services; Accounting Services; Photographic Services; Food Services; Radio Services; Credit Services; Theme Park Services; Music Services; Financial Services; Full-line Vending Services; Health Care Services; Remote Access Services; Payment Services; Computer Services; Search Services; Network Services; Subscription Services; Virtual Reality Services; Advertising Services; Rental Services; Programming Services; Beverage Services; Credit/Debit Card Services; Freight Services; Stored Value Card Services; Beauty Services; Tax Services; Leasing Services; Medical Services; Emergency Services; Publishing Services; Counseling Services; Satellite Services; Screening Services; Real Estate Services; Telephone Services; Ticket Services; Television Services; Dating Services; Information Services; Lottery Services; Software Services; Reservation Services; Communication Services; Intranet Services; Adult Services; Referral Services; Repair Services; Legal Services; Consulting Services; Maintenance Services; Moving Services; Trade Show Services; Design Services; Lodging Services; Mail Services; Fast Food Services; Automated Services; Recording Services; Clothing Services; Wireless Services; Human Services; and Encryption Services.

12. A league device, comprising: game means wherein means are provided for play by at least one player, and at least one opponent, of a game of skill, said game means being positioned adjacent a means for accepting and disbursing currency wherein said game means and said means for accepting and disbursing currency further contain means to enable independent or simultaneous operation of said game means and said means for accepting and disbursing currency.

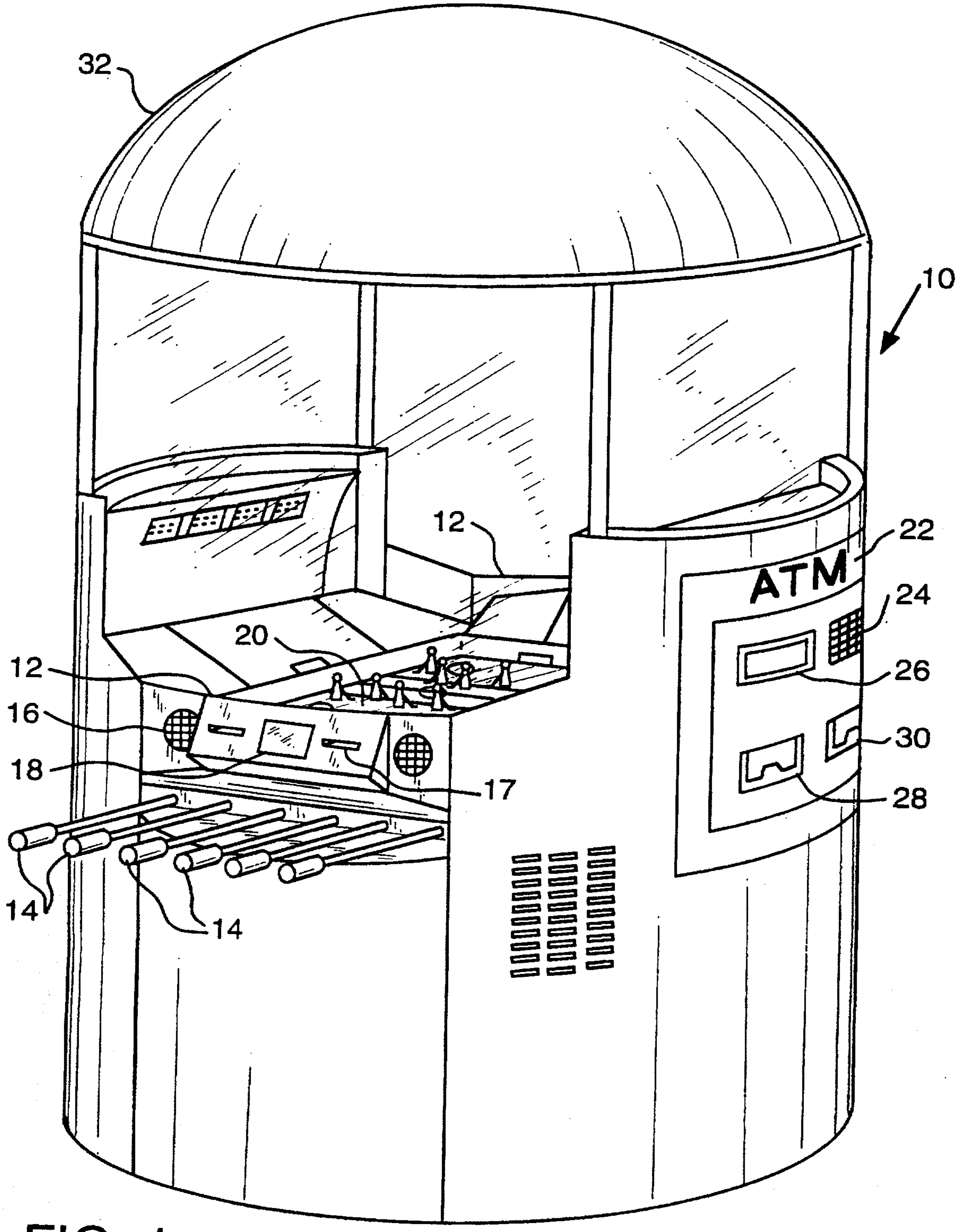


FIG. 1

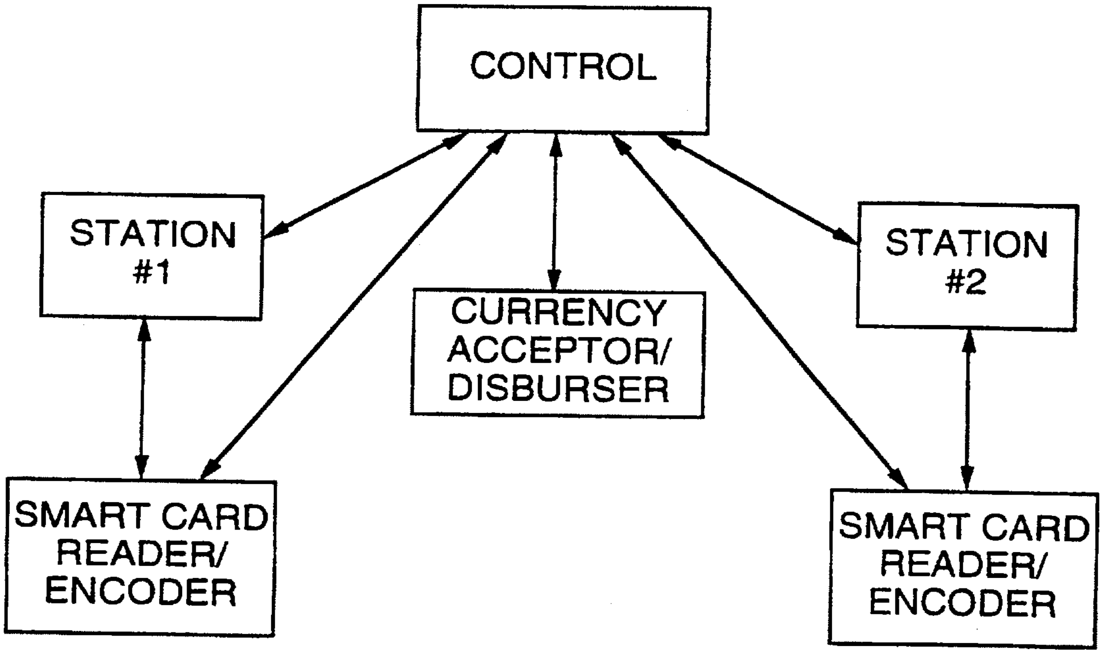

CONTROL
STATION #1
CURRENCY ACCEPTOR/ DISBURSER
STATION #2
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 2a

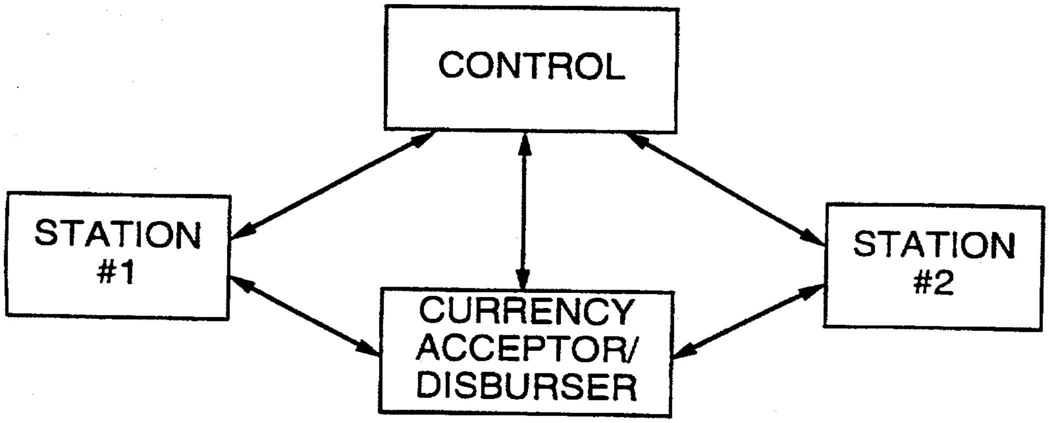

CONTROL
STATION #1
STATION #2
CURRENCY ACCEPTOR/ DISBURSER

FIG. 2b

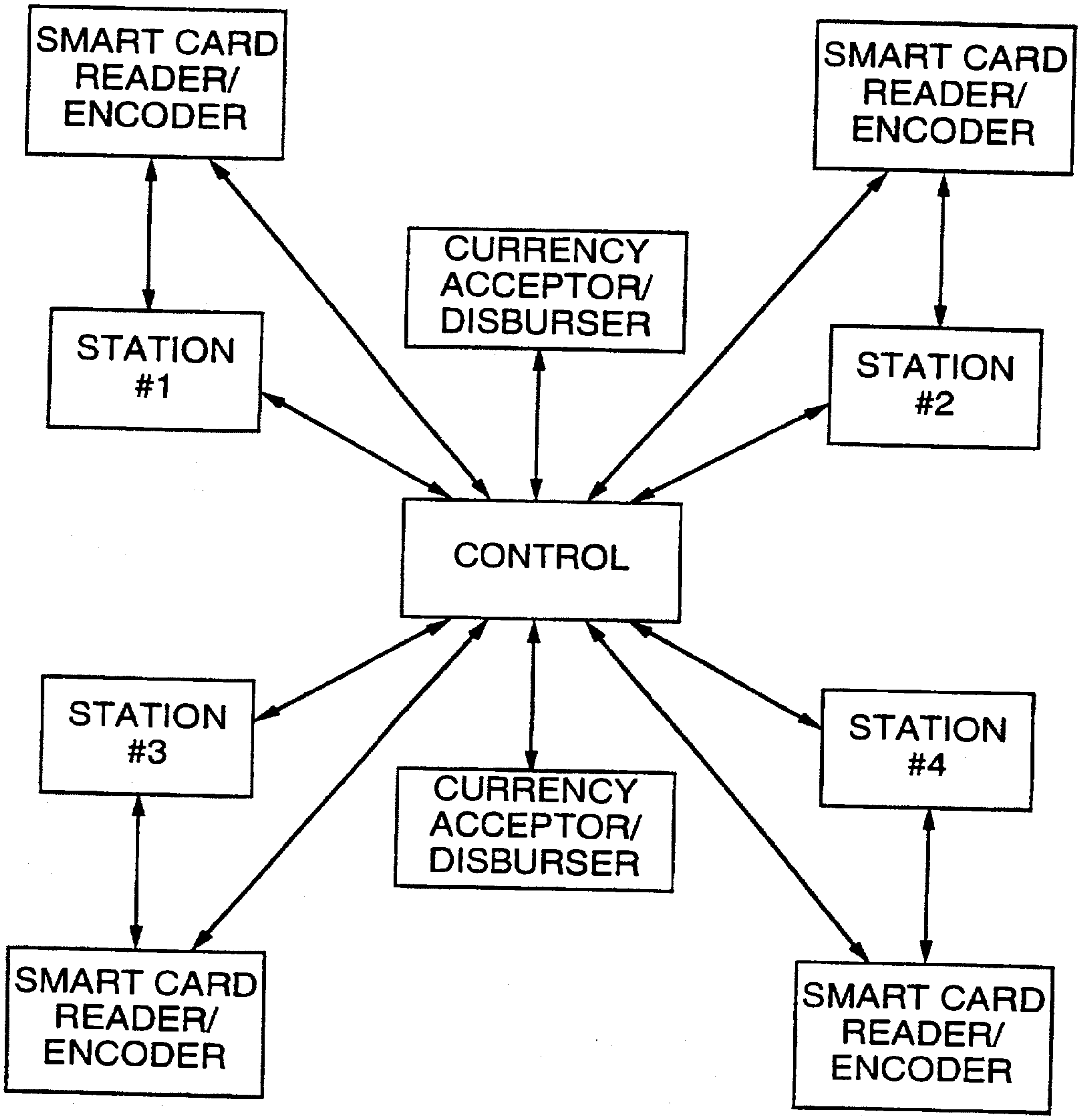

SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER
CURRENCY ACCEPTOR/ DISBURSER
STATION #1
STATION #2
CONTROL
STATION #3
STATION #4
CURRENCY ACCEPTOR/ DISBURSER
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 3

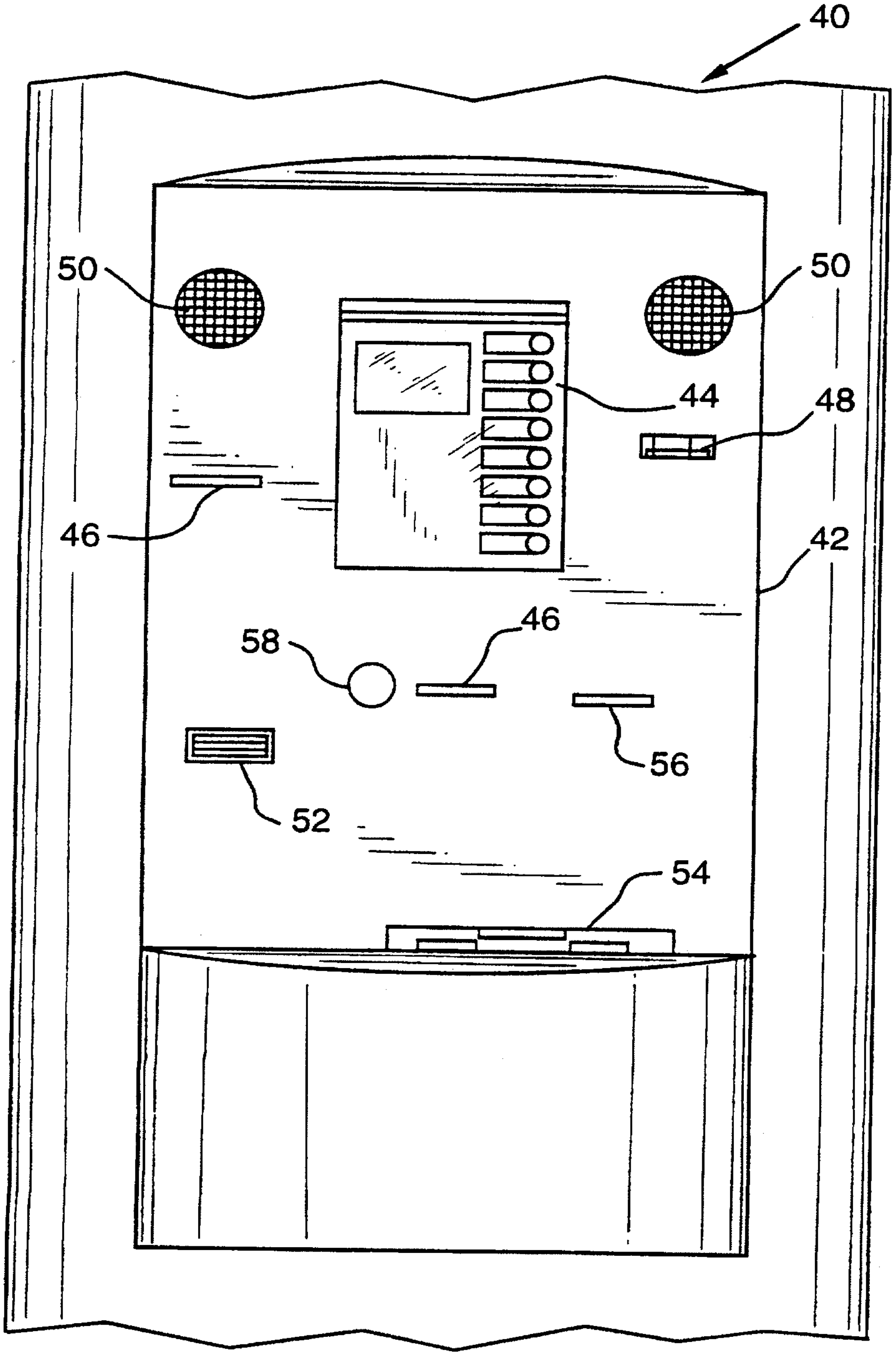


FIG. 4

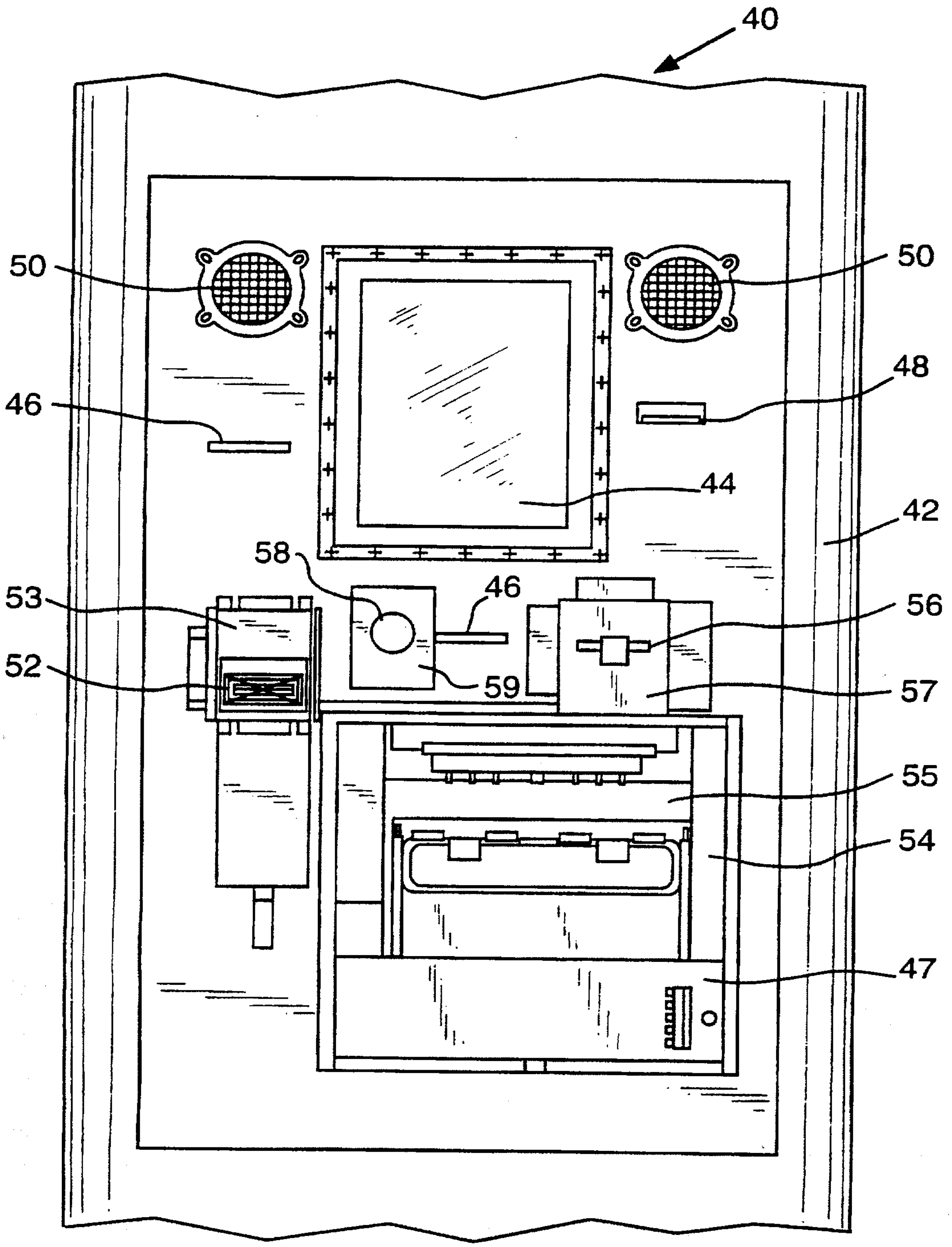


FIG. 5

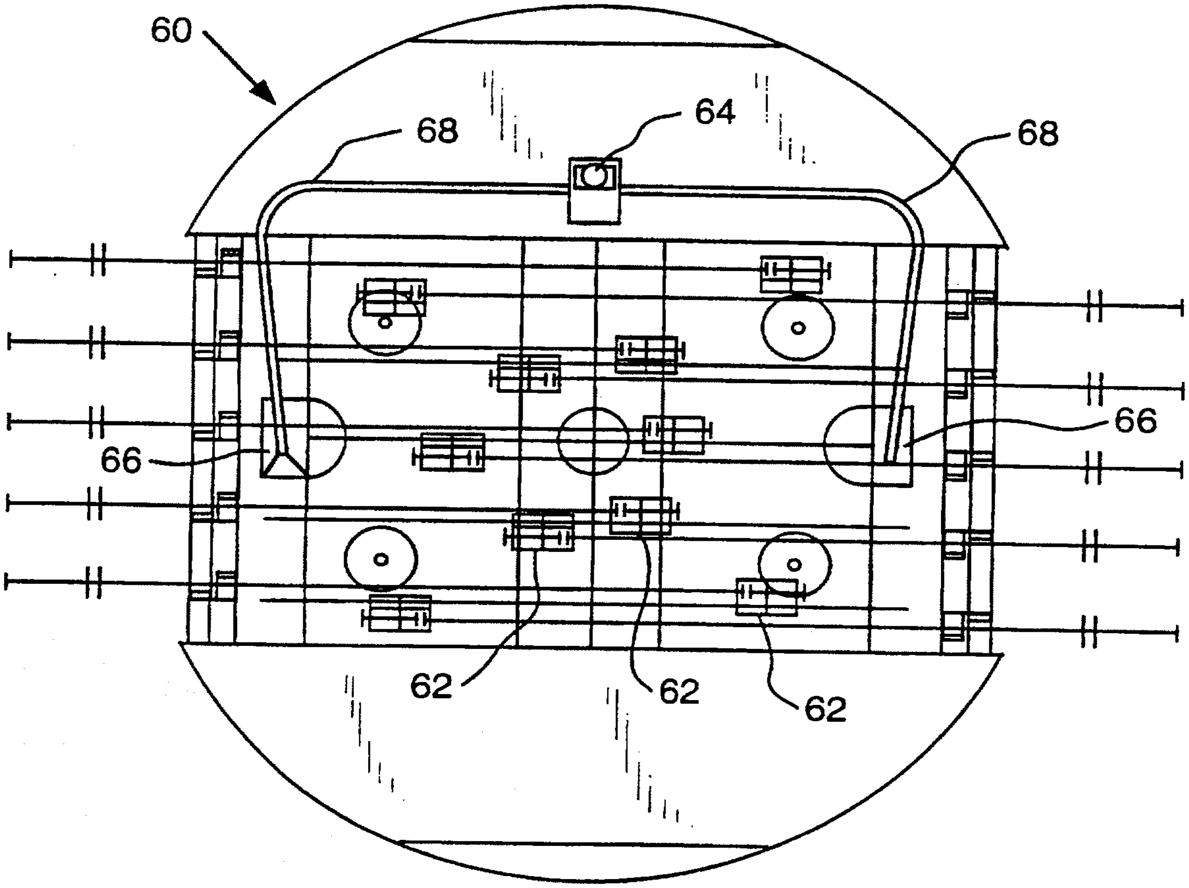


FIG. 6

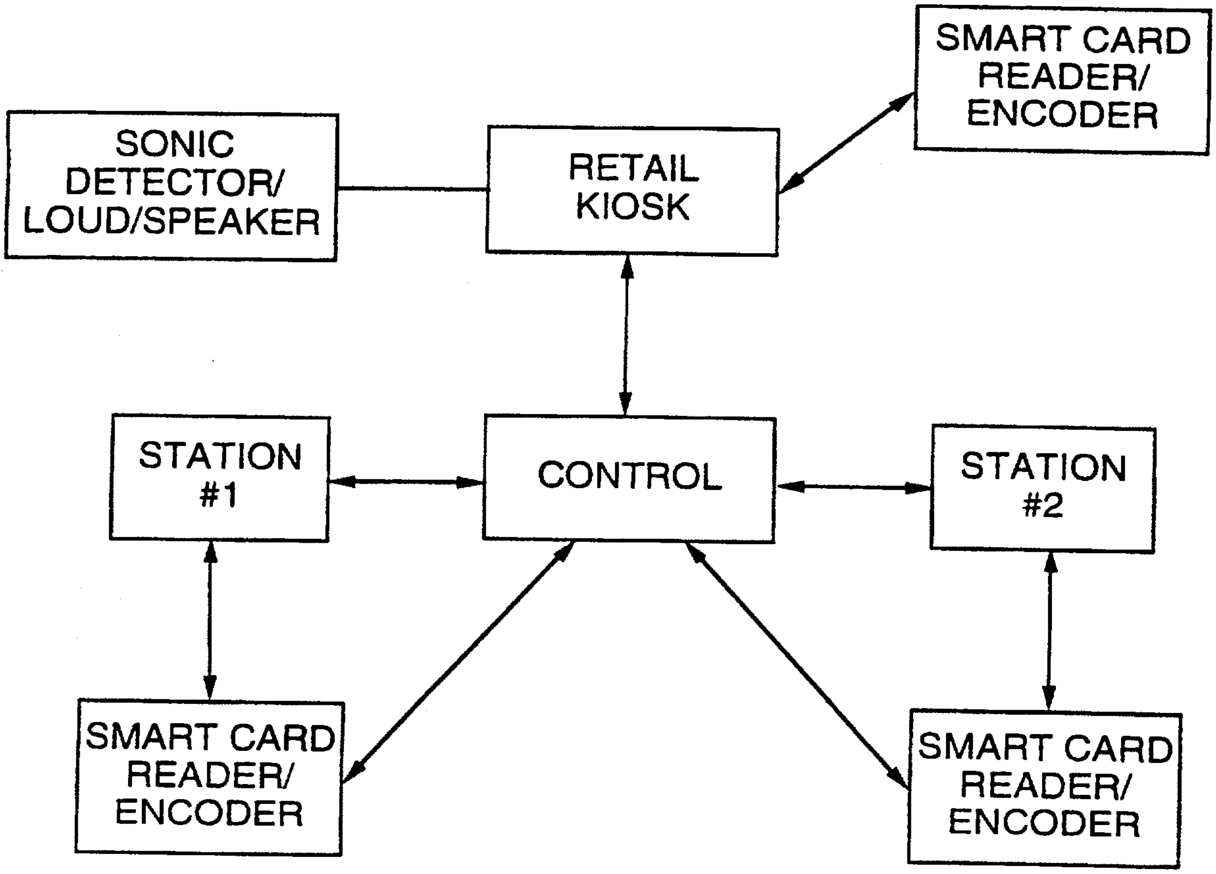

SMART CARD READER/ ENCODER
SONIC DETECTOR/ LOUD/SPEAKER
RETAIL KIOSK
STATION #1
CONTROL
STATION #2
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 7

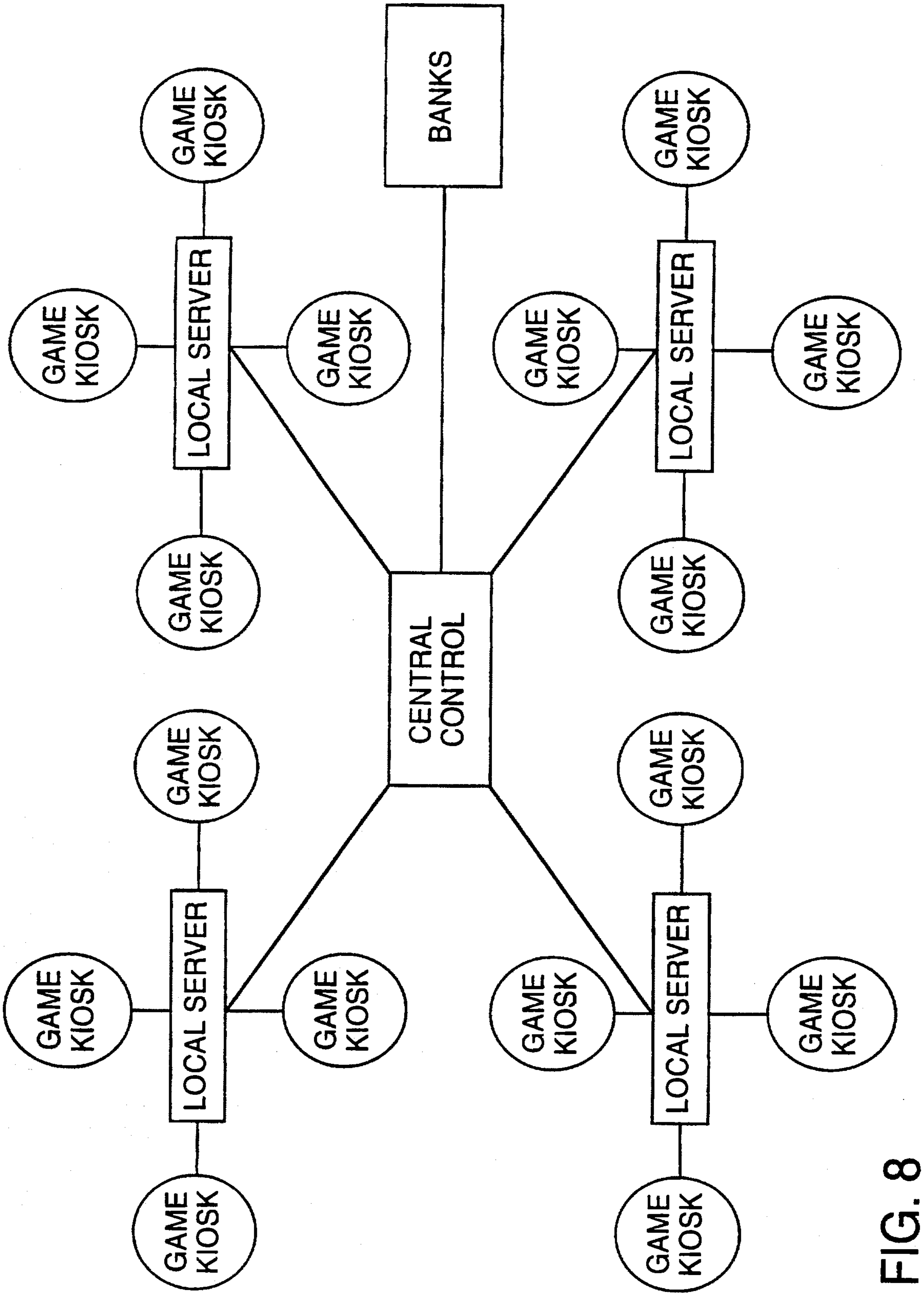

BANKS
CENTRAL CONTROL
LOCAL SERVER
LOCAL SERVER
LOCAL SERVER
LOCAL SERVER
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08072

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :A63F 9/22; G06F 19/00
US CL :235/279; 463/25, 42, 46
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 463/1, 4, 7, 25, 29, 40, 42, 46; 235/279

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- A	US 5,083,271 A (THACHER et al) 21 January 1992, entire document.	1-4, 7-9, 12 ---------------- 5, 6, 10, 11
A	US 4,669,730 A (SMALL) 02 June 1987, entire document.	5, 6, 10, 11

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 17 AUGUST 1997	Date of mailing of the international search report 10 SEP 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES SCHAAF Telephone No. (703) 308-3397

Electronic Acknowledgement Receipt

EFS ID:	7960998
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	06-JUL-2010
Filing Date:	21-AUG-2007
Time Stamp:	17:49:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDSofJuly06-2010.pdf	10190938 bfec2b25ddf22852d0345130285f91ae0549 80d6	yes	198

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	Foreign Reference	4	166
	Foreign Reference	167	198

Warnings:

Information:

Total Files Size (in bytes):	10190938

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010014881	A1	2001-08-16	Drummond Jay Paul	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1	00/54214	WO	A1	2000-09-14	Bionetrix Systems Corp		□
	2	98/08581	WO	A1	1998-03-05	Barcelou David M		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Communication pursuant to Article 94(3) EPC of April 9, 2010 in related EP application 02789831.1	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	3711
Examiner Name	
Attorney Docket Number	CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-07-06
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06K 9/00

A1

(11) International Publication Number: WO 00/54214

(43) International Publication Date: 14 September 2000 (14.09.00)

(21) International Application Number: PCT/US00/05722

(22) International Filing Date: 7 March 2000 (07.03.00)

(30) Priority Data:
09/264,726 9 March 1999 (09.03.99) US

(71) Applicant: BIONETRIX SYSTEMS CORPORATION [US/US]; 8150 Leesburg Pike, Suite 1230, Vienna, VA 22182 (US).

(72) Inventors: BIANCO, Peter, G.; 7710 Whiterim Terrace, Potomac, MD 20854 (US). BOON, William, T.; 13170 Flynn Court, Bristow, VA 20136 (US). STERLING, Robert, B.; 3941 Washington Street, Kensington, MD 20895 (US). WARE, Karl, R.; 3244 Pope Street, S.E., Washington, DC 20020 (US).

(74) Agents: SOKOHL, Robert, E. et al.; Sterne, Kessler, Goldstein & Fox P.L.L.C., Suite 600, 1100 New York Avenue, N.W., Washington, DC 20005–3934 (US).

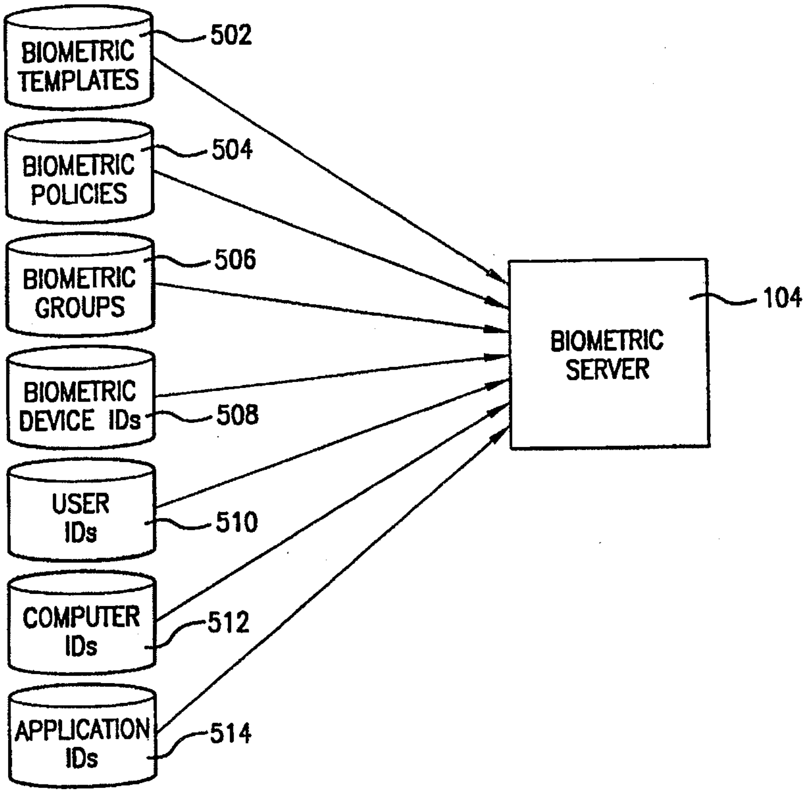
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ALLOWING ACCESS TO ENTERPRISE RESOURCES USING BIOMETRIC DEVICES

(57) Abstract

A system, method and computer program product that utilizes biometric measurements for the authentication of users to enterprise resources. The system includes a biometric server that stores the engine and collections of data required by the system to authenticate users. The collections of data include biometric templates (502), biometric policies (504), biometric groups (506), biometric device IDs (508), users IDs (510), computer IDs (512) and application IDs (514). In the present invention, it is the biometric policies (504) that determine the way or method in which a user is to be authenticated by the system. The pre–defined biometric policies (504) include an OR policy, an AND policy, a contingent policy, a random policy and a threshold policy. The execution of the biometric template (502) is created and stored in the biometric server (104) each time a user enrolls in a different biometric device (508). Biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece		Republic of Macedonia	**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's	**NZ**	New Zealand		
CM	Cameroon		Republic of Korea	**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

System, Method and Computer Program Product for Allowing Access to Enterprise Resources Using Biometric Devices

Background of the Invention

Field of the Invention

The present invention relates generally to a system, method and computer program product for allowing access to enterprise resources, and more particularly to the utilization of biometric measurements for the authentication of users, and thus access, to enterprise resources.

Related Art

Enterprise resources include computers, applications and data. Computers are often connected using one or more networks. There are many types of computer networks. Various types of networks include, but are not limited to, local-area networks (LAN), wide-area networks (WAN), the Internet and intranets. In general, a computer network may or may not be private. A typical private network is centrally controlled.

The resulting connectivity provided by a network enables several features such as sharing of data and other resources on the network. For example, networks enable applications such as electronic mail, network file systems (sharing of data using disks accessed over networks), distributed processing (different computers executing different parts of a program, generally in parallel) and sharing of printers and servers. These applications usually result in enhanced communication capabilities, efficient use of resources, and/or faster processing of data, thereby leading to productivity gains within an enterprise.

Provision of network connectivity and applications generally entails the operation of several network elements implemented according to predefined interfaces. Network elements include, but are not limited to, hardware circuits/devices and software entities (e.g., a software object, a process or a thread) which may operate according to interface specifications to provide the network connectivity or applications. The interfaces may be based on open protocols or proprietary protocols.

An open interface is public. Examples of open interfaces are Transmission Control Protocol/Internet Protocol (TCP/IP) and IEEE 802 family of protocols, both of which are commonly used in the networking community. Alternately, a proprietary interface is privately owned and controlled. An example of a proprietary interface is System Network Architecture (SNA) implemented mostly at IBM. Following is a brief description of the various types of networks.

A LAN connects computers that are geographically close together (e.g., in the same building). LANS are typically private networks being owned and controlled by an enterprise.

A WAN connects computers that are farther apart geographically and are connected by telephone lines or radio waves (e.g., in multiple offices and distant geographies). WANS are also typically private networks owned and controlled by an enterprise. Multiple LANs can be connected by a WAN.

The Internet is a global network connecting millions of computers. As of 1998, the Internet has more than 100 million users worldwide, and that number is growing rapidly. More than 100 countries are linked into exchanges of data, news and opinions. Unlike private networks which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Users can choose which Internet services to use and which local services to make available to the global Internet community. There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

An ISP is a company that provides access to the Internet. For a monthly fee, the ISP gives you a software package, username, password and access phone number. Equipped with a modem, a user can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. In addition to serving individuals, ISPs also serve large individual enterprises, providing a direct connection from the enterprise's networks to the Internet. ISPs themselves are connected to one another through Network Access Points (NAPs).

An intranet is a privately owned and controlled network. An intranet's host sites may look and act just like any other host site, but a firewall surrounding an intranet fends off unauthorized access. Like the Internet itself, intranets are used to share information (i.e. data). Secure intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols.

As enterprise resources grow so does the complexity and importance of protecting them. In general, the administration of resource protection involves determining the type of identification mechanism to protect enterprise resources, maintaining the integrity of the chosen identification mechanism, managing users, determining which enterprise resources to protect and determining alternative ways of allowing a user access to enterprise resources when the normal way of authentication is faulty. The administration of resource protection in a network is not only a complex and expensive task, but it may conflict with the desired productivity the networking of resources provides.

As discussed above, one of the results of networking together enterprise resources is the increase in productivity through enhanced communication and more efficient use of the resources. While this increase in productivity is important to any enterprise, so is the protection of its resources. While a network works to provide easier access to enterprise resources, an authentication mechanism for protecting the same resources works to restrict access to them. Therefore, so as to not offset the increase in productivity a network provides to an enterprise, an enterprise needs to balance adequate resource protection with an efficient means of administering such protection.

Summary of the Invention

The present invention is directed to a system, method and computer program product that utilizes biometric measurements for the authentication of users to enterprise resources. The system includes a biometric server that stores the engine and collections of data required by the system to authenticate users. The collections of data include biometric templates, biometric policies, biometric groups, biometric device IDs, user IDs, computer IDs and application IDs. In the present invention, the biometric policies determine the way or method in which a user is to be authenticated by the system. The execution of the biometric policies involves the use of one or more biometric templates. One unique biometric template is created and stored in the biometric server each time a user enrolls in a different biometric device. Biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. These measurements, called biometric measurements, may include, but are not limited to, measurements of finger and hand geometry, retina and facial images, weight, DNA data, breath, voice, typing stroke and signature.

The types of data stored in the biometric server are partially determined through the operations of an enrollment station and an administration station. The enrollment station is used to enroll users into biometric system. The administration station is used to perform overall management duties and to initially setup the data in biometric server. A satellite enrollment station can be used to enroll users into biometric system at remote locations. Finally, an alternate biometric server is a backup or standby server to biometric server. The alternate biometric server ensures that the system is always available to authenticate users.

The biometric policies of the present invention provide flexibility to the level of protection for individual enterprise resources. The pre-defined biometric polices include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. This is done through the layering of both biometric devices and non-biometric devices. The layering of devices allows for the combination of one or more devices in a logical way (via biometric policies) to protect each enterprise resource. The present invention also allows different threshold values to be set for each biometric device. In other words, the present invention can tailor the authentication level based on probability that each user must pass before the user gains access to enterprise resources (e.g., 1/1000, 1/10,000, or 1/1000,0000 that the user is who claims to be).

Another feature of the present invention is directed to a method of storing both biometric templates and digital certificates in a hierarchical structure for ease of access to the biometric templates and the digital certificates. Another feature of the present invention is directed to utilizing the system of the present invention as a roaming profile server in a certificate authority system.

Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

Brief Description of the Figures

The present invention will be described with reference to the accompanying drawings, wherein:

FIG. 1 is a block diagram of the physical components of a biometric authentication system connected by a network according to a preferred embodiment of the present invention;

FIG. 2 is a block diagram of a typical enterprise network system incorporating the biometric authentication system according to a preferred embodiment of the present invention;

FIG. 3 is a block diagram of a computer system preferably used to implement the present invention;

FIG. 4 illustrates the dynamic steps to establish communication between a client and a server executing an object-oriented program. For illustration purposes, FIG. 4 is broken into nine(9) figures including FIG. 4A, FIG. 4B, FIG. 4C, FIG. 4D, FIG. 4E, FIG. 4F, FIG. 4G, FIG. 4H and FIG. 4I;

FIG. 5 illustrates various collections of data stored in the biometric server of the present invention;

FIG. 6 is a flowchart illustrating a typical sequence of steps an administrator may take to initially setup a biometric server;

FIG. 7 is a block diagram of the objects involved in authenticating a user by the present invention;

FIGs. 8A and 8B are a flowchart depicting the high-level operation of authenticating a user by the present invention;

FIG. 9 is a flowchart illustrating the typical operation of a biometric device as it tests a user;

FIG. 10 is a block diagram of the objects involved in starting the authentication process of the present invention with "live" biometric data;

FIG. 11 presents a flowchart depicting the high-level operation of the objects in FIG. 10;

FIG. 12 is a block diagram of the objects involved in the enrollment process of the present invention;

FIG. 13 is a flowchart illustrating the typical operation of the enrollment process of the present invention;

FIG. 14 is a window or screen shot generated by the graphical user interface of the present invention;

FIG. 15 is a chart illustrating the layering process of the present invention;

FIG. 16 is a flowchart illustrating the process of layering using biometric policies of the present invention;

FIG. 17 is a flowchart illustrating the steps involved in executing an OR policy of the present invention;

FIG. 18 is a flowchart illustrating the steps involved in executing an AND policy of the present invention;

FIG. 19 is a flowchart illustrating the steps involved in executing a CONTINGENT policy of the present invention;

FIG. 20 is a flowchart illustrating the steps involved in executing a RANDOM policy of the present invention;

FIG. 21 is a flowchart illustrating the steps involved in executing a THRESHOLD policy of the present invention;

FIG. 22 is a flowchart illustrating the steps involved in executing OR policy having a list of biometric policies of the present invention;

FIG. 23 is a flowchart illustrating the steps involved in executing an AND policy having a list of biometric policies of the present invention;

FIG. 24 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of biometric policies of the present invention;

FIG. 25 is a flowchart illustrating the steps involved in executing an OR policy having a list of policies or devices of the present invention;

FIG. 26 is a flowchart illustrating the steps involved in executing an AND policy having a list of policies or devices of the present invention;

FIG. 27 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of policies or devices of the present invention;

FIG. 28 illustrates an enterprise connected by a WAN incorporating multiple biometric systems of the present invention;

FIG. 29 is a block diagram illustrating how the present invention can be integrated with a public key system;

FIG. 30 is a diagram illustrating various types of networks and how each type of network can be connected to other networks;

FIG. 31 is a flowchart illustrating the steps involved in executing a CONTINGENT policy having a list of biometric policies of the present invention;

FIG. 32 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a list of biometric policies of the present invention;

FIG. 33 is a flowchart illustrating the steps involved in executing a CONTINGENT policy having a list of policies or devices of the present invention; and

FIG. 34 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a list of policies or devices of the present invention.

Detailed Description of the Preferred Embodiments

A. Overview of the Invention

The inventors of the present invention recognized that a solution did not exist that effectively balances the protection of resources with ease of access to the same resources in a networked environment. The general solution of the present invention is twofold. First, use as adequate an identification mechanism as possible to protect enterprise resources. And second, provide a method and system that utilizes the adequate identification mechanism to provide effective authentication to resources in a networked environment. This method and system for authentication must not decrease the productivity that a network provides an enterprise.

1. Determining an Adequate Identification Mechanism

Billions of dollars have been lost by thousands of enterprises due to inadequate authentication to enterprise resources. For years enterprises have protected valuable resources through various types of identification mechanisms that do not conclusively authenticate a user. These inadequate identification mechanisms include, but are not limited to, passwords, smart cards and tokens. The reason why passwords, smart cards and tokens do not conclusively authentic a user is due to a human factor involved with using these identification mechanisms. In fact, the weakest link in authentication is the human factor.

The human factor creates problems that can lead to unauthorized access since these mechanisms require a user to either know something and/or keep something in his or her possession. For example, password identification requires a user to remember a password. Whereas, tokens and smart cards require a user to have the token or smart card in his or her possession to gain access to enterprise resources. Anything a user knows or has in possession can be compromised.

When inadequate authentication exists people gain unauthorized access to enterprise resources. While a user who gains unauthorized access can be a "cracker" or "hacker" (e.g., a person outside the enterprise), more often the user is from within the enterprise itself (e.g., an employee of the enterprise). An example of this is as follows. As discussed above, password identification requires User A to remember a password. If User A's password is written down, or User B sees User A typing a password at a keyboard, then User B can use User A's password to effectively be User A as far as the enterprise is concerned. The result is that User B now has access to all the resources User A has access to. As with passwords, a similar scenario can happen with tokens or smart cards when User A misplaces a token or smart card and User B finds it. The damage that can be done to resources in a networked environment far exceeds the damage that can be done to resources contained within a single computer (e.g., not networked).

Many enterprises reduce the cost and complexity of administering its resource protection by incorporating a process called "single sign-on." Single sign-on provides each user with one password, token or smart card to access all enterprise resources. Most people can remember one password without writing it down and/or keep track of one token or smart card. While this reduces the complexity and cost of administering resource protection, it reduces the probability that the user gaining access is authentic. Now, one password may compromise all enterprise resources.

The probability that the user gaining access is authentic can be increased by forcing each user to use multiple passwords, tokens or smart cards for different resources. Many people have difficulty in managing multiple passwords, tokens or smart cards. This increases the likelihood that a user will write down passwords or misplace tokens and smart cards. When this happens, once again all enterprise resources may be compromised.

Another aspect of why password, tokens or smart cards are inadequate identification mechanisms involves the sharing of these between users. An example that can cost an enterprise millions of dollars a year is a practice called "buddy punching." Buddy punching typically involves two users or employees within an enterprise that requires its employees to use a password to "punch in and out" of work each day. Password, or even tokens and smart cards, make is easy for one employee to "punch in" another employee at the beginning of the day and then "punch out" that same employee at the end of the day. The practice of "buddy punching" allows an employee who stays home a particular day to still have the benefit of receiving a paycheck for that day.

Therefore, the inventors of the present invention recognized that an identification mechanism is needed that avoids the weakest link in authentication that is a result of the human factor discussed above.

2. *Biometric Identification Mechanism: An Adequate Authentication Mechanism*

A biometric identification mechanism eliminates the weakest link caused by the human factor. Biometric identification mechanisms, or biometric devices, utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. Biometric identification mechanisms include two basic categories of biometric measurements. The first category involves measuring a unique characteristic found on a user's body. This may include, but is not limited to, finger and hand geometry, retina and facial images, weight, DNA data and breath. The second category involves measuring a user's behavioral characteristics. This may include, but is not limited to, voice, typing stroke and signature. In general, anything that can be measured on a user that is unique can be used as a biometric measurement.

While anything that can be measured on a user that is unique can be used as a biometric measurement, the best biometric measurements to use for authentication purposes depend on the consistency over time of the biometric measured. For example, user weight is a biometric measurement. Because weight is a biometric measurement that fluctuates frequently for many people, it is not a desirable biometric measurement to use for authentication purposes.

The general process of using biometric identification mechanisms as an authentication mechanism is as follows. The user is prompted for a particular biometric measurement that is used by a biometric device to generate a value. The value gets stored in a template as stored biometric data. When the user wants to gain access to a resource that is protected by the biometric device, the user is prompted for live biometric data. The live biometric data is matched with the stored biometric data. In reality, the live biometric data and the stored biometric data will never be exactly the same. Therefore, a user must come within some tolerance to pass the biometric device and gain access to the protected resources. As mentioned above, the biometric device utilizes a scientific technique to identify a user based on biometric measurements. The tolerance is typically predetermined by the vendor for the particular biometric device used.

A specific example of how biometric identification works can be illustrated by a typical fingerprint device. A fingerprint device measures the geometry of a fingerprint. First, a user is prompted for multiple samples of a fingerprint. For each sample, a number of characteristics or measurements are identified. Then, for all of the multiple samples, a number of common characteristics or measurements are identified. The common characteristics or measurements are processed through a unique algorithm which generates a unique template to store the biometric data. When a "live" fingerprint is presented for identification, it is processed through the same algorithm. If the output from the "live" process matches the stored biometric data within a certain tolerance, the user is considered to be authenticated and gains access to which ever resource the fingerprint device is protecting.

A specific example of how biometric identification works when behavioral measurements are involved can be illustrated by a typical signature device. Here, a user is prompted for multiple samples of a signature. For each sample, characteristics or measurements are identified. The characteristics or measurements include the pressure, sequence of events, direction, relative vectors and speed. One example of the sequence of events is to identify that when the user signed his or her signature, that "t" was crossed before "I" dotted. An example of direction is that the user crossed a "t" from right to left. Relative vectors may include the information that "F" is 2.1 the height of "e." Finally, speed recorded is the time it took the user to sign a signature from start to finish.

As with fingerprint devices, common characteristics or measurements are identified for the multiple samples. These common characteristics or measurements are processed through a unique algorithm which generates a unique template to store the biometric data. When a "live" signature is presented for identification, it is processed through the algorithm. If the output from the "live" process matches the stored biometric data within a certain predetermined tolerance, the user is considered to be authenticated.

The use of biometric identification mechanisms as a means for authentication eliminates the problems discussed above involving the use of passwords, tokens or smart cards. Because biometric measurements involve either a unique characteristic found on a user's body (e.g., fingerprint) or a user's behavioral characteristics (e.g., signature), it is impossible for users to forget or lose the mechanism of authenticating themselves. Now, it is impossible for User

B to "steal" the mechanism of authenticating User A to the enterprise. Likewise, the practices of users sharing passwords and "buddy punching" are eliminated.

While the use of biometric devices can conclusively authenticate a user, the inventors of the present invention recognized that a method and system was needed that utilizes biometric devices to provide effective authentication to resources in a networked environment while not decreasing the productivity a network provides an enterprise.

Most enterprises contained in one office today have a LAN. But, more often enterprises today span multiple offices and distant geographies. These enterprises typically have a WAN. As discussed above, networks provide increased productivity to an enterprise by allowing users easy access to all the resources on the network. This is true independent of which office the user is at and where the resource is located within the enterprise. In contrast, resource protection limits the accessability of resources to a user without first being authenticated. Therefore, if the administration of resource protection is not efficient, then the increase in productivity gained by networking is lost. Simply put, if the right user cannot gain access to needed resources, then the enterprise suffers from a decrease in productivity. Yet, if unauthorized users gain access to enterprise resources, then the enterprise also suffers from a potential decrease in productivity. This potential decrease in productivity is due partly to resource loss.

The present invention overcomes limitations that are encountered when resource protection is used in a networked environment. The present invention has the following benefits: (1) flexibility to use the right biometric measurement for an environment; (2) allows user mobility within the enterprise; (3) flexibility in the degree of authentication required to protect each resource; (4) allows remote enrollment of users into a resource protection system; (5) allows remote refreshing of biometric templates; and (6) ensures the integrity of software loaded on remote computers in the network. The present invention also allows different threshold values to be set for each biometric device. In other words, the present invention can tailor the authentication level based on probability that each user must pass before gains access to enterprise resources (e.g., 1/1000, 1/10,000, or 1/1000,0000 that the user is who claims to be).

3. *Biometric Authentication System*

FIG. 1 is a block diagram of the functional components of biometric authentication system 102 (also called "biometric system" herein) connected by network 114 according to a preferred embodiment of the present invention. Biometric system 102 includes biometric server 104, enrollment station 106, administration station 108, alternate biometric server 110 and satellite enrollment station 112. Network 114 connects the functional components of biometric system 102. The connectivity provided by network 114 enables such features as the sharing of data and other resources on biometric system 102.

The topology of network 114 as shown in FIG. 1 is called a bus topology. In general, the topology of a network is the geometric arrangement of functions (i.e., computers) within the system. Other common types of network topologies include star and ring topologies. Although the present invention is illustrated in FIG. 1 as incorporating a bus topology, the present invention can equally be applied to other topologies.

Biometric server 104 stores the engine for biometric system 102. Biometric server 104 also stores collections of data required by biometric system 102. Both the functions of the engine and the data stored in biometric server 104 will be discussed in further detail below. The types of data stored in biometric server 104 are partially determined through the operations of enrollment station 106 and administration station 108. Enrollment station 106 is used to enroll users into biometric system 102. Enrollment station 106 has attached to it every type of biometric device used by biometric system 102 to enroll and ultimately authenticate users. When a user is enrolled into biometric system 102, the user may be enrolled with as many biometric devices as the administrator deems necessary.

Administration station 108 is used by the administrator of biometric system 102 to do perform overall management duties. The administrator can also use administration station 108 to generate various reports. The reports may include a list of different types of data stored in biometric server 104 (e.g., a list of the currently enrolled users in biometric system 102). In addition, administration station 108 is typically used to setup the initial data in biometric server 104. Another component is satellite enrollment station 112. Enrollment station 112 is used to enroll users into biometric system 102 at remote locations. Satellite enrollment station 112 may have as many biometric devices attached to it as administration station 108, but alternatively may also be a scaled down version of administration station 108.

One or more alternate biometric servers 110 are backup or standby servers to biometric server 104. Alternate biometric server 110 stores the exact same data as biometric server 104. Only in the event that biometric server 104 fails does alternate biometric server 110 become active and take over the responsibility of authenticating users. The purpose of alternate biometric server 110 is to ensure that biometric system 102 is always available to authenticate users.

There are other ways to ensure the availability of biometric system 102, however, including: biometric server 104 and alternate biometric server 110 having equal responsibility to authenticate users; administration station 108 backup and tape and/or CD-ROM backup. The biometric server 104 and alternate biometric server 110 having equal responsibility to authenticate users means that they are both active at all times. There is a constant synchronization between biometric server 104 and alternate biometric server 110. In the event that one or the other server fails, the other server takes over the responsibility of authenticating users. When the failed server becomes active again, it initiates synchronization with the other server.

Another way to ensure the availability of biometric system 102 is through administration station 108 backup. Here, administration station 108 acts like a master biometric repository. Administration station 108 updates all active biometric servers 104 simultaneously. The final way to ensure the availability of biometric server 102 is through a tape and/or CD-ROM backup.

Although a preferred embodiment of the present invention includes all of the functional components of biometric system 102 discussed above, several (or all) components may be combined as long as the functionality of each component still exists within biometric system 102 as described above. For example, enrollment station 106 and administration station 108 can be combined into one functional component. In addition, several components of biometric system 102 are optional. For example, an enterprise may not have the need to remotely enroll users or may just desire not to. Therefore, satellite enrollment station 112 would not be needed.

4. Network System

As mentioned above, various types of networks include, but are not limited to, LANs, WANs, the Internet and intranets. An enterprise may utilize one type of network or any combination of the different types of networks. FIG. 30 is a diagram illustrating the various types of networks and how each type of network can be connected to other networks.

FIG. 30 includes LAN 3002, LAN 3004, LAN 3006, LAN 3008, WAN 3010, Internet 3012, firewall 3014, connection 3016, host 3018, connection 3020, connection 3022, connection 3024, connection 3026, connection 3028 and connection 3030. Connections 3016, 3024, and 3026 through 3030 are typically provided by an ISP.

As shown in FIG. 30, LAN 3002, LAN 3004 and LAN 3006 are connected to WAN 3010. LAN 3008 and host 3018 are also connected to WAN 3010 via the Internet 3012. Connections 3020 and 3022 are typically virtual private networks (VPN). A VPN is a network that is constructed by using public wires to provide connectivity. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Host 3018 may have a type of access to WAN 3010 called dial-up access. Dial-up access refers to connecting a host (i.e., device) to a network via a modem and a public telephone network. Dial-up access is really just like a phone connection, except that the parties at the two ends are computer devices rather than people. Because dial-up access uses normal telephone lines, the quality of the connection is not always good and data rates are limited. An alternative way to connect two computers is through a leased line, which is a permanent connection between two devices. Leased lines provide faster throughput and better quality connections, but they are also more expensive.

WAN 3010 can also be implemented as an intranet as described above. Thus, firewall 3014 can be used to protect WAN 3010 by fending off unauthorized access. Many network systems today incorporate a firewall. A firewall is a system designed to prevent unauthorized access to or from a network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. Once a user is authorized to access the network, firewalls are further designed to prevent unauthorized transfer of data to and from the network. All data entering or leaving the intranet pass through the firewall, which examines each transmission and blocks those that do not meet the specified security criteria. Firewalls can be implemented in both hardware and software, or a combination of both. A firewall is considered a first line of defense in protecting private information (i.e., data).

FIG. 2 is a block diagram of an enterprise network system 202 incorporating biometric system 102 according to a preferred embodiment of the present invention. It is important to note that network system 202 may be one type of network or any combination of the different types of networks described in reference to FIG. 30 above. Referring again to FIG. 30, various functional components of biometric system 102 can be physically located at one or more locations in FIG. 30. For example, biometric system 102 may be located at LAN 3002, LAN 3004, LAN 3006, LAN 3008, WAN 3010 and/or host 3018.

In addition to the components of biometric system 102, network system 202 includes one or more applications, such as application 204, one or more application interfaces, such as application interface 206, one or more user computers, such as user computer 208, one or more remote/web computers, such as remote/web computer 210, web server 212 and web server interface 214. All of the components in network system 202 are considered resources of the enterprise. Network 114 connects both the functional components of biometric system 102 and the additional functional components of network system 202. This connectivity enables such features as the sharing of data and other resources on network system 202.

Examples of application 204 may include, but are not limited to, electronic mail and word processing. Each application 204 has an application interface 206 that allows it to communicate over network 114 to other resources or components in network system 202. In addition, network system 202 includes one or more of user computer 208. Each user computer 208 is located within the enterprise and typically has one or more biometric devices attached to it. User computer 208 is one location where users can gain access to network system 202. To facilitate user access, each computer 208 provides an interface for users to be authenticated by biometric system 102.

Remote/web computer 210 provides the same functions as user computer 208, but remote/web computer 210 accesses network 114 via the Internet. In order for remote/web computer 210 to connect to network 114, it must go through web server 212. Web server interface 214 allows web server 212 to communicate over network 114 to other resources or components in network system 202, including biometric system 102.

In a preferred embodiment of the present invention, users can be required to be authenticated by biometric system 102 when they try to access various points in network system 202. These various access points include network system 202 itself, one or more of application 204 and/or one or more of user computer 208. Because enterprise networks today typically span multiple offices and distant geographies, the different access points in network system 202 may potentially have very different environments. The inventors of the present invention recognized that there is a need for flexibility to use the appropriate biometric device or measurement for the environment. To achieve this flexibility there is a need for many different types of biometric devices to be utilized in network system 202.

5. *The Need for the Appropriate Biometric Measurement for an Environment*

The appropriate biometric measurement must be used for an environment. The type of environment depends on the location in the network of the biometric device that will be reading the biometric measurement. As mentioned above, biometric devices utilize a scientific technique to identify a user based on compared measurements of unique personal characteristics. Biometric measurements, may include, but are not limited to, measurements of finger and hand geometry, retina and facial images, weight, DNA data, breath, voice, typing stroke and signature. There are two aspects of the environment that must be addressed in order to determine the appropriate biometric measurement for that particular environment: a physical aspect and a psychological aspect.

The physical aspect of the environment involves, but is not limited to, lighting and noise. For example, in an environment with poor lighting, a user's iris or facial image may be difficult for the biometric device to measure. Likewise, in a noisy environment a user's voice may be hard to measure.

The psychological aspect of the environment involves the comfort level of users. An example of exceeding a user's comfort level is requiring a user to give a DNA sample to gain access to enterprise resources he or she must access every day. There are certain comfort levels that users of a network have come accustomed to and may refuse to exceed that level.

The result of not using the appropriate biometric measurement for the environment increases the likelihood that the user will not gain access to required resources when needed, thus decreasing enterprise productivity. This happens when the biometric device cannot read a biometric measurement or when users refuse to give the required "live" biometric data for authentication. Therefore, what is needed is the flexibility to use the appropriate biometric measurement for the environment.

The flexibility to use the appropriate biometric measurement for the environment results in the need for many different types of off-the-shelf biometric devices in a single network. Therefore, the authentication task is often complicated by the fact that each of the biometric devices may be provided by several vendors. Currently, biometric devices must conform to a pre-defined interface (or standard) to operate as a part of an integrated network. While the availability of each biometric device from multiple vendors may lead to reduction in prices, the management of networks having biometric devices from different vendors poses additional limitations.

For example, some vendors may allow their biometric devices to be managed from proprietary platforms only. Some vendors may support standards based network management applications (e.g., Simple Network Management Protocol), but the integration of the management of their devices into a network often requires extensive training. For example, the installation of the software to work (i.e., interface) with a network may require training from the vendor. Administrators may need more training for providing on-going support. Such training may need to be provided each time a new biometric device is added to the network. In addition, substantial effort may be required on the part of the vendors to develop software which interfaces with an enterprise's existing network. The resulting overhead due to development and training is unacceptable in most enterprises. This problem of conformity to a pre-defined interface to operate as a part of an integrated network applies equally as well to non-biometric devices.

6. Open Interface

The open interface of the present invention includes a device open interface to allow for the integration of biometric system 102 with biometric devices. The device open interface of the present invention provides an interface that all incompatible biometric and non-biometric devices can communicate with. This provides flexibility to an enterprise in several ways. One way it provides flexibility is that an enterprise can now use the appropriate biometric measurement for the environment.

Another way the present invention's device open interface provides flexibility is by allowing an enterprise to integrate existing non-biometric devices into biometric system 102 (FIG.1). This flexibility is important because all users within an enterprise do not have to be enrolled into biometric system 102 at the same time. Also, some users may never have to be enrolled into biometric system 102 and still be able to gain access to network system 202 (FIG. 2).

Another flexibility provided by the device open interface is by allowing an enterprise to supplement biometric system 102 with non-biometric devices or new biometric devices as they are developed. As mentioned above, biometric devices utilize a scientific technique to identify a user based on biometric measurements. The device open interface provided by the present invention allows an enterprise the flexibility to use any off-the-shelf biometric or non-biometric device to protect a resource. As will be shown later, the flexibility of the open interface enables administrators to combine biometric devices via biometric policies for the authentication of users.

The device open interface is propriety software that is used to communicate to biometric devices in order to retrieve live sample data, match live sample data against stored data (i.e., biometric templates), enroll an individual on each biometric device, and allow administrators to set threshold values. A threshold value indicates the level of identification the biometric device must determine for the user to pass the device. Furthermore, the device open interface has the ability to detect that the biometric device is present, signs of life readings (e.g., that a human is actually present and not a mannequin), etc.

Other open interfaces can be added as needed, including an application open interface, a database open interface and a directory open interface.

B. Preferred Implementation of the Present Invention

1. A Preferred Environment

Biometric server 104, enrollment station 106, administration station 108, alternate biometric server 110 and satellite enrollment station 112 could be implemented using computer 302 as shown in FIG. 3. Obviously, more than one of these functional components could be implemented on a single computer 302.

Computer 302 includes one or more processors, such as processor 304. Processor 304 is connected to communication bus 306. Computer 302 also includes main memory 308, preferably random access memory (RAM). Control logic 310 (i.e., software) and data 312 (such as the data stored in biometric server 104) are stored in the main memory 308, and may also be stored in secondary storage 314.

Computer 302 also includes secondary storage 314. Secondary storage 314 includes, for example, hard disk drive 316 and/or removable storage drive 318, representing a floppy disk drive, a magnetic tape drive, a compact disk drive, etc. Removable storage drive 318 reads from and/or writes to removable storage unit 320 in a well known manner.

Removable storage unit 320, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, etc. As will be appreciated, removable storage unit 320 includes a computer usable storage medium having stored therein computer software and/or data.

Computer programs (also called computer control logic) are stored in main memory 308, secondary storage 314 and/or removable storage unit 320. Such computer programs, when executed, enable computer 302 to perform the functions of the present invention as discussed herein. In particular, the computer programs, when executed, enable processor 304 to perform the functions of the present invention. Accordingly, such computer programs represent controllers of computer 302.

In another embodiment, the invention is directed to a computer program product comprising a computer readable medium having control logic (computer software) stored therein. The control logic, when executed by processor 304, causes processor 304 to perform the functions of the invention as described herein.

In another embodiment, the invention is implemented primarily in hardware using, for example, a hardware state machine. Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

Computer 302 also includes input devices 322 and display devices 324. Input devices 322 include a keyboard, a mouse, a microphone, a camera, etc. Display devices 324 include a computer monitor, a printer, a speaker, a projector, etc.

2. *A Preferred Software Programming Language and Network Architecture*

As discussed above, computer programs when executed, enable computer 302 to perform the functions of the present invention as discussed herein. In a preferred embodiment, the present invention is implemented using computer programs written in an object-oriented programming language. Object-oriented programming is a type of programming in which programmers define not only the data type of a data structure, but also the types of operations (functions) that can be applied to the data structure. In this way, the data structure becomes an object that includes both data and functions. In addition, programmers can create relationships between one object and another. For example, objects can inherit characteristics from other objects.

One of the principal advantages of object-oriented programming techniques over procedural programming techniques is that they enable programmers to create modules that do not need to be changed when a new type of object is added. A programmer can simply create a new object that inherits many of its features from existing objects. This makes object-oriented programs easier to modify. To perform object-oriented programming, one needs an object-oriented programming language (OOPL). C++ and Smalltalk are two of the more popular languages, and there are also object-oriented versions of Pascal.

While a preferred embodiment of the present invention is implemented using computer programs written in an object-oriented programming language, the present invention can also be implemented using procedural programming languages, etc.

As discussed above, one or more of computers 302 is connected by a network. A preferred embodiment of the present invention uses a type of network architecture called a peer-to-peer object architecture. Before peer-to-peer object architecture can be understood, a type of network architecture called client/server architecture must be described. Client/server architecture is a network architecture in which each computer or process on the network is either a client or a server. Servers are computers or processes dedicated to managing disk drives (file servers), printers (print servers), applications/functions or network traffic (network servers). In fact, a server is any computer or device that allocates resources for an application. Clients are personal computers or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, execution of functions and even processing power.

FIG. 4 illustrates the dynamic steps to establish communication that occur between a client and a server executing an object-oriented program. In FIG. 4A, the client has switchboard object 402 and listen object 404 waiting for a request from the server. In FIG. 4B, init object 406 determines that it needs to perform a specific task. In FIG. 4C, init object 406 creates comm object 408. Comm object 408 is used to communicate with the client. Then, comm object 408 makes a connection to listen object 404 in FIG. 4D. Once comm object 408 makes the connection, listen object 410 creates comm object 410 and relocates comm object 410 to switchboard object 402. Comm object 410 is used to communicate back to the server (i.e., between the two piers), via comm object 408.

At this point, as shown in FIG. 4F, there is two-way communication between the client and the server (i.e., between the two piers) through comm object 408 and comm object 410. Init object 406 knows which receiver object needs to be created by the client (i.e., receiving pier) to preform the specific task required. Therefore, once this communication is established, init object 406 sends a request to the client (i.e., receiving pier) to create the specific receiver object. In FIG. 4G, switchboard object 402 receives the request, via comm object 410, and creates receiver object 412. Once receiver object 412 is created, comm object 410 is relocated to receiver object 412 in FIG. 4H. Now, as shown in FIG. 4I, init object 406 and receiver object 412, via comm object 408 and comm object 410, can communicate back and forth until receiver object 412 completes the task requested by init object 406.

As stated above, a preferred embodiment of the present invention uses a type of network architecture called a peer-to-peer object architecture. A peer-to-peer object architecture is when each computer in the network has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Therefore, in a preferred embodiment of the present invention, all computers 302 can operate as either a server or a client.

As discussed above, one advantage of using an object-oriented programming language is that it allows programmers to create modules that do not need to be changed when a new type of object is added. This advantage will be further illustrated as the present invention is described in detail.

C. Biometric Server Data of the Present Invention

As stated above, biometric server 104 of FIG. 1 is the engine of biometric system 102. In fact, it is this engine that ultimately determines whether or not a user is authenticated by biometric system 102. In addition, biometric server 104 stores data accessed by biometric system 102. The data stored in biometric server 104 can be configured in one of two ways. One way is through the use of a database. The other way is through the use of a directory.

The first way that data in biometric server 104 can be configured involves the use of a database to facilitate access to the data. In general, a database is a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database is similar to an electronic filing system. To access information from a database, you need a database management system (DBMS). This is a collection of programs that enables you to enter, modify organize, and select data in a database.

Traditional databases are organized by tables, fields, records, and files. A field is a single piece of information; a record is one complete set of fields; and a file is a collection of records. For example, a telephone book is analogous to a file. It contains a list of records, each of which consists of three fields: name, address, and telephone number.

An alternative concept in database design is known as Hypertext. In a Hypertext database, any object, whether it be a piece of text, a picture, or a film, can be linked to any other object. Hypertext databases are particularly useful for organizing large amounts of disparate information, but they are not designed for numerical analysis.

The present invention may also be implemented using a standard database access method called Open DataBase Connectivity (ODBC). The goal of ODBC is to make it possible to access any data from any application, regardless of which DBMS is handling the data. ODBC manages this by inserting a middle layer, called a database driver , between an application and the DBMS. The purpose of this layer is to translate the application's data queries into commands that the DBMS understands. For this to work, both the application and the DBMS must be ODBC-compliant – that is, the application must be capable of issuing ODBC commands and the DBMS must be capable of responding to them.

The second way that data in biometric server 104 can be configured involves the use of a directory to facilitate access to the data. A preferred embodiment of the present invention utilizes a hierarchical directory called a X.500 directory. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. In addition to utilizing a X.500 directory, a Lightweight Directory Access Protocol (LDAP) may also be utilized.

LDAP is a set of protocols for accessing directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

In the following sections, the various collections of data stored in biometric server 104 are first discussed with reference to FIG. 5. Next, with reference to FIG. 6, a typical sequence of steps an administrator may take to initially setup biometric server 104 is discussed. Engine functions of biometric server 104 is discussed in Section D with reference to FIGs. 7-13.

1. Data Stored in Biometric Server

In FIG. 5, biometric server 104 (FIG. 1) stores collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. One or more unique biometric template 502 is created and stored in biometric server 104 each time a user enrolls on a different biometric device. Biometric template 502 stores the user's unique biometric measurement for a particular biometric device, which is then used to match against the user's "live" biometric measurement when the biometric device is attempting to identify the user.

Biometric policies 504 determine the method or way in which a user is to be authenticated by biometric server 104. Specific pre-defined policies provided by the present invention include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. The present invention also allows the administrator to define other biometric policies 504. The specific way in which each policy is executed is described later in detail.

Each pre-defined biometric policy 504 has a list of devices associated with it. The list of devices identifies the biometric devices that are used to execute the particular biometric policy 504. Each biometric device in the list of devices has a threshold value and a timeout value associated with it. The threshold value (e.g., false acceptance rate) indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

Each administrator defined biometric policy 504 can either have a list of biometric policies or a list of policies or devices. The list of biometric policies identifies the biometric policies that are used to execute the particular biometric policy 504. The list of policies or devices identifies the biometric policies and/or devices that are used to execute the particular biometric policy 504.

FIG. 5 illustrates that biometric groups 506 are also stored in biometric server 104. Biometric groups 506 are a logical way of combining one or more users that need access to the same set of resources. For example, all users in the accounting department of an enterprise need specific resources to perform accounting tasks. Therefore, one of biometric group 506 can be defined as "accounting group." Here, when a user is put into "accounting group," that user (once authenticated by biometric system 102) has access to the same resources as all the other users in "accounting group."

Each user can be put into one or more biometric groups 506. When the user attempts to gain access to a resource in a particular group, the user must be authenticated by whichever biometric policy 504 is associated with that particular group. When a user first attempts to log into network system 202, biometric system 102 may be implemented so that the user has a default biometric group 506 and is therefore first authenticated by the biometric policy 504 associated with the user's default biometric group 506. An example of default biometric groups 506 may be dependent on the location from which the user is attempting to gain access to network system 202. Possible different locations include from a location within network system 202 itself and from a remote location outside of network system 202.

Another way in which multiple biometric groups 506 for a single user may be implemented in biometric system 102 is to query the user for the biometric group 506 in which the user wishes to be authenticated into. An additional way is for biometric system 102 to prioritize each user's biometric groups 506. Here, if the user is authenticated by biometric system 102 into a biometric group 506 with a higher priority, then the user is automatically authentication into the user's biometric groups 506 that have a lower priority. One possible way in which the priority scheme may be implemented is to give a higher priority to biometric groups 506 that the most difficult biometric policies 504 associated with them.

A biometric device ID 508 identifies a biometric device. Each biometric device has a unique ID. Thus, the collection of biometric device IDs 508 of FIG. 5 allows the present invention to uniquely identify each biometric device in network system 102 (FIG. 2). Similarly, a user ID 510 uniquely identifies a user in network system 102.

As discussed above, various points a user may be required to be authenticated at by biometric system 102 include network system 202, one or more host computers, application 204 and/or user computer 208 of FIG. 2. Each computer 208 and application 204 within network system 202 must be registered. This registration is done by assigning unique IDs to each computer 208 and application 204, as will be discussed below. A computer ID 512 uniquely identifies each computer 208 in network system 202. Similarly, an application ID 514 uniquely identifies each application 204 in network system 202. Thus, collections of computer IDs 512 and application IDs 514 allow the present invention to uniquely identify each location in network system 120 that a user may be required to be authenticated at by biometric system 102.

2. *Setup of Biometric Server Data*

In the present invention, preferably the administrator of biometric system 102 determines the data that is stored in biometric server 104. FIG. 6 is a flowchart illustrating a typical sequence of steps an administrator may take to initially setup biometric server 104. In step 602, a unique computer ID 512 is assigned to each computer in network system 202. In step 603, a unique application ID 514 is assigned to each application in network system 202. Similarly, in step 604, a unique biometric device ID 508 is assigned to each biometric device in network system 202. Next, as shown in step 606, a determination is made as to which biometric devices will be attached to each computer 208 (FIG. 2).

In step 608, biometric groups 506 to be used within biometric system 102 are defined. In particular, the administrator defines each biometric group 504 by determining a logical grouping of resources within network system 202 that each member of that biometric group 504 will need to access. Next, in step 610, biometric policies 504 are defined. Each biometric policy 504 has associated with it a list of devices. Biometric policies 504 determine the method or way in which a user is to be authenticated by biometric server 104. One biometric policy 504 is assigned to each biometric group 506 in step 612. In step 613, one biometric policy 504 is assigned to each application ID 514.

In step 614, for every user that needs to gain access to network system 202 resources, the user is assigned a unique user ID 510. Then, each new user is put into a biometric group 506 in step 616. Once the user's biometric group 506 is determined, then in step 618, the types of devices the user needs to be enrolled in are determined by looking at the biometric policy 504 assigned to the user's biometric group 506. Once it is known which biometric policy 504 will be applied, a biometric template 502 is created for each biometric device 508 associated with the biometric policy 504 by enrolling the user in each device. This is shown in step 620. Alternatively, a biometric template 502 can be created for each biometric device within network system 202. Finally, in step 622, each computer ID 512, biometric device ID 508, biometric group 506, biometric policy 504, user ID 510, biometric template 502 and application ID 514 is stored in biometric server 104.

The steps shown in FIG. 6 can be performed in a variety of orders as should be apparent to those skilled in the art. Once biometric server 104 is setup (i.e., biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514 are all defined) the administrator interacts via a graphical user interface (GUI) to customize biometric server 104.

FIG. 14 is a sample window or screen shot generated by the GUI of the present invention. FIG. 14 illustrates the data stored in biometric server 104 as being logically stored in five tree structures (with the exclusion of application IDs 514). The five tree structures include biometric users tree 1402, biometric groups tree 1404, biometric computers tree 1406, biometric policy tree 1408 and biometric devices tree 1410. Biometric users tree 1402 includes a list of user IDs 510 registered by the administrator. As illustrated in FIG. 14, "Administrator" and "bobs" are two examples of user IDs 510. Biometric groups tree 1404 includes a list of biometric groups 506 as defined by the administrator. Examples of biometric groups include "Account Operators" and "Administrators."

Biometric computers tree 1406 includes a list of computer IDs 512. The list of computer IDs 512 represent the computers registered by the administrator. Examples of computer IDs 512 includes "BSCLAPTOP" and "BSCLAPTOP1." The fourth tree illustrated in FIG. 14 is biometric policy tree 1408. Biometric policy tree 1408 includes the list of both pre-defined and administrator-defined biometric policies 504. Pre-defined biometric policies 504 include "OR policy," "AND policy," "CONTINGENT policy," "RANDOM policy" and "THRESHOLD policy." Finally, biometric devices tree 1410 includes a list of biometric device IDs 508 registered by the administrator. Examples of biometric device IDs include "BSC Password Device" and "Visionics FaceIt."

An additional tree structure not shown in FIG. 14 is an application tree. As discussed above, a user may be required to be authenticated if the user attempts to access a particular application associated with a biometric policy 504. Although an application tree is not shown in the sample window of FIG. 14, the GUI of the present invention may be modified to include not only an application tree, but any other type of tree the administrator may deem to be desirable.

The present invention also allows for an administrator to define information groups. Information groups are a logical way of combining users that need access to the same types of information within each application in network system 202. For example, one possible type of application within network system 202 is a database containing information about each user. The administrator of biometric system 102 may determine that only the human resource department should have access to user medical information. Here, one information group can be defined as "medical information." The users put into "medical information" are only those users in the human resource department. Therefore, a biometric policy 504 can be associated either directly with an application ID or with an information group to authenticate users prior to allowing them access to information in applications.

The present invention, through the use of the GUI, is preferably implemented as a "drag and drop" application. "Drag and drop" applications allow an administrator to drag objects to specific locations on the screen to perform actions on them. For example, in the Macintosh environment, you can drag a document to the trashcan icon to delete it. This is a classic case of "drag and drop" functionality. When implemented well, drag-and-drop functionality is both faster and more intuitive than alternatives, such as selecting options from a menu or typing in commands. Nevertheless, the present invention is not limited to being implemented as a "drag and drop" application.

Referring back again to FIG. 14, an example of "drag and drop" functionality is the ability of the administrator to drag the "OR Policy" to the "Administrators" biometric group to either define or redefine the policy for that group. Another example includes dragging user ID "Administrator" to the "Administrators" biometric group. Now, the user who has user ID "Administrator" must pass the "OR Policy" to be authenticated by biometric system 102 (FIG. 1).

The administrator may also drag a biometric policy 504 to an application ID 514 (not shown in FIG. 14). For example, if the administrator drags the "AND Policy" to a particular application ID, then every user who attempts to access the application that the application ID is assigned to must pass the "AND Policy." Thus, the present invention provides different levels of authentication granularity. For example, a particular user may be assigned to a biometric group 506 that allows access to a spreadsheet if the user passes two biometric devices. However, to gain access to a payroll application, the user must also pass a third biometric device. Users that are not members of the biometric group 506 do not even have the opportunity to access the payroll application. The present invention provides complete flexibility to protect network resources.

As mentioned above in reference to FIG. 6, in step 620, a biometric template 502 is created for the user for each biometric device that is determined to be in the list of devices associated with a biometric policy 504 that is further associated with the user's biometric group 506. Therefore, there is a possibility that a user may not be enrolled in a particular biometric device that the user is required to pass in order to gain access to a particular application. This situation occurs when the biometric policy 504 that is assigned to the user's biometric group 506 and the biometric policy 504 that is assigned to the application ID 514 have different biometric devices in their list of devices. One way to avoid such a situation is to enroll the user with every biometric device in biometric system 102 and not just with the biometric devices that are determined to be in the biometric policy 's 504 list of devices that is associated with the user's biometric group 506. As illustrated above, various duties exist within biometric system 102. The discussion above infers that it is the administrator who performs all of these duties. In actuality, these duties can be delegated to multiple people having different positions within biometric system 102 (FIG. 1). These positions can include an administrator (with limited duties from the ones described above), a biometric policy manager, a device hardware and software manager and an enrollment manager. The administrator has actual administrative privileges within biometric system 102. The actual duties of the administrator could be limited to the adding and deleting of users, biometric groups 506 (FIG. 5), computers 208 (FIG. 2) and applications 204 (FIG. 2) with biometric system 102. Another position within biometric system 102 is the biometric policy manager. This position is akin to a security officer. The biometric policy manager is responsible for defining biometric policies 504 and attaching them to both biometric groups 506 and application IDs 514. The biometric policy manager would also be responsible for the combinations of biometric devices and for the strength of the threshold value associated with each biometric device.

Another position within biometric system 102 is a device hardware and software manager. This person is responsible for managing the software and hardware for biometric devices within biometric system 102. The device hardware and software manager will install the biometric devices, keep the versions up to date and maintain the devices. The final position is an enrollment manager. This person is given the ability to enroll users onto biometric system 102. Responsibility includes taking the new users through the process of enrolling for the different devices. The enrollment manager is generally a nontechnical person working in the human resource department of an enterprise. For simplicity, the following discussion will refer only to an administrator. It should be understood that the administrator may be one person performing one, all, or any number of the positions described above.

D. Biometric Server Functions of the Present Invention

In one embodiment of the present invention, biometric server 104 is implemented as computer 302 operating as described in reference to FIG. 3 above. Computer 302 executes computer programs to enable it to perform the functions of the present invention. Thus, biometric server 104 executes computer programs to perform its functions. As discussed above, the computer programs executed by biometric server 104 are preferably written in an object-oriented programming language and executed in a peer-to-peer object architecture.

An advantage of any object-oriented program, and thus also with computer programs executed by biometric server 104, is that they enable programmers to create modules that do not have to be changed when a new type of object is added. An object includes both the data and functions required to perform a task. Thus, by implementing the functions to be performed by biometric server 104 as objects, created modules do not need to be changed when a new type of object (or function) is added. This implementation of the present invention reduces complexity and thus increases efficiency. This interchangeability of functions (implemented as objects) of the present invention is explained in more detail in reference to FIGs. 7, 8, 12 and 13 below.

Described above with reference to FIG. 4, is the dynamic steps involved in establishing communication between a client and a server executing an object-oriented program. As biometric server 104 of the present invention executes its various functions, the same dynamic steps involved in communication between the server and client occur for each function as shown in FIGs. 4A through 4I. FIG. 4 shows a generic init object 406 and a generic receiver object 412. As is shown in FIGs.7 and 12, for each type of function performed by biometric server 104, init object 406 and receiver object 412 are replaced by specific init and receiver objects that perform their specific functions.

The types of functions performed by biometric server 104, through the execution of computer software, includes authenticating a user and enrolling a user. For simplicity, the figures used to illustrate the individual functions of biometric server 104 do not include switchboard object 402 and listen object 404 of FIG. 4.

1. Authenticating a User

FIG. 7 is a block diagram of the objects involved in authenticating a user of the present invention. As described above, a peer-to-peer object architecture is when each computer in the network has equivalent capabilities and responsibilities (e.g., a single computer can perform as a server and then at other times perform as a client). This allows for each computer in the network to initiate communication with any other computer in the network. FIG. 7 includes biometric server 104 (FIG. 1), computer 208 (or alternatively remote/web computer 210, both from FIG. 2), authentication interface 704, authentication interface 706, authentication object 708, database object 710, policy object 712, comm object 716, comm object 718, authentication object 720 and biometric device object 722. Here, biometric server 104 is performing as the server and computer 208 is performing as the client.

It is important to note that authentication interface 704 and authentication interface 706 are not part of the present invention. In fact, authentication interface 704 and authentication interface 706 are specific to the particular operating system and/or application the present invention is interfacing with. In general, operating systems provide a software platform on top of which other programs, called applications, can run. Applications must be written to run on top of a particular operating system. The choice of operating system, therefore, determines to a great extent the applications that can be run. Examples of operating systems include Windows NT, UNIX and Solaris. The present invention interfaces with the applicable operating system through application interface 706.

Authentication object 708 replaces init object 406 (FIG. 4). Authentication object 708 is used to request computer 208 to authenticate a user. Comm object 716 is attached to authentication object 708 and replaces comm object 408 (FIG. 4). Authentication object 708 and authentication object 720 communicate, via comm object 716 and comm object 718.

Policy object 712 is also attached to authentication object 708. Policy object 712 differs depending on the specific biometric policy 504 (FIG. 5). As discussed above, it is biometric policy 504 (FIG. 5) that determines the method or way in which a user is to be authenticated by biometric server 104. It is important to note that a user is not authenticated until he or she passes biometric policy 504. In the present invention, a user is never authenticated by solely passing one or more biometric devices without also passing his or her biometric policy 504. The type of communication between authentication object 708 and authentication object 720 is very dependent on the particular biometric policy 504 being used to authenticate the user.

In FIG. 7, database object 710 stores the data described above in reference to FIG. 5. The data includes collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. Authentication object 720 replaces receiver object 412 (FIG. 4). Authentication object 720 is used to perform the specific task requested by authentication object 708. Comm object 718 replaces comm object 410 (FIG. 4). Finally, biometric device object 722 is used to identify the user by determining if the user passes the biometric device. Biometric device object 722 differs depending on what biometric device the user is attempting to pass.

FIGs. 8A and 8B present a flowchart depicting the high-level operation of the objects in FIG. 7. In step 802, a user is at computer 208 and types in user ID 510 (FIG. 5) given to him or her by the administrator. Authentication interface 704 recognizes this as a login request. As mentioned above, to facilitate user access, each computer 208 provides an interface for users to be authenticated by biometric system 102 (FIG. 1). This interface is authentication interface 704. In step 804, authentication interface 704 sends the login request, which includes a computer ID 512 (FIG. 5) and user ID 510, to biometric server 104. Application interface 706 actually receives the login request. Based on the fact that the request is one for login, authentication object 708 gets initialized in step 806 (e.g., the login request starts the engine in biometric system 102). Prior to authentication object 708 being initialized, it is a generic init object 406 as described in reference to FIG. 4.

In step 808, authentication object 708 creates database object 710 and passes user ID 510 to it. Based on user ID 510, database object 710 determines the user's biometric group 506 (FIG. 5) in step 810. As described previously, the administrator has already determined which biometric group 506 the user is in. Based on biometric group 506, database object 710 determines the biometric policy 504 (FIG. 5) that is assigned to biometric group 506.

In step 811, database object 710 determines whether the required biometric templates 502 (FIG. 5) for the user are stored in biometric object 710 to execute the user's biometric policy 504. In addition, database object 710 also determines if computer 208 has the required biometric devices attached to it to execute the user's biometric policy 504. If the required biometric templates 502 or the required biometric devices do not exist, then control transfers to step 836. In step 836, biometric server 104 communicates, via authentication interface 706 and authentication interface 704, to computer 208 that the user cannot be authenticated. Authentication interface 704 then denies the user access. At this point the flowchart in FIGs. 8A and 8B ends. Alternatively, if in step 811 the required biometric templates 502 and the required biometric devices do exist, then control transfers to step 812.

In step 812, database object 710 creates policy object 712 and relocates policy object 712 to authentication object 708. Policy object 712 knows the specific type of biometric policy 504 (e.g. OR policy, AND policy, etc.), the list of devices for biometric policy 504 and the required biometric templates 502. There is one biometric template 502 for each biometric device ID (FIG. 5) 508 listed in the list of devices. Each biometric template 502 contains the user's stored biometric data to be used in testing the user on a particular biometric device. In addition, each biometric device in the list of devices has associated with it a threshold value and a timeout value. As explained above, the threshold value indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

In step 814, communication is established between biometric server 104 and computer 208. This communication is established exactly as described in reference to FIG. 4. In step 816, based on biometric policy 504 and its list of devices, authentication object 708 sends a request to computer 208 to test the user on a particular biometric device. The request includes biometric device ID

508, biometric template 502, the threshold value and the timeout value. Biometric template 502, the threshold value and the timeout value are all determined by user ID 510 and biometric device ID 508.

In step 818, based on the request, authentication object 720 is created. In step 820, authentication object 720 looks at biometric device ID 508 and creates biometric device object 722. Authentication object 720 then passes to biometric device object 722 biometric template 502, the threshold value and the timeout value. In step 822, biometric device object 722 tests the user on the specific biometric device and returns the results to authentication object 720. The results include a score and whether the user passed or failed the biometric device. Authentication object 720 then sends the results back to authentication object 708 in step 824, via comm object 718 and comm object 716.

In step 826, authentication object 708 looks at both the results and policy object 712 and determines whether the user passed biometric policy 504, failed biometric policy 504 or needs to be tested on another biometric device. Policy object 712 determines how many different biometric devices the user needs to be tested on. In step 828, if the user passed biometric policy 504, then control transfers to step 830. In step 830, the fact that the user passed biometric policy 504 is communicated, via authentication interface 706 and authentication interface 704, to computer 208. Authentication interface 704 then allows the user access to enterprise resources. Alternatively, if in step 828, the user did not pass biometric policy 504, then control transfers to step 832.

In step 832, if the user failed biometric policy 504, then control transfers to step 834. In step 834, the fact that the user failed biometric policy 504 is communicated, via authentication interface 706 and authentication interface 704, to computer 208. Authentication interface 704 then denies the user access to enterprise resources. Alternatively, if in step 832, the user did not fail biometric policy 504, then control transfers to step 836. In step 836, the next biometric device to test the user on is determined and another request is sent to authentication object 720. At this point control returns to step 820 and the user gets tested on the next biometric device. The flowchart in FIG. 8 continues until the user either passes or fails biometric policy 504.

Step 822 of FIG 8. is further explained in FIG. 9. FIG. 9 is a flowchart illustrating the typical operation of a biometric device as it tests a user. In step 902, the biometric device receives a request to test a user. The request includes the user's biometric template 502, a threshold value and a timeout value. Again, the threshold value and timeout value are user ID 510 and biometric device ID 508. In step 904, the biometric device prompts the user for "live" biometric data. In step 906, the biometric device attempts to read the "live" biometric data.

The biometric device, in step 908, determines whether or not the biometric data has been read. As discussed above, if the environment is not conducive for reading the particular biometric measurement (e.g., the environment has poor lighting and the biometric device is trying to read facial image data), then the biometric device may not be able to read the "live" biometric data. If the "live" biometric data has not been read in step 908, then in step 910, the actual time the biometric device has attempted to read the "live" biometric data is compared to the timeout value. If the actual time is greater than or equal to the timeout value, then control transfers to step 912 and the user fails the biometric device. Alternatively, if the actual time is less than the timeout value, then control transfers back to step 906 and the biometric device attempts to read the "live" biometric data again. This loop continues until either the "live" biometric data has been read or the actual time is greater than or equal to the timeout value (i.e., the time expires to read the "live" biometric data).

In step 908, if the "live" biometric data has been read, then control transfers to step 914. In step 914, a score is determined by matching the "live" biometric data with the data stored in biometric template 502. In step 916, the score determined by step 914 is compared to the threshold value. If the score is greater than or equal to the threshold value, then control transfers to step 918. In step 918, the user passes the biometric device and the flowchart in FIGs. 8A and 8B ends. Alternatively, in step 916, if the score is less than the threshold value then control passes to step 920. In step 920, the actual time is once again compared to the timeout value. If the actual time is greater than or equal to the timeout value, then control transfers to step 922 and the user fails the biometric device. At this point the flowchart in FIG 9 ends. If the actual time is less than the timeout value, then control transfers back to step 906 and the device attempts again to read the "live" biometric data.

The process described above to authenticate a user shows biometric template 502 being matched on the client side (i.e., at computer 208). While this is a preferred embodiment of the present invention, it is important to recognize that biometric template 502 can just as easily be matched on the server side (i.e., at biometric server 104).

As pointed out above, it is the login request that starts the engine in biometric system 102 to authenticate a user. The login request is initiated by a user typing in a user ID 510 (FIG. 5). In another embodiment of the present invention, it is "live" biometric data that identifies the user and starts the engine in biometric system 102 to authenticate a user. FIG. 10 is a block diagram of the objects involved in starting the authentication process of the present invention with "live" biometric data. FIG. 10 includes computer 208 (or alternatively remote/web computer 210, both from FIG. 2), monitor object 1004, biometric device object 1006, identify user ID object 1008 and database object 1010.

Monitor object 1004 is provided by the present invention for each computer 208 in the enterprise where the administrator desires to have "live" biometric data start off the engine in biometric system 102 to authenticate a user. Monitor object 1004 is up and waiting for "live" biometric data to be presented. In addition, monitor object 1004 is specialized (e.g., a fingerprint monitor object waits for "live" fingerprint data and a facial image monitor object waits for "live" facial image data).

FIG. 11 presents a flowchart depicting the high-level operation of the objects in FIG. 10. In step 1102, monitor object 1004 is waiting for "live" biometric data to be presented. In step 1104, once "live" biometric has been presented, monitor object 1004 creates biometric device object 1006. Because monitor object 1004 is specialized, there is no need for monitor object 1004 to be aware of any biometric device IDs 508 (FIG. 5). In step 1106, biometric device object 1006 causes a biometric device to read the "live" biometric data. This "live" biometric gets returned to monitor object 1004.

In step 1108, monitor object 1004 sends an identify request to identify user ID object 1008. The identify request includes the "live" biometric data and computer ID 512 (FIG. 5). The "live" biometric data is used to to identify user ID object 1008 on biometric server 104 (FIG. 1). Computer ID 512 uniquely identifies computer 208. Although not illustrated in FIGs. 10 and 11 for simplicity reasons, the same steps in establishing communication between objects must occur as shown in FIG. 4. In step 1110, identify user ID object 1008 creates a database object 1010 and passes to it the "live" biometric data. Database object 1010 contains the same data as described in reference to database object 710 in FIG. 7. In step 1112, an attempt is made to match the "live" biometric data with biometric data stored in a biometric template 502 (FIG. 5).

In step 1114, if a match was successful, then control transfers to step 1116. In step 1116, the user ID 510 (FIG. 5) that belongs to the matching biometric template 502 is determined. In step 1118, once user ID 510 is determined, then the authentication process proceeds as described in step 804 in FIG. 8. If in step 1114 a match was not successful, then control transfers to step 1120. In step 1120, the user is prompted to present "live" biometric data and control transfers back to step 1102. Because monitor object 1004 is always waiting for "live" biometric data to be presented, it does not matter if the same user presents the next "live" biometric data. Each time "live" biometric data is presented to monitor object 1004, it does not distinguish it from previously presented "live" biometric data.

2. *Enrolling a User*

As stated above, one of the advantages of object-oriented programming techniques over procedural programming techniques is that they enable programmers to create modules that do not need to be changed when a new type of object is added. This advantage is illustrated in FIG. 12. FIG. 12 is a block diagram of the objects involved in the enrollment process of the present invention. FIG. 12 includes biometric server 104 (FIG. 1), enrollment interface 1206, enrollment object 1208, comm object 1214, policy object 1212, database object 1210, enrollment station 106 (FIG. 1), enrollment interface 1204, enrollment object 1220, comm object 1218 and biometric device object 1222. Here, biometric server 104 is performing as the server and enrollment station 106 is performing as the client.

Enrollment station 106 is used to enroll users into biometric system 102. Enrollment station 106 has attached to it every type of biometric identification device used by biometric system 102 to identify and ultimately authenticate users.

It is important to note that enrollment interface 1204 and enrollment interface 1206 are not part of the present invention. In fact, enrollment interface 1204 and enrollment interface 1206 are specific to the particular operation system the present invention is interfacing with.

Enrollment object 1208 replaces init object 406 (FIG. 4). Enrollment object 1208 is used to request enrollment station 106 to enroll a user on a biometric device. Comm object 1214 is attached to enrollment object 1208 and replaces comm object 408 (FIG. 4). Enrollment object 1208 and enrollment object 1220 communicate, via comm object 1214 and comm object 1218.

Policy object 1212 is also attached to enrollment object 1208. Policy object 1212 is the same as policy object 712 (FIG. 7). As discussed above, it is the policy that determines the method or way in which a user is to be authenticated by biometric server 104. Database object 1210 stores the same data as database object 710 as described in reference to FIG. 7. Enrollment object 1220 replaces receiver object 412 (FIG. 4). Enrollment object 1220 is used to perform the specific task in enrolling a user on a biometric device. Comm object

1218 replaces comm object 410 (FIG. 4). Finally, biometric device object 1222 is used to enroll the user by requesting multiple samples of a particular type of "live" biometric data from the user. Biometric device object 1222 uses the samples of biometric data to create an unique biometric template 502 (FIG. 5) for the user.

FIG. 13 presents a flowchart depicting the high-level operation of the objects in FIG. 12. In step 1302, a user is at enrollment server 106 and types in user ID 510 (FIG. 5) given to the user by the administrator. Enrollment interface 1204 recognizes this as an enrollment request. To facilitate user enrollment, enrollment station 106 provides an interface for users to be enrolled by biometric system 102 (FIG. 1). This interface is enrollment interface 1204. In step 1304, enrollment interface 1204 sends an enrollment request, which includes computer ID 512 (FIG. 5) and user ID 510, to biometric server 104. Enrollment interface 1206 actually receives the enrollment request. Based on the fact that the request is one for enrollment, enrollment object 1208 gets initialized in step 1306 (e.g., the enrollment request starts the engine in biometric system 102). Prior to enrollment object 1208 being initialized, it is generic init object 406 as described in reference to FIG. 4.

In step 1308, enrollment object 1208 creates database object 1210 and passes user ID 510 to it. Based on user ID 510, database object 1210 determines the user's biometric group 506 (FIG. 5) in step 1310. As described previously, the administrator has already determined which biometric group 506 the user is in. Based on biometric group 506, database object 1210 determines the biometric policy 504 (FIG. 5) that is assigned to biometric group 506.

In step 1312, database object 1210 creates policy object 1212 and relocates policy object 1212 to enrollment object 1208. Policy object 1212 knows the specific type of biometric policy 504 (e.g. OR policy, AND policy, etc.) and its list of devices for that biometric policy 504. In step 1314, communication is established between biometric server 104 and enrollment station 106. This communication is established exactly as described in reference to FIG. 4. In step

1316, based on the list of devices, enrollment object 1208 sends a request to enrollment station106 to test the user on a particular biometric device. The request includes biometric device ID 508 (FIG. 5) that identifies the particular biometric device the user is to be enrolled in.

In step 1318, based on the request, enrollment object 1220 is created. In step 1320, enrollment object 1220 looks at biometric device ID 508 and creates biometric device object 1222. Biometric device object 1222 causes the biometric device to enroll the user in step 1322. In particular, the user is asked to give biometric measurements a few different times. For example, the user may be asked to give multiple fingerprint measurements for each finger. The enrollment of a user in a device creates a biometric template 502 (FIG. 5). In step 1324, enrollment object 1220 sends biometric template 502 to enrollment object 1208, via comm object 1218 and comm object 1214. Then, in step 1326, enrollment object 1208 stores biometric template 502 in database object 1210.

In step 1328, it is determined based on the list of devices, if the user needs to be enrolled in another biometric device. Although the user should at least be enrolled in the biometric devices listed in his or her list of devices, the administrator can decide to enroll the user in a biometric device not listed in the list of devices. If in step 1328, it is determined the user does not need to be enrolled in another biometric device, then control transfers to step 1330 and the flowchart in FIG. 13 ends. Alternatively, if the user does need to be enrolled in another biometric device, then control transfers to step 1332. In step 1332, the next biometric device to enroll the user in is determined and a request is sent to enrollment object 1220. The request includes biometric device ID 508 for the next biometric device. Control transfers again to step 1320. This process continues until the user is enrolled in all the required biometric devices.

As described with reference to FIGs. 12 and 13, in one embodiment of the present invention the user is enrolled through enrollment station 106. Typically, enrollment station 106 and the administrator are physically located at the same location within the enterprise. When a new user needs to enroll into the resource protection system, it may not be convenient for that user to physically be at the same location as administration. This presents two additional limitations for networked environments.

The first limitation deals with the use of any identification device. To enroll a user into biometric system 102 (FIG. 1) an administrator needs to be sure that the user enrolling is really the right person. This is difficult to do when the user and administrator are not physically at the same location.

The second limitation deals with the use of biometric identification devices. Many biometric measurements change over time. For example, people grow older, lose or gain weight, etc. In the case of biometric templates storing a user's facial image, the biometric data in the template may need to be updated from time to time. Once again, if the user and administrator are not physically at the same location in the network, the administrator needs to be sure the user requesting to update a template is really the person he or she says.

The inventors of the present invention recognized that what is needed is a scheme for remotely authenticating a user prior to allowing that user to either enroll or re-enroll with a particular biometric device to update a biometric template. Remote enrollment and/or re-enrollment (refreshing of biometric templates) can be either initiated by the administrator or the user.

There are several scenarios of where remote enrollment and/or re-enrollment is used. The first scenario already mentioned above is when the administrator and the user desiring to be enrolled or re-enrolled in biometric system 102 are not physically at the same location in the network. The administrator still needs to authenticate the user first. There are at least two possible solutions to this problem. The first involves assigning a temporary password (or token or smart card) to the user. The user goes to one of remote/web computers 210 (FIG. 2) and types in the password. Once biometric system 102 authenticates the user by the password, then the user starts the enrollment process. Of course, the temporary password expires after one use. In the case of re-enrollment (refreshing of templates) if the user is currently enrolled in multiple biometric devices, then one of the other biometric devices can be used to authenticate the user prior to allowing the user to refresh a biometric template 502 (FIG. 5) on the desired biometric device.

The second solution for remote enrollment and/or re-enrollment takes advantage of the fact that certain biometric devices are attached to remote/web computer 210. Several examples involve the use of facial image and voice recognition biometric devices. If an administrator is familiar with how the user looks, then the administrator can use video conferencing to authenticate the user prior to allowing the enrollment process to begin. If an administrator is familiar with the user's voice, then a voice recognition device can be used to speak to the administrator to authenticate the user.

A second scenario is when an enterprise desires not to use an administrator to enroll users into biometric system 102. Here, if the enterprise has an existing non-biometric identification system in place, it is easy to changeover from its existing system to biometric system 102. What is important to note is that the integrity of the existing non-biometric identification system must not be in question. For instance, if User B has access to another User A's password, then User B can enroll into biometric system 102 and gain access to User A's resources. Assuming the integrity of the existing identification system is good, then the method of authentication of the existing identification system is used to introduce the user to biometric system 102. Once the user is introduced to biometric system 102, the user can no longer gain access to enterprise resources through the old method. This is also important because it provides flexibility in rolling out biometric system 102 by not having to enroll all users at the same time.

E. Biometric Policies

The inventors of the present invention recognized a limitation when identification devices are used in any environment, whether or not the environment is networked. Enterprises with many resources have the desire to protect some resources more than others. For example, an enterprise may not care if its electronic bulletin board is accessed by every user in the enterprise. Whereas, an enterprise may want only the enterprise president to access merger and acquisition information. If an enterprise applies the same level of protection to all its resources, then one of two scenarios will occur. The first scenario is applying a lower-end level of protection to all resources. Here the result is inadequate authentication to some network resources. The second scenario is applying a higher-end level of protection to all resources. While this scenario may adequately protect all resources in the network, it would make the administration of resource protection more complex and thus decrease network productivity.

Biometric policies 504 (FIG. 5) of the present invention provides the flexibility to apply the appropriate level of protection to each network resource without decreasing network productivity. As discussed above, it is the biometric policies 504 of the present invention that determine the method or way in which a user is to be authenticated by biometric server 104 (FIG. 1). It is important to note that a user is not authenticated until he or she passes a biometric policy 504. In the present invention, a user is never authenticated by solely passing one or more biometric devices without the user also passing his or her biometric policy 504.

The specific way in which biometric policies 504 provide flexibility to the level of protection for each resource is through the layering of identification devices, including both biometric and non-biometric devices. The layering of identification devices allows the administrator of biometric system 102 (FIG. 1) to combine one or more identification devices in a logical way to protect each resource. Layering also allows the administrator to adjust the level of identification each biometric device must determine in order for the user to pass the biometric device. This is accomplished through threshold values as described above.

FIG. 15 is a chart illustrating an example of the layering process of biometric system 102 for a particular enterprise. Chart 1502 has columns and rows. Users can be required to be authenticated by biometric system 102 when they try to access various points in network system 202. The columns of chart 1502 represent the various points in network system 202. The various points (in this particular enterprise) include network system 202 itself, one or more of applications 204, one or more of user computers 208, Internet access 1504 and dial-in access 1506. The rows in chart 1502 represent the identification devices used in biometric system 102. The identification devices include both biometric and non-biometric devices. Non-biometric devices (in this particular enterprise) include password and smart card devices. Biometric devices (in this particular enterprise) include fingerprint, voice recognition, facial image and signature.

Once the administrator identifies the various points in network system 202 that require protection and the identification devices, the administrator determines the layering process of the present invention. The layering process for a single resource can include the steps illustrated by FIG. 16.

FIG. 16 is a flowchart that illustrates the process of layering for a single resource of the present invention. In step 1602, a resource in network system 202 that requires protection is identified. In step 1604, the non-biometric devices that are going to be utilized in protecting the resource are identified. Here, the administrator may decide to not use any non-biometric devices. In step 1606, the biometric devices that are going to be utilized in protecting the resource are identified. Again, the administrator may decide to use zero, one or more of the biometric devices. Finally, in step 1608, for each identified biometric device its threshold value is determined. Chart 1502 (FIG. 15) illustrates the possible values of threshold value as being L (low), M (medium) and H (high). The present invention is not limited to representing the values of threshold values this way. In fact, possible values of threshold values can be represented in other ways. One possible way is numerically where the threshold value can have as many different values as the administrator desires.

Referring again to FIG. 15, network system 202 is protected by two biometric devices and no non-biometric devices. The two biometric devices include a fingerprint device and a voice recognition device. Fingerprint device's threshold value is set at M. Voice recognition device's threshold value is set at L. Therefore, for a user to access network system 202, the user might *potentially* be tested on both a fingerprint device and a voice recognition device. When tested, the user might have to pass the fingerprint device with at least a M threshold value and pass the voice recognition device with at least a L threshold value.

The reason why the user might only *potentially* be tested on both devices is because ultimate authentication into biometric system 102 is governed by biometric polices 504. For example, an OR biometric policy would only require the user from above to pass either the fingerprint device or the voice recognition device. The only way the user will be tested on both devices is if the user fails the first device tested on. An AND biometric policy requires the user to be tested on both biometric devices to be authenticated. But even with the AND biometric policy the user may be tested on one of the biometric devices. If the user fails the first biometric device tested on, then the user automatically fails the AND policy and there is no need to test the user on the second biometric device.

Although biometric policies 504 have been introduced above, this section explains in detail the various pre-defined biometric policies and administrator-defined policies provided by the present invention. As explained above, each biometric policy has a list of devices associated with it. The list of devices identifies the biometric devices that are used to execute the biometric policy. Each biometric device in the list of devices has a threshold value and a timeout value associated with it. The threshold value indicates the level of identification the biometric device must determine for the user to pass the device. The timeout value indicates the time in which the biometric device has to identify the user to the level of identification indicated by the threshold value.

As stated above, the present invention not only provides specific pre-defined biometric policies but also allows the administrator to define other administrator-defined policies. The specific pre-defined biometric polices include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy. The pre-defined biometric policies are limited to having only biometric devices in their list of devices. This limits being able to use non-biometric devices to protect a resource. Therefore, the present invention also provides administrator-defined policies having a list of policies or devices. An additional administrator-defined type of policy includes biometric policies within a policy. Described in detail below, are the pre-defined biometric policies and the administrator-defined policies.

1. OR Policy

The user passes an OR policy of the present invention if the user passes one of the biometric devices in the list of devices. FIG. 17 is a flowchart illustrating the steps involved in executing the OR policy of the present invention. In step 1702, the n number of biometric devices in the list of devices greater than two is determined. An OR policy will typically have at least two different biometric devices in its list of devices. In step 1704, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1706. In step 1708, the first score is compared to a first biometric device threshold value. If the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1710. In step 1710, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1708 the first score is less than the first biometric device threshold value, then control transfers to step 1712.

In step 1712, the second biometric device in the list of devices is determined. Once the second biometric device is determined, the user is tested on the second biometric device to produce a second score in step 1714. In step 1716, the second score is compared to a second biometric device threshold value.

If the second score is greater than or equal to the second biometric device threshold value, then control transfers to step 1718. In step 1718, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1716 the second score is less than the second biometric device threshold value, then control transfers to step 1720.

In step 1720, if n is not greater than zero, then control transfers to step 1722. If control transfers to step 1722 it means that the list of devices has only two biometric devices in it and the user has failed both biometric devices. In step 1722, the user has failed the OR policy and the flowchart in FIG. 17 ends. Alternatively, if in step 1720 n is greater than zero, then control transfers to step 1724. In this situation the list of devices has more than two biometric devices in it. In step 1724, the next biometric device is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 1726. In step 1728, the next score is compared to a next biometric device threshold value. If the next score is greater than or equal to the next biometric device threshold value, then control transfers to step 1730. In step 1730, the user has passed the OR policy and the flowchart in FIG. 17 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1728 the next score is less than the next biometric device threshold value, then control transfers to step 1732.

In step 1732, one is subtracted from n and control returns to step 1720. In step 1720, if n is not greater than zero then the user has failed all the biometric devices in the list of devices. Here, control transfers to step 1722. In step 1722, the user has failed the OR policy and the flowchart in FIG. 17 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1720 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 17 continues until the user has either failed all the biometric devices or the user passes one biometric device in the list of devices.

Although the OR policy will typically have at least two different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the OR policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the OR policy by being tested on the fingerprint device with the left index finger and by being tested on the fingerprint device with the right index finger. The user only needs to pass the fingerprint device using one of the biometric measurements to pass the OR policy. Other single biometric devices that can be used to test multiple biometric measurements are facial image (different angles of a face), retina image (right and left retina), hand geometry (right and left hand), voice recognition (two different phrases), different lighting (visible and infra red), etc.

2. *AND Policy*

The user passes an AND policy of the present invention if the user passes all of the biometric devices in the list of devices. FIG. 18 is a flowchart illustrating the steps involved in executing the AND policy of the present invention. In step 1802, the n number of biometric devices in the list of devices greater than two is determined. An AND policy will typically have at least two different biometric devices in its list of devices. In step 1804, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1806. In step 1808, the first score is compared to a first biometric device threshold value. If the first score is less than the first biometric device threshold value, then control transfers to step 1810. In step 1810, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1808 the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1812.

In step 1812, the second biometric device in the list of devices is determined. Once the second biometric device is determined, the user is tested on the second biometric device to produce a second score in step 1814. In step 1816, the second score is compared to a second biometric device threshold value. If the second score is less than the second biometric device threshold value, then control transfers to step 1818. In step 1818, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1816 the second score is greater than or equal to the second biometric device threshold value, then control transfers to step 1820.

In step 1820, if n is not greater than zero, then control transfers to step 1822. If control transfers to step 1822 it means that the list of devices has only two biometric devices in it and the user has passed both biometric devices. In step 1822, the user has passed the AND policy and the flowchart in FIG. 18 ends. Alternatively, if in step 1820 n is greater than zero, then control transfers to step 1824. In this situation the list of devices has more than two biometric devices in it. In step 1824, the next biometric device is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 1826. In step 1828, the next score is compared to a next biometric device threshold value. If the next score is less than the next biometric device threshold value, then control transfers to step 1830. In step 1830, the user has failed the AND policy and the flowchart in FIG. 18 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1828 the next score is greater than or equal to the next biometric device threshold value, then control transfers to step 1832.

In step 1832, one is subtracted from n and control returns to step 1820. In step 1820, if n is not greater than zero then the user has passed all the biometric devices in the list of devices. Here, control transfers to step 1822. In step 1822, the user has passed the AND policy and the flowchart in FIG. 18 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 1820 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 18 continues until the user has either passed all the biometric devices or the user fails one biometric device in the list of devices.

Although the AND policy will typically have at least two biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the AND policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the AND policy by being tested on the fingerprint device with the left index finger and by being tested on the fingerprint device with the right index finger. The user needs to pass the fingerprint device using both of the biometric measurements to pass the AND policy. As mentioned above with the OR policy, the other single biometric devices can also be used with the AND policy to test multiple biometric measurements.

3. CONTINGENT Policy

The user passes a CONTINGENT policy of the present invention if either the user exceeds a minimum threshold (i.e., a first biometric device threshold value) associated with a first biometric device or if the user exceeds a contingent threshold associated with the first biometric device and the user exceeds a minimum threshold (i.e., a contingent biometric device threshold value) associated with a contingent biometric device. FIG. 19 is a flowchart illustrating the steps involved in executing the CONTINGENT policy of the present invention. The are typically two different biometric devices in the list of devices for the CONTINGENT policy. In step 1902, a contingent threshold value is determined. In step 1904, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 1906.

In step 1908, the first score is compared to a first biometric device threshold value. If the first score is greater than or equal to the first biometric device threshold value, then control transfers to step 1910. In step 1910, the user has passed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 1908 the first score is less than the first biometric device threshold value, then control transfers to step 1912.

In step 1912, the first score is compared to the contingent threshold value. In step 1912, if the first score is less than the contingent threshold value, then control transfers to step 1914. In step 1914, the user has failed the CONTINGENT policy. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1912 the first score is greater than or equal to the contingent threshold value, then control transfers to step 1916. The contingent threshold value is used to give the user a second chance to pass the CONTINGENT policy and thus be authenticated by biometric system 102.

In step 1916, the contingent biometric device in the list of devices is determined. The type of biometric device selected for the contingent biometric device may be based environmental conditions as discussed above. Once the contingent biometric device is determined, the user is tested on the contingent biometric device to produce a contingent score in step 1918. In step 1920, the contingent score is compared to a contingent biometric device threshold value. If the contingent score is less than the contingent biometric device threshold value, then control transfers to step 1924. In step 1924, the user has failed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 1920 the contingent score is greater than or equal to the contingent biometric device threshold value, then control transfers to step 1922. In step 1922, the user has passed the CONTINGENT policy and the flowchart in FIG. 19 ends. At this point the user has been authenticated by biometric system 102.

Although the CONTINGENT policy will typically have two biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with multiple biometric measurements to pass the CONTINGENT policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the CONTINGENT policy by being tested on the fingerprint device with the user's left index finger first. If the user passes the fingerprint device with his or her left index finger, then the user passes the CONTINGENT policy. If the user fails the fingerprint device with his or her left index finger, and the first score is greater than or equal to the contingent threshold value score, the user is tested on the fingerprint device with the right index finger. As mentioned above with the OR policy, the other single biometric devices can also be used with the CONTINGENT policy to test multiple biometric measurements.

4. RANDOM Policy

The user passes a RANDOM policy of the present invention if the user passes a random biometric device. FIG. 20 is a flowchart illustrating the steps involved in executing a RANDOM policy of the present invention. In step 2002, the n number of biometric devices in the list of devices is determined. A RANDOM policy will typically have at least two different biometric devices in its list of devices. In step 2004, a random number from one to n is picked and the random number is set equal to x. In step 2006, the ✗ biometric device in the list of devices is determined. Once the ✗ biometric device is determined, the user is tested on the ✗ biometric device to produce a score in step 2008.

In step 2010, the score is compared to a biometric device threshold value. If the score is less than the biometric device threshold value, then control transfers to step 2012. In step 2012, the user has failed the RANDOM policy and the flowchart in FIG. 20 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2010 the score is greater than or equal to the biometric device threshold value, then control transfers to step 2014. In step 2014, the user has passed the RANDOM policy and the flowchart in FIG. 20 ends. At this point the user has been authenticated by biometric system 102.

The RANDOM policy is used to request a random biometric measurement from the user each time the user attempts to be authenticated by biometric system 102. Another embodiment of the RANDOM policy is to modify the list of devices to be a list of either fingerprints or word phrases. Here, the user may be tested on a random fingerprint (e.g., the index finger of the user's left hand). Alternatively, the user may be tested on a random word phrase (e.g., "My name is Bob Smith.").

Although the RANDOM policy will typically have at least two different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with any one of multiple biometric measurements to pass the RANDOM policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the RANDOM policy by being tested on any one of the user's fingers. If the user passes the fingerprint device with the random finger, then the user passes the RANDOM policy. As mentioned above with the OR policy, the other single biometric devices can also be used with the RANDOM policy to test multiple biometric measurements.

5. THRESHOLD Policy

The user passes a THRESHOLD policy of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more biometric devices in the list of devices. FIG. 21 is a flowchart illustrating the steps involved in executing a THRESHOLD policy of the present invention. In step 2102, the n number of biometric devices in the list of devices greater than one is determined. A THRESHOLD policy typically has one or more different biometric devices in its list of devices. In step 2104 a total threshold score is determined. In step 2106, the first biometric device in the list of devices is determined. Once the first biometric device is determined, the user is tested on the first biometric device to produce a first score in step 2108.

In step 2110, a temp score is set equal to the first score. In step 2112, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 2114. In step 2114, the user has passed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2112 the temp score is less than the total threshold score, then control transfers to step 2116.

In step 2116, if n is not greater than zero, then control transfers to step 2118. In step 2118, the user has failed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2116 n is greater than zero, then control transfers to step 2120. In step 2120, the next biometric device in the list of devices is determined. Once the next biometric device is determined, the user is tested on the next biometric device to produce a next score in step 2122.

In step 2124, temp score gets multiplied by the next score and the product gets stored back into temp score. In another embodiment of the RANDOM policy, temp score may be added to the next score and the sum stored back into temp score. In step 2126, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 2128. In step 2128, the user has passed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2126 the temp score is less than the total threshold score, then control transfers to step 2130.

In step 2130, one is subtracted from n and control returns to step 2116. In step 2116, if n is not greater than zero then the user has been tested all the biometric devices in the list of devices. Here, control transfers to step 2118. In step 2118, the user has failed the THRESHOLD policy and the flowchart in FIG. 21 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2116 n is greater than zero, this means there are still more biometric devices in the list of devices that the user has not been tested on yet. The flowchart in FIG. 21 continues until the user has either been tested on all the biometric devices in the list of devices or temp score is greater than or equal to the total threshold score.

Although the THRESHOLD policy typically has one or more different biometric devices in its list of devices, the list of devices may have a single biometric device. Here, the user is tested on a single biometric device with any one of multiple biometric measurements to pass the THRESHOLD policy. For example, if the single biometric device is a fingerprint device, the user may be required to pass the THRESHOLD policy by being tested on multiple fingers until the total threshold score is reached. As mentioned above with the OR policy, the other single biometric devices can also be used with the THRESHOLD policy to test multiple biometric measurements.

6. Biometric Policies Having a List of Biometric Policies

As discussed above, the present invention allows for administrator-defined policies. Once type of administrator-defined policy is a biometric policy having a list of biometric policies. Here, instead of the biometric policy having a list of biometric devices as discussed above, this type of biometric policy has a list of biometric policies. The types of biometric policies that can be listed in the list of biometric policies include an OR policy, an AND policy, a CONTINGENT policy, a RANDOM policy and a THRESHOLD policy (all described above). This type of policy is also limited to testing a user on biometric devices only.

The other type of administrator-defined policy is a policy having a policy list of policies or devices. This administrator-defined policy allows for the use of non-biometric devices.

a. OR Policy Having a List of Biometric Policies

The user passes an OR policy having a list of biometric policies of the present invention if the user passes one of the biometric policies in the list of biometric policies. FIG. 22 is a flowchart illustrating the steps involved in executing the OR policy having a list of biometric policies of the present invention. In step 2202, the n number of biometric policies in the list of biometric policies greater than two is determined. The OR policy will always have at least two biometric policies in its list of biometric policies. In step 2204, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 2206. Here, the steps in the flowchart that applies to the first biometric policy are executed. For example, if the first biometric policy is a CONTINGENT policy, then the flowchart in FIG. 19 would be executed. Referring to FIG. 19, the outcome of FIG. 19 is either the user passes or fails the CONTINGENT policy. Therefore, this information gets returned to step 2206 of FIG. 22.

In step 2208, if the user passes the first biometric policy, then control transfers to step 2210. In step 2210, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2208 the user fails the first biometric policy, then control transfers to step 2212.

In step 2212, the second biometric policy in the list of biometric policies is determined. Once the second biometric policy is determined, the second biometric policy is executed in step 2214. Here, the steps in the flowchart that applies to the second biometric policy are executed. For example, the second biometric policy can be the same type of policy as the first biometric policy or it can be one of the other biometric policies.

In step 2216, if the user passes the second biometric policy, then control transfers to step 2218. In step 2218, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2216 the user fails the second biometric policy, then control transfers to step 2220.

In step 1220, if n is not greater than zero, then control transfers to step 2222. If control transfers to step 2222 it means that the list of biometric policies has only two biometric policies in it and the user has failed both biometric policies. In step 2222, the user has failed the OR policy and the flowchart in FIG. 22 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2220 n is greater than zero, then control transfers to step 2224. In this situation the list of biometric policies has more than two biometric policies in it. In step 2224, the next biometric policy is determined. Once the next biometric policy is determined, the next biometric policy is executed in step 2226.

In step 2228, if the user passes the next biometric policy, then control transfers to step 2230. In step 2230, the user has passed the OR policy and the flowchart in FIG. 22 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2228 the user fails the next biometric policy, then control transfers to step 2232.

In step 2232, one is subtracted from n and control returns to step 2220. In step 2220, if n is not greater than zero then the user has failed all the biometric policies in the list of biometric policies. Here, control transfers to step 2222. In step 2222, the user has failed the OR policy and the flowchart in FIG. 22 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2220 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 22 continues until the user has either failed all the biometric policies or the user passes one biometric policy in the list of biometric policies.

b. AND Policy Having a List of Biometric Policies

The user passes an AND policy having a list of biometric policies of the present invention if the user passes all of the biometric policies in the list of biometric policies. FIG. 23 is a flowchart illustrating the steps involved in executing an AND policy having a list of biometric policies of the present invention. In step 2302, the n number of biometric policies in the list of biometric policies greater than two is determined. This type of AND policy will always have at least two biometric policies in its list of biometric policies. In step 2304, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 2306. Here, the steps in the flowchart that applies to the first biometric policy are executed. For example, if the first biometric policy is a AND policy, then the flowchart in FIG. 18 would be executed. Referring to FIG. 18, the outcome of FIG. 18 is either the user passes or fails the AND policy. Therefore, this information gets returned to step 2306 of FIG. 23.

In step 2308, if the user fails the first biometric policy, then control transfers to step 2310. In step 2310, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2308 the user passes the first biometric policy, then control transfers to step 2312.

In step 2312, the second biometric policy in the list of biometric policies is determined. Once the second biometric policy is determined, the second biometric policy is executed in step 2314. Here, the steps in the flowchart that applies to the second biometric policy are executed.

In step 2316, if the user fails the second biometric policy, then control transfers to step 2318. In step 2318, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2316 the user passes the second biometric policy, then control transfers to step 2320.

In step 1320, if n is not greater than zero, then control transfers to step 2322. If control transfers to step 2322 it means that the list of biometric policies has only two biometric policies in it and the user has passed both biometric policies. In step 2322, the user has passed the AND policy and the flowchart in FIG. 23 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2320 n is greater than zero, then control transfers to step 2324. In this situation the list of biometric policies has more than two biometric policies in it. In step 2324, the next biometric policy is determined. Once the next biometric policy is determined, the next biometric policy is executed in step 2326.

In step 2328, if the user fails the next biometric policy, then control transfers to step 2330. In step 2330, the user has failed the AND policy and the flowchart in FIG. 23 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2328 the user passes the next biometric policy, then control transfers to step 2332.

In step 2332, one is subtracted from n and control returns to step 2320. In step 2320, if n is not greater than zero then the user has passed all the biometric policies in the list of biometric policies. Here, control transfers to step 2322. In step 2322, the user has passed the AND policy and the flowchart in FIG. 23 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2320 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 23 continues until the user has either passed all the biometric policies or the user fails one biometric policy in the list of biometric policies.

c. RANDOM Policy Having a List of Biometric Policies

The user passes a RANDOM policy having a list of biometric policies of the present invention if the user passes a random biometric policy. FIG. 24 is a flowchart illustrating the steps involved in executing the RANDOM policy having a list of biometric policies of the present invention. In step 2402, the n number of biometric policies in the list of biometric policies is determined. This type of RANDOM policy will always have at least two biometric policies in its list of biometric policies. In step 2404, a random number from one to n is picked and the random number is set equal to ✗. In step 2406, the ✗ biometric policy in the list of biometric policies is determined. Once the ✗ biometric policy is determined, the ✗ biometric policy is executed in step 2408. Here, the steps in the flowchart that applies to the first biometric policy are executed.

In step 2410, if the user passes the ✗ biometric policy, then control transfers to step 2412. In step 2412, the user has passed the RANDOM policy and the flowchart in FIG. 24 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2410 the user fails the ✗ biometric policy, then control transfers to step 2414. In step 2414, the user has failed the RANDOM policy and the flowchart in FIG. 24 ends. At this point the user has not been authenticated by biometric system 102.

The RANDOM policy having a list of biometric policies is used to request the user to pass a random biometric policy 504 each time the user attempts to be authenticated by biometric system 102.

d. CONTINGENT Policy Having a List of Biometric Policies

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a CONTINGENT policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a CONTINGENT policy having a list of biometric policies of the present invention if either the user exceeds a minimum threshold (i.e., a first composite threshold value) associated with a first biometric policy or if the user exceeds a contingent threshold associated with the first biometric policy and the user exceeds a minimum threshold (i.e., a contingent threshold value) associated with a contingent biometric policy. FIG. 31 is a flowchart illustrating the steps involved in executing the CONTINGENT policy having a list of biometric policies of the present invention. With this type of CONTINGENT policy there is always two biometric policies in the list of biometric policies.

In step 3102, a contingent threshold value is determined. In step 3104, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, then the first biometric policy is executed in step 3106. The results from the execution of the first biometric policy are whether or not the user passed the first biometric policy and a first composite threshold value.

In step 3108, whether the user passed the first biometric policy is determined. If the user passed the first biometric policy, then control transfers to step 3110. In step 3110, the user has passed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3108 the user failed the first biometric policy, then control transfers to step 3112.

In step 3112, the first composite threshold value is compared to the contingent threshold value. If the first composite threshold value is less than the contingent threshold value, then control transfers to step 3114. In step 3114, the user has failed the CONTINGENT policy. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3112 the first composite threshold value is greater than or equal to the contingent threshold value, then control transfers to step 3116. The contingent threshold value is used to give the user a second chance to pass the CONTINGENT policy and thus be authenticated by biometric system 102.

In step 3116, the contingent biometric policy in the list of biometric policies is determined. Once the contingent biometric policy is determined, then the contingent biometric policy is executed in step 3118. In step 3120, if the user passed the contingent biometric policy, then control transfers to step 3122. In step 3122, the user has passed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3120 the user failed the contingent biometric policy, then control transfers to step 3124. In step 3124, the user has failed the CONTINGENT policy and the flowchart in FIG. 31 ends. At this point the user has not been authenticated by biometric system 102.

e. THRESHOLD Policy Having a List of Biometric Policies

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a THRESHOLD policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a THRESHOLD policy having a list of biometric policies of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more biometric policies in the list of biometric policies. FIG. 32 is a flowchart illustrating the steps involved in executing the THRESHOLD policy having a list of biometric policies of the present invention. In step 3202, the n number of biometric policies in the list of biometric policies greater than one is determined. This type of THRESHOLD policy can have one or more biometric policies in its list of biometric policies. In step 3204 a total threshold score is determined. In step 3206, the first biometric policy in the list of biometric policies is determined. Once the first biometric policy is determined, the first biometric policy is executed in step 3208. The results from the execution of the first biometric policy are whether or not the user passed the first biometric policy and a first composite threshold value.

In step 3210, a temp score is set equal to the first composite threshold value. In step 3212, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 3214. In step 3214, the user has passed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3212 the temp score is less than the total threshold score, then control transfers to step 3216.

In step 3216, if n is not greater than zero, then control transfers to step 3218. In step 3218, the user has failed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3216 n is greater than zero, then control transfers to step 3220. In step 3220, the next biometric policy in the list of biometric policies is determined. Once the next biometric policy is determined, the next biometric policy gets executed in step 3222. The results from the execution of the next biometric policy are whether or not the user passed the next biometric policy and a next composite threshold value.

In step 3224, temp score gets multiplied by the next composite threshold value and the product gets stored back into temp score. In step 3226, the temp score is compared to the total threshold score. If the temp score is greater than or equal to the total threshold score, then control transfers to step 3228. In step 3228, the user has passed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3226 the temp score is less than the total threshold score, then control transfers to step 3230.

In step 3230, one is subtracted from n and control returns to step 3216. In step 3216, if n is not greater than zero then all the biometric policies in the list of biometric policies have been executed. Here, control transfers to step 3218. In step 3218, the user has failed the THRESHOLD policy and the flowchart in FIG. 32 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3216 n is greater than zero, this means there are still more biometric policies in the list of biometric policies that have not been executed. The flowchart in FIG. 32 continues until all the biometric policies in the list of biometric policies have been executed or temp score is greater than or equal to the total threshold score.

7. *Biometric Policies having a List of Policies or Devices*

The other type of administrator-defined policy is a biometric policy with a policy list of policies or devices. This administrator-defined policy allows for the combined use of biometric devices, non-biometric devices and/or biometric policies. This type of policy gives added flexibility that all the other policies mentioned above do not provide. With this type of policy, it is possible for a user to be authenticated by biometric system 102 by being tested on a single non-biometric device. This is important because it provides flexibility in converting to biometric system 102 by not having to enroll all users at the same time with biometric devices. Here, a user can continue to use the non-biometric device the user has always used to log into biometric system 102.

There are two ways in which biometric system 102 provides flexibility in rolling out biometric system 102 by not having to enroll all users at the same time with biometric devices. The first way is by not assigning a user to a biometric group 506. Here, when biometric system 102 discovers that the user does not have a biometric group 506, the previous way of allowing users to gain access to enterprise resources (e.g., passwords, tokens or smart cards) takes control to authenticate the user. The second way is when the administrator has assigned the user to a biometric group 506. The second way involves an OR policy with a list of policies or devices of the present invention as described below.

If the user has been assigned to a biometric group 506, then the flexibility of not requiring all users to be enrolled in biometric devices at the same time requires a slight variation from what was described in reference to FIGs. 8A and 8B above. As described above, in step 811, database object 710 (FIG. 7) determines whether the required biometric templates 502 (FIG. 5) for the user are stored in biometric object 710 (FIG. 7) to execute the user's biometric policy 504 (FIG. 5). In addition, database object 710 also determines if computer 208 (FIG. 2) has the required biometric devices attached to it to execute the user's biometric policy 504. If the required biometric templates 502 or the required biometric devices do not exist, then control transfers to step 836. In step 836, biometric server 104 (FIG. 1) communicates to computer 208 that the user cannot be authenticated. Authentication interface 704 (FIG. 7) then denies the user access. Therefore, to provide the flexibility of not requiring all users to be enrolled in biometric devices at the same time, biometric server 104 knows when to skip over step 811 (e.g., a flag) and go directly to step 812 (FIGs. 8A and 8B).

a. OR Policy Having a List of Policies or Devices

The user passes an OR policy having a list of policies or devices of the present invention if the user passes one of the elements in the list of policies or devices. FIG. 25 is a flowchart illustrating the steps involved in executing the OR policy having a list of policies or devices of the present invention. In step 2502, the n number of elements in the list of policies or devices greater than two is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of OR policy will always have at least two elements in its list of polices or devices. In step 2504, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 2506.

In step 2506, the first element is either a biometric or a non-biometric device. FIGs. 8A, 8B and 9 involve the user being tested on a biometric device. Referring again to FIGs. 8A, 8B and 9, when a user gets tested on a biometric device, the result returned includes both a score and whether the user passed or failed the biometric device. The flowchart in FIG. 25 utilizes the information of whether the user passed or failed only. As with biometric devices, when the user is tested on a non-biometric device, the result includes whether the user passed or failed the non-biometric device. Thus, in step 2506, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2504, if the first element is a biometric policy, then control transfers to step 2508. In step 2508, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy). Whether the first element is a biometric policy or a device, controls transfers to step 2510.

In step 2510, if the user passes the first element, then control transfers to step 2512. In step 2512, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). An example of the flexibility biometric system 102 provides by not forcing all users to be enrolled in biometric system 102 at the same time can be illustrated here. Assume the non-biometric device the user has used in the past to gain access to enterprise resources is a password device. If the first element in the list of policies or devices is a password device, the user can be authenticated by biometric system 102 by passing the password device.

Alternatively, if in step 2510 the user fails the first element, then control transfers to step 2514. In step 2514, it is determined whether the second element in the list of policies or devices is a biometric policy. If the second element is not a biometric policy, then control transfers to step 2516. In step 2516, the second element is either a biometric or a non-biometric device. The user is tested on the second element and the result indicates whether the user passed or failed the second element (i.e, the device).

Alternatively, in step 2514, if the second element is a biometric policy, then control transfer to step 2518. The second element is executed to determine whether the user passes or fails the second element (i.e., the biometric policy). Whether the second element is a biometric policy or a device, controls transfers to step 2520. In step 2520, if the user passes the second element, then control transfers to step 2522. In step 2522, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2520 the user fails the second element, then control transfers to step 2524.

In step 2524, if n is not greater than zero, then control transfers to step 2526. If control transfers to step 2526 it means that the list of policies or devices has only two elements in it and the user has failed both elements. In step 2526, the user has failed the OR policy and the flowchart in FIG. 25 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2524 n is greater than zero, then control transfers to step 2528. In this situation the list of policies or devices has more than two elements in it.

In step 2528, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 2530. In step 2530, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device).

Alternatively, in step 2528, if the next element is a biometric policy, then control transfer to step 2532. The next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy). Whether the next element is a biometric policy or a device, controls transfers to step 2534. In step 2534, if the user passes the next element, then control transfers to step 2536. In step 2536, the user has passed the OR policy and the flowchart in FIG. 25 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2534 the user fails the next element, then control transfers to step 2538.

In step 2538, one is subtracted from n and control returns to step 2524. In step 2524, if n is not greater than zero then the user has failed all the elements in the list of policies or devices. Here, control transfers to step 2526. In step 2526, the user has failed the OR policy and the flowchart in FIG. 25 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2524 n is greater than zero, this means there are still more elements in the list of policies or devices. The flowchart in FIG. 25 continues until the user has either failed all the elements or the user passes one element in the list of policies or devices.

b. AND Policy Having a List of Policies or Devices

The user passes an AND policy having a list of policies or devices of the present invention if the user passes all of the elements in the list of policies or devices. FIG. 26 is a flowchart illustrating the steps involved in executing the AND policy having a list of policies or devices of the present invention. In step 2602, the n number of elements in the list of policies or devices greater than two is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of AND policy will always have at least two elements in its list of polices or devices. In step 2604, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 2606.

In step 2606, the first element is either a biometric or a non-biometric device. In step 2606, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2604, if the first element is a biometric policy, then control transfers to step 2608. In step 2608, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy). Whether the first element is a biometric policy or a device, controls transfers to step 2610.

In step 2610, if the user fails the first element, then control transfers to step 2612. In step 2612, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2610 the user passes the first element, then control transfers to step 2614. In step 2614, it is determined whether the second element in the list of policies or devices is a biometric policy. If the second element is not a biometric policy, then control transfers to step 2616. In step 2616, the second element is either a biometric or a non-biometric device. The user is tested on the second element and the result indicates whether the user passed or failed the second element (i.e, the device).

Alternatively, in step 2614, if the second element is a biometric policy, then control transfer to step 2618. The second element is executed to determine whether the user passes or fails the second element (i.e., the biometric policy). Whether the second element is a biometric policy or a device, controls transfers to step 2620. In step 2620, if the user fails the second element, then control transfers to step 2622. In step 2622, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 2620 the user passes the second element, then control transfers to step 2624.

In step 2624, if n is not greater than zero, then control transfers to step 2626. If control transfers to step 2626 it means that the list of policies or devices has only two elements in it and the user has passed both elements. In step 2626, the user has passed the AND policy and the flowchart in FIG. 26 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2624 n is greater than zero, then control transfers to step 2628. In this situation the list of policies or devices has more than two elements in it.

In step 2628, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 2630. In step 2630, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device).

Alternatively, in step 2628, if the next element is a biometric policy, then control transfer to step 2632. The next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy). Whether the next element is a biometric policy or a device, controls transfers to step 2634. In step 2634, if the user fails the next element, then control transfers to step 2636. In step 2636, the user has failed the AND policy and the flowchart in FIG. 26 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2634 the user passes the next element, then control transfers to step 2638.

In step 2638, one is subtracted from n and control returns to step 2624. In step 2624, if n is not greater than zero then the user has passed all the elements in the list of policies or devices. Here, control transfers to step 2626. In step 2626, the user has passed the AND policy and the flowchart in FIG. 26 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 2624 n is greater than zero, this means there are still more elements in the list of policies or devices. The flowchart in FIG. 26 continues until the user has either passed all the elements or the user fails one element in the list of policies or devices.

c. RANDOM Policy Having a List of Policies or Devices

The user passes a RANDOM policy having a list of policies or devices of the present invention if the user passes a random element. FIG. 27 is a flowchart illustrating the steps involved in executing a RANDOM policy having a list of policies or devices of the present invention. In step 2702, the n number of elements in the list of policies or devices is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of RANDOM policy will always have at least two elements in its list of polices or devices. In step 2704, a random number from one to n is picked and the random number is set equal to x. In step 2706, it is determined whether the ✗ element in the list of policies or devices is a biometric policy. If the ✗ element is not a biometric policy, then control transfers to step 2708.

In step 2708, the ✗ element is either a biometric or a non-biometric device. In step 2708, the user is tested on the ✗ element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device).

Alternatively, in step 2706, if the ✗ element is a biometric policy, then control transfers to step 2710. In step 2710, the ✗ element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the ✗ element (i.e., the biometric policy). Whether the ✗ element is a biometric policy or a device, controls transfers to step 2712.

In step 2712, if the user passes the ✗ element, then control transfers to step 2714. In step 2714, the user has passed the RANDOM policy and the flowchart in FIG. 27 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 2712 the user fails the ✗ element, then control transfers to step 2716. In step 2716, the user has failed the RANDOM policy and the flowchart in FIG. 27 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1).

This type of RANDOM policy is used to request the user to pass a random biometric policy 504 or identification device each time the user attempts to be authenticated by biometric system 102.

d. CONTINGENT Policy Having a List of Policies or Devices

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a CONTINGENT policy having a list of policies or devices. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a CONTINGENT policy having a list of policies or devices of the present invention if either the user exceeds a minimum threshold associated with a first element or if the user exceeds a contingent threshold associated with the first element and the user exceeds a minimum threshold associated with a contingent element. FIG. 33 is a flowchart illustrating the steps involved in executing the CONTINGENT policy having a policy list of policies or devices of the present invention. This type of CONTINGENT policy always has two elements in the list of policies or devices. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device.

In step 3302, a contingent threshold value is determined. In step 3304, it is determined whether the first element is a biometric policy. If the first element is not a biometric policy, then control transfers to step 3306. In step 3306, the first element is either a biometric or a non-biometric device. FIGs. 8A, 8B and 9 involve the user being tested on a biometric device. Referring again to FIGs. 8A, 8B and 9, when a user gets tested on a biometric device, the result returned includes both a score and whether the user passed or failed the biometric device. As with biometric devices, when the user is tested on a non-biometric device, the result includes whether the user passed or failed the non-biometric device. This result can be modified to also include a score. Thus, in step 3306, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device) and a first score.

Alternatively, in step 3304, if the first element is a biometric policy, then control transfers to step 3308. In step 3308, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy) and a first composite threshold value. Whether the first element is a biometric policy or a device, control transfers to step 3310.

In step 3310, if the user passes the first element, then control transfers to step 3312. In step 3312, the user has passed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3310 the user fails the first element, then control transfers to step 3314. In step 3314, it is determined whether the first composite threshold value or the first score was returned and it is set equal to temp score.

In step 3316, it is determined whether temp score is less than the contingent threshold value. If the temp score is less than the contingent threshold value, then control transfers to step 3318. In step 3318, the user has failed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has not been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3316 it is determined that temp score is greater than or equal to the contingent threshold value, then control transfers to step 3320.

In step 3320, it is determined whether the contingent element is a biometric policy. If the contingent element is not a biometric policy, then control transfers to step 3322. In step 3322, the contingent element is either a biometric or a non-biometric device. Thus, in step 3322, the user is tested on the contingent element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the contingent element.

Alternatively, in step 3320, if the contingent element is a biometric policy, then control transfers to step 3324. In step 3324, the contingent element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the contingent element. Whether the contingent element is a biometric policy or a device, controls transfers to step 3326.

In step 3326, if the user passes the contingent element, then control transfers to step 3328. In step 3328, the user has passed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3326 the user fails the first element, then control transfers to step 3330. In step 3330, the user has failed the CONTINGENT policy and the flowchart in FIG. 33 ends. At this point the user has not been authenticated by biometric system 102.

e. THRESHOLD Policy Having a List of Policies or Devices

As discussed above each biometric policy returns a pass/fail result. In addition, the biometric policy can also provide one or more threshold values relating to the biometric devices in the list of devices associated with the biometric policy. In other words, each biometric policy returns a composite threshold value that is generated from one or more of the threshold values generated by the biometric devices. The composite threshold values are returned regardless of whether the biometric policy was passed or failed by the user. These composite threshold values can then be used by a THRESHOLD policy having a list of biometric policies. This feature provides the administrator with flexibility to adjust the level of authentication.

The user passes a THRESHOLD policy having a list of policies or devices of the present invention if the user exceeds a total threshold (i.e., total threshold score) while being tested on one or more elements in the list of policies or devices. FIG. 34 is a flowchart illustrating the steps involved in executing a THRESHOLD policy having a policy list of policies or devices of the present invention. In step 3402, the n number of elements in the list of policies or devices greater than one is determined. An element can be one of the biometric polices described herein, a biometric device or a non-biometric device. This type of THRESHOLD policy will have one or more elements in its list of polices or devices. In step 3404, a total threshold score is determined. In step 3406, it is determined whether the first element in the list of policies or devices is a biometric policy. If the first element is not a biometric policy, then control transfers to step 3408.

In step 3408, the first element is either a biometric or a non-biometric device. In step 3408, the user is tested on the first element (i.e., either a biometric or a non-biometric device) and the result indicates whether the user passed or failed the first element (i.e., the device) and a first score.

Alternatively, in step 3406, if the first element is a biometric policy, then control transfers to step 3410. In step 3410, the first element (i.e., the biometric policy) is executed and the result indicates whether the user passed or failed the first element (i.e., the biometric policy) and a first composite threshold value. Whether the first element is a biometric policy or a device, control transfers to step 3412.

In step 3412, it is determined whether the first composite threshold value or the first score was returned and it is set equal to temp score. In step 3414, if temp score is less than the total threshold score, then control transfers to step 3416. In step 3416, the user has passed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has been authenticated by biometric system 102 (FIG. 1). Alternatively, if in step 3414 the temp score is greater than or equal to the total threshold score, then control transfers to step 3418.

In step 3418, if n is not greater than zero, then control transfers to step 3420. If control transfers to step 3420 it means that the list of policies or devices has only one element. In step 3420, the user has failed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3418 n is greater than zero, then control transfers to step 3422. In this situation the list of policies or devices has more than one element in it.

In step 3422, it is determined whether the next element in the list of policies or devices is a biometric policy. If the next element is not a biometric policy, then control transfers to step 3424. In step 3424, the next element is either a biometric or a non-biometric device. The user is tested on the next element and the result indicates whether the user passed or failed the next element (i.e, the device) and a next score.

Alternatively, in step 3422, if the next element is a biometric policy, then control transfer to step 3426. In step 3426, the next element is executed to determine whether the user passes or fails the next element (i.e., the biometric policy) and to get a next composite threshold value. In step 3428, it is determined whether the next composite threshold value or the next score was returned and it is set equal to temp2 score. In step 3430, temp score is multiplied temp2 score and the product is stored back in temp score.

In step 3432, if temp score is less than the total threshold score, then control transfers to step 3434. In step 3434, the user has passed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has been authenticated by biometric system 102. Alternatively, if in step 3432 the temp score is greater than the total threshold value, then control transfers to step 3436.

In step 3436, one is subtracted from n and control returns to step 3418. In step 3418, if n is not greater than zero then all the elements in the list of biometric policies have been executed. Here, control transfers to step 3420. In step 3420, the user has failed the THRESHOLD policy and the flowchart in FIG. 34 ends. At this point the user has not been authenticated by biometric system 102. Alternatively, if in step 3418 n is greater than zero, this means there are still more elements in the list of policies or devices that have not been executed. The flowchart in FIG. 34 continues until all the elements in the list of policies or devices have been executed or temp score is greater than or equal to the total threshold score.

8. Multi-User Biometric Policy

As described above, biometric groups 506 (FIG. 5) are a logical way of combining users that need access to the same set of resources. Some biometric groups 506 are important enough that the biometric policies 504 attached to them require one or more users to be authenticated by biometric system 102 (FIG. 1) to pass the biometric policy 504. This type of biometric policy 504 is called a multi-user biometric policy. The multi-user biometric policy has a list of users. Examples of where the multi-user biometric policy is useful are described next.

The first example involves the various duties that exist within biometric system 102. These duties can be delegated between different positions within biometric system 102. The different positions may include an administrator, a biometric policy manager, a device hardware and software manage and an enrollment manager. Each position must be given the proper authority within biometric system 102 to be able to perform the duties required of that particular position. One way that the proper authority can be given is to create a biometric group 506 for each of the positions. It is very important that only authorized users get put in these biometric groups 506. If an unauthorized user gets put in one or more of these biometric groups 506, then the security of biometric system

102 is compromised. The multi-user biometric policy of the present invention provides the flexibility required for biometric system 102 to ensure that only authorized users get put into one of these biometric groups 506.

The second example involves resources (e.g., computers, applications, data, etc.) within network system 202 (FIG. 2) that need to be protected with the highest security. This type of situation also occurs in non-networked environments. Historically, a bank protects its vault by requiring at least two people to know different parts of the combination in order to open the vault. The multi-user biometric policy of the present invention provides the flexibility required for both networked and non-networked environments in the protection of the types of resources that require the highest security. This is accomplished by defining the required biometric groups 506 and then attaching a multi-user biometric policy to them.

As described above, the multi-user biometric policy has a list of users. Each user in the list of users is represented by the unique user ID 510 that was assigned to that user when he or she enrolled in biometric system 102. The multi-user biometric policy can be implemented as any one of the biometric policies 504 described herein. When biometric server 104 executes the multi-user biometric policy, biometric server 104 first must determine which user IDs 510 are in the list of users. For each user ID 510, biometric server 104 must then determine the biometric policy 504 that particular user must pass in order to be authenticated by biometric system 102. Since the multi-user biometric policy has a list of users, more than one user may have to be authenticated prior to any one user being authenticated by biometric system 102.

An example of how a multi-user biometric policy may be used to protect merger information that no user may gain access to without the president of the enterprise first authorizing it is as follows. The biometric policy 504 attached to the merger information can be defined as an AND multi-user biometric policy with the enterprise president's user ID 510 in the list of users. Here, only users who are also in the list of users may even attempt to gain access to the merger information. No user, even if that user is authenticated by biometric system 102, will gain access to the merger information unless the president also is authenticated by biometric system 102.

All of the above described biometric policies 504 of the present invention provides the flexibility to apply the appropriate level of protection to each network resource without decreasing network productivity. As discussed above, it is the biometric policies 504 that determines the method or way in which a user is to be authenticated by biometric server 104. Although impossible to describe every possible logical variation of biometric policies 504, it should be obvious to one skilled in the art that the logical variations are limitless.

F. Biometric System Security Infrastructure

In general, system security refers to techniques for ensuring that both data stored in a computer and data transported within a system cannot be read or compromised. Inventors of the present invention recognized the importance of securing data within biometric system 102 (FIG. 1). They also recognized the importance of biometric system 102 to integrate easily into existing enterprise security infrastructures.

For example, many network systems today incorporate a firewall. As described above, a firewall is a system designed to prevent unauthorized access and transfer to or from a network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All data entering or leaving the intranet pass through the firewall, which examines each transmission and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. A second line of defense is data encryption. Because many enterprise networks today incorporate one or more firewalls to protect their data, the present invention has been designed in such a way that it integrates easily with existing firewalls.

For greater security, data can be encrypted. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. Encryption is one of the most effective ways to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text and encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric key encryption (also called public-key encryption) and symmetric key encryption. As discussed below, the present invention uses encryption to protect data within biometric system 102.

The inventors of the present invention recognized that there are three main areas in network system 202 (FIG. 2) where the security of data must be maintained. These include persistent data stored in biometric server 104 (FIG. 1), data transported across network 114 (FIG. 1) and biometric device software stored in network system 202.

1. Persistent Data Stored in Biometric Server

FIG. 5 illustrates the various collections of persistent data that are stored in biometric server 104 (FIG. 1). Biometric server 104 stores collections of biometric templates 502, biometric policies 504, biometric groups 506, biometric device IDs 508, user IDs 510, computer IDs 512 and application IDs 514. Of these collections of data, biometric templates 502 are especially important to secure. Each biometric template 502 stores a user's unique biometric measurement that is used to match against the user's "live" biometric measurement when the biometric device is attempting to identify the user. Accordingly, the present invention utilizes well-known encryption techniques to protect data stored in biometric server 104.

2. *Data Transported Across the Network System*

All data within biometric system 102 and all data that gets transported to and from biometric system 102, via network 114, must be secure. As mentioned above, biometric templates 502 are especially important to secure because they store user biometric data. As described in reference to the flowchart of FIGs. 8A and 8B above, a preferred process of authenticating a user by biometric system 102 shows biometric template 502 being matched on the client side (i.e., at computer 208 from FIG. 2). In order for biometric template 502 to be matched on the client side, biometric template 502 must be transported over network 114 from biometric server 104 to computer 208. To further ensure the security of biometric templates 502, the present invention transports biometric templates 502 in an encrypted format over network 114 at all times using session keys.

3. *Biometric System Software*

A limitation with all networks is the impossibility for an administrator to know if an unauthorized person is tampering with software loaded on a computer located at a different location from the administrator within the enterprise. Although it is important for a resource protection administrator to be alarmed when biometric system software has been tampered with, it is equally important for the network administrator to be alarmed when other types of software have been tampered with on computers in the network. Therefore, the inventors of the present invention recognized that what is needed is a way of alarming an administrator of a networked system when software has been tampered with on computers in the network.

To protect biometric system software, the present invention incorporates a software integrity object located at each location in network system 202 (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.) that biometric devices are attached to.

The software integrity object of the present invention is always active and its job is to repeatedly check to ensure all biometric system software (i.e., a data file) loaded at the same location as the software integrity object has not been tampered with. This can be done in many ways. One way is for the software integrity object to calculate, for each biometric system software file, a file date, a file size and a byte-wise sum of the file. Also utilized is a mask value and a starting mask value. The software integrity object then executes the following equation (or a similar equation/formula for assuring software integrity):

$$\sum_{i=o}^{\text{Number of Files}} \left[(\text{File Date})_i + (\text{File Size})_i + (\sum_{j=o}^{\text{File Size}} (\text{File Byte})_j)_i + \text{Item Mask} \right] + \text{Starting Mask}$$

This equation is first executed when the file that is to be protected is first loaded at a location. The first outcome of the equation is stored in a secured environment. The same equation is then repeatedly calculated with the same software. The outcome is then compared to the first outcome stored in the secured environment. If the two do not match, the software integrity object realizes the file containing the software may have been tampered with and sends an alarm to the administrator. The software integrity object is not limited to protecting biometric system software. The software integrity object can be used to protect all software (e.g., files) in network system 202 (FIG. 2).

G. *Biometric Devices and Mobility within a Networked Environment*

The inventors of the present invention recognized a limitation that is encountered when biometric devices are used in a networked environment without biometric system 102 (FIG. 1). As discussed above, for a biometric device to authenticate a user it must have access to the user's biometric template. The present invention provides a scheme for easy access to all user biometric templates 502 such that a user can access network system 202 from any location (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.). The scheme involves storing all biometric templates 502 in a central location. The central location is biometric server 104 (FIG. 1) as described above. Now, via network 114, a user can access his or her biometric template 502 from any location in network system 202. Also, each location in network system 202 knows precisely where to go to locate all biometric templates 502.

Storing all biometric templates 502 in one central location is efficient when network 114 is a LAN. Efficiency problems may arise when network 114 is a WAN. As described above, a WAN connects computers that are farther apart and are connected by data transmission lines or radio waves (e.g., in multiple offices and distant geographies). For example, if an enterprise has multiple offices around the country and all users are accessing one biometric server 104 to gain access to biometric templates 502 for authentication, this is likely to slow down authentication to enterprise resources. To avoid the efficiency problems that will occur if all biometric templates 502 were stored in one biometric server 104, multiple biometric systems 102 can be placed in various locations in network system 202. But here again the problem of a location (e.g., computer 208, enrollment station 106, remote/web computer 210, satellite enrollment station 112, etc.) in network system 202 not knowing precisely where to go to locate needed biometric templates 502 reoccurs.

The inventors of the present invention solved this problem by two different methods. The first method involves the storing of biometric templates 502 within network system 202 in a hierarchical structure. The second method involves the accessing of a hierarchical directory to locate biometric templates 502 within network system 202.

1. Hierarchical Storage of Biometric Templates

FIG. 28 illustrates an enterprise 2800 connected by a WAN incorporating multiple biometric systems 102. Each square in FIG. 28 represents a different office (i.e., location) in enterprise 2800. Each office (i.e., square) has its own LAN and its own biometric system 102. The offices in enterprise 2800 are connected by a WAN.

FIG. 28 shows enterprise 2800 logically organized in a hierarchical structure. Office 2802 is the corporate office and is located at the top of the hierarchical structure. Block 2818 and block 2820 represent logical grouping of offices within enterprise 2800. As shown in FIG. 28, block 2818 includes office 2804, office 2806 and office 2808. Block 2820 includes office 2810, office 2812, office 2814 and office 2816.

The means for determining the logical groupings of offices can involve a number of factors. Several factors can include offices frequently traveled between, grouping offices that do not employ an administrator with offices that do, the adequacy of the WAN connections between various offices, etc.

Because each office has its own biometric system 102, this presents a question of how individual users can avoid having to register at each biometric system 102 and still travel anywhere in enterprise 2800 and be authenticated. One solution is to have a backup copy of all user biometric templates 502 in enterprise 2800 stored in the biometric server at each office. This solution is undesirable for several reasons. As explained in reference to FIG. 1, alternate biometric server 110 is a backup server to biometric server 104 and stores the exact same data. Therefore, it is likely to be expensive to maintain a complete copy of all biometric templates 502 in enterprise 2800 in both biometric server 104 and alternate biometric server 110 at each office. Another reason why this solution is undesirable is the management of various copies of the same biometric template 502 at various locations. When a user refreshes a biometric template 502 (as discussed above) each copy of the old biometric template 502 in enterprise 2800 must be replaced. This increases the possibility that the same biometric template 502 may have different versions in enterprise 2800.

The inventors of the present invention came up with a scheme for hierarchically storing biometric templates within enterprise 2800. In enterprise 2800, all biometric templates 502 are stored at corporate office 2802. Then the additional storage of biometric templates 502 at individual offices depends on the logical block (e.g. either block 2818 or block 2820) the office is in.

The procedure is as follows. First, each office in enterprise 2800 stores the biometric templates 502 for every user enrolled in biometric system 102 at that office. Then, in each logical block, start with the offices at the bottom of the hierarchical structure. For example, in block 2818 start with office 2806 and office 2808. Office 2806 and office 2808 only store the biometric templates 502 for users that were enrolled in biometric systems 102 at those offices. Then, following the hierarchical structure up to office 2804, office 2804 stores the biometric templates 502 for users that were enrolled at office 2804, and also copies of all the biometric templates 502 stored at office 2806 and office 2808. This procedure is repeated until the top of the hierarchical structure is reached (i.e., corporate office 2802).

Thus, with the above hierarchical structure, the farthest any office will have to go to get a user's biometric template is corporate office 2802. For example, say User A was enrolled at office 2812. This means that User A's biometric templates 502 are stored at office 2812, office 2810 and corporate office 2802. If User A travels to office 2806, office 2806 will have to follow the hierarchical structure up to corporate office 2802 to retrieve a copy of User A's biometric templates 502. This scheme allows the biometric templates 502 within enterprise 2800 to be stored at the minimum number of locations, while still providing each user the flexibility to be authenticated by biometric system 102 from any office within the enterprise.

Not only does the hierarchical structure of enterprise 2800 provide ease of access, but also a means of backing up biometric templates 502 within enterprise 2800.

2. Hierarchical Directory for Locating Biometric Templates

The second method involves the accessing of a hierarchical directory to locate biometric templates 502 within enterprise 2800 (FIG. 28). As described above, one example of a hierarchical directory is a X.500 directory. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. Therefore, the same scheme as discussed above for storing biometric templates 502 can be used for storing a X. 500 directory. The X.500 directory will include pointers to the offices that user biometric templates 502 are stored.

H. Other Applications

A computer, as described in reference to FIG. 3, is more than the typical desktop computer. For example, both cars and ATM machines incorporate computers, home and office physical security systems incorporate computers, etc. Thus, the present invention is not limited to the protection of resources in a networked environment as described above. Following are just some of the various applications where the present invention can be applied.

1. Digital Certificates

The inventors of the present invention recognized a limitation that is encountered when digital certificates are used in a networked environment without biometric system 102 (FIG. 1). Generally, a digital certificate defines user privileges. More specifically, a digital certificate attaches to an electronic message and is used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public keys, private keys and a variety of other identification information. The applicant's public key is signed by the CA. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. Today, a user must pass a password device, or use a token or smart card, or any combination thereof, to gain access to a digital certificate. Because each user's digital certificate is stored on one computer within the network, the digital certificate is bound to a single computer. This limits the user from going to a different computer to gain access to the network.

The inventors of the present invention recognized that a way of adequately authenticating a user prior to gaining access to his or her digital certificate is needed that avoids the weakest link in authentication caused by the human factor, as discussed above. In addition, the inventors of the present invention recognized that a scheme is needed for easy access to all user digital certificates such that a user can gain access to required resources from any location within the enterprise. Thus, the present invention requires a user to be authenticated by biometric devices to gain access to digital certificates avoids the weakest link in authentication caused by the human factor.

The scheme for easy access to all user digital certificates, such that a user can gain access to his or her digital certificate from any location within the enterprise, is the same scheme as described above in reference to FIG. 28 and the storing of biometric templates 502. In enterprise 2800, all digital certificates are stored at corporate office 2802. Then the additional storage of digital certificates at individual offices depends on the logical block (e.g. either block 2818 or block 2820) the office is in.

The procedure is as follows. First, each office in enterprise 2800 stores the digital certificates for every user that was issued a digital certificate at that office. Then, in each logical block, start with the offices at the bottom of the hierarchical structure. For example, in block 2818 start with office 2806 and office 2808. Office 2806 and office 2808 only store the digital certificates for users that were issued digital certificates at those offices. Then, following the hierarchical structure up to office 2804, office 2804 stores the digital certificates for users that were issued digital certificates at office 2804, and also copies of all the digital certificates stored at office 2806 and office 2808. This procedure is repeated until the top of the hierarchical structure is reached (i.e., corporate office 2802).

Thus, with the above hierarchical structure, the farthest any office will have to go to get a user's digital certificate is corporate office 2802. For example, say User A was issued a certificate at office 2812. This means that User A's digital certificate is stored at office 2812, office 2810 and corporate office 2802. If User A travels to office 2806, office 2806 will have to follow the hierarchical structure up to corporate office 2802 to retrieve a copy of User A's digital certificate. Once it is determined that the user is finished with his or her digital certificate, the digital certificate must be re-retrieved the next time the user requests access to his or her digital certificate

Not only does the hierarchical structure of enterprise 2800 provide ease of access, but also a means of backing up digital certificates within enterprise 2800.

The use of a hierarchical directory to locate biometric templates 502 within enterprise 2800 (FIG. 28) as described above works equally as well for digital certificates. The X.500 directory will include pointers to the offices that user digital certificates are stored.

2. *Roaming Profile Server*

The concept of using a public key to decode a digital certificate attached to a message was introduced above. Some cryptographic systems use two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. For example, when User A wants to send a secure message to User B, User A uses User B's public key to encrypt the message. User B then uses his or her private key to decrypt the message.

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key. But it is imperative to ensure that users' private keys are kept secret. A user's private keys, among other things, are contained in a unique encrypted user profile. Therefore, a user needs to be adequately authenticated prior to allowing the user access to the user's private keys (i.e., decrypt the user's profile).

There exist public key systems that provide a public key infrastructure. One example of such public key systems is Entrust/PKI™. A public key infrastructure is a comprehensive system that provides public key encryption and digital signature services. The purpose of a public key infrastructure is to manage public keys and digital certificates. By managing keys and digital certificates through a public key infrastructure, an enterprise establishes and maintains a trustworthy networking environment. A public key infrastructure enables the use of encryption and digital signature services across a wide variety of applications.

Public key systems must also manage user profiles. Each profile contains a user's private keys. As mentioned above, the authentication of users prior to allowing them access to their profiles is imperative. Public key systems allow for the authentication of users in one of two ways. The first way is through a password device supplied by the public key system itself. As discussed above, a password device is an inadequate identification mechanism because it can not avoid the weakest link in authentication caused by the human factor.

The second way that public key systems allow for the authentication of users is through an identification device interface. The identification device interface allows third-party vendors of identification devices to create an identity device module that interfaces with it. This way third-party vendors provide the authentication of users prior to allowing them access to their profiles within the public key system.

Various third-party vendors of both biometric and non-biometric devices have created identity device modules for their devices to facilitate user authentication within public key systems. The non-biometric devices (e.g, password, smart cards and tokens) are inadequate identification mechanisms because they can not avoid the weakest link in authentication caused by the human factor.. Alternatively, biometric devices do conclusively authenticate a user by avoiding the weakest link in authentication caused by the human factor. Although a single biometric device can conclusively authenticate a user, the inventors of the present invention recognized that biometric system 102 (FIG. 1) can be used to provide flexibility and additional security in the authentication of users prior to allowing them access to profiles within the public key system. This flexibility and additional security provided by biometric system 102 is the ability to use multiple biometric devices for the authentication of individual users. In addition, the inventors of the present invention recognized that a scheme is needed for easy access to all profiles such that a user can gain access to the user's profile from any location within the enterprise.

FIG. 29 is a block diagram illustrating how biometric system 102 of the present invention can be integrated with a public key system. FIG. 29 includes public key system engine 2902, identification device interface 2904, public key system manager and directory 2906, biometric identity device module 2908, biometric server 104 (FIG. 1) and profile server 2910. Public key system engine 2902, identification device interface 2904 and public key system manager and directory 2906 are not part of the present invention. They are part of a generic public key system. Biometric identity device module 2908, biometric server 104 (FIG. 1) and profile server 2910 are part of the present invention.

Public key system engine 2902 performs the various functions of the public key system. Public key system engine 2902 interacts with the various applications (e.g., e-mail, browsers, etc.) that it provides the use of encryption and digital signatures for. Identification device interface 2904 allows third-party vendors of identification devices to create an identity device module that interfaces with it. Biometric identity device module 2908 is one of these identity device modules that interfaces with identification device interface 2904. Biometric identity device module 2908 acts similar to the open interface of the present invention as described above.

Public key system manager and directory 2906 stores and manages public keys. Biometric server 104 operates exactly as described above. Finally, profile server 2910 stores all of the users' profiles in the public key system. Profile server 2910 is attached to biometric server 104 and acts as a roaming profile server for the public key system.

Biometric identity device module 2908 works with identification device interface 2904 to provide the desired profile from profile server 2910. But prior to providing the desired profile, biometric identity device module 2908 and biometric server 104 work together to authenticate the user. All data transported between biometric identity device module 2908 and biometric server 104 is encrypted. This data includes the profiles and biometric templates 502 (FIG. 5).

Incorporating biometric system 102 (FIG. 1) into a public key system helps to avoid the limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for the environment in which the user is trying to get access to his or her profile, increase user mobility within the enterprise, remotely enroll and re-enroll users into biometric system 102 and to ensure the integrity of software loaded on remote computers.

3. *Phone Authentication and Clearance Verification*

Phones can be implemented as a voice recognition device. Thus, biometric system 102 (FIG. 1) can be used to authenticate employees for access to various phones within the enterprise. Biometric system 102 can also be used to apply clearance verification for each employee to make certain calls. For phone authentication and clearance verification, biometric groups 506 (FIG. 5) can be defined in such a way that employees in certain biometric groups 506 are only allowed to make certain types of phone calls (e.g., local calls, long-distance calls, 800 calls, 900 calls, etc.) and/or have access to certain phones within the enterprise.

Incorporating biometric system 102 (FIG. 1) into phone authentication and clearance verification helps to avoid some of the limitations discussed above. Biometric system 102 provides the flexibility to use a phone as a voice recognition device, increase employee mobility within the enterprise, apply the needed degree of authentication required to protect each type of phone call and remotely enroll and re-enroll customers into biometric system 102.

4. *Access/Facility Control*

Current physical access/facility control systems require the user to enter a password to activate and/or deactivate the system. As described above, biometric devices for identification mechanisms eliminate the weakest link caused by the human factor. Biometric devices can be attached to the entry of each physical location in an enterprise that authentication is required for entry. Then, biometric system 102 (FIG. 1) can be used to provide flexibility in protection and efficient administration as described above.

Biometric groups 506 (FIG. 5) can be defined in such a way that users in certain biometric groups 506 are only allowed access to certain physical locations within an enterprise. One problem that any enterprise has with physical access to locations is that one authenticated person may allow one or more unauthenticated people in the location. Here, a facial image device may be utilized to continuously scan a location to determine if any unauthenticated people are present. If the facial image device determines that an unauthenticated person is present, biometric system 102 can alarm the administrator.

Incorporating biometric system 102 (FIG. 1) into a physical access/facility control system helps to avoid limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for the environment in which the entry is located, increase user mobility within the enterprise, apply the needed degree of authentication required to protect each type of physical location, remotely enroll and re-enroll users into biometric system 102 and to ensure the integrity of software loaded at remote entries.

5. *Banking and Financial*

Today, more than ever, adequate authentication mechanisms are needed in the banking and financial industries. Transactions that once required interaction between two people, now are encouraged to be done via ATM machines or automated phone systems. Currently, transactions are approved by a customer entering a correct pin. As the types of human-to-machine transactions increase, so does the number of different pins each user is required to remember. The result is that either customers write their pins down and/or they use the same pin for many different types of transactions. If a pin is written down, this increases the chance that another person will see the pin and use it to gain unauthorized access to transactions.

Incorporating biometric system 102 (FIG. 1) into current banking and financial transaction systems (e.g., ATM machines), avoids all of the limitations discussed above. Biometric system 102 provides the flexibility to use the right biometric measurement for an environment in which the ATM machine is located, increase customer mobility, apply the needed degree of authentication required to protect each transaction, remotely enroll and re-enroll customers into biometric system 102 and to ensure the integrity of software loaded on remote ATM machines.

6. Silent Signal

Silent signal is a way of silently signaling for assistance through the use of biometric devices. Silent signal is particularly applicable to access/facility control and the banking and financial industries. This feature of the present invention allows a user to enter a normal (i.e., expected) biometric measurement under normal conditions or an alarm biometric measurement under emergency conditions. One example of silent signal incorporates a fingerprint device. Say a fingerprint device is used for authentication at an ATM machine. Biometric policies 504 (FIG. 5) of biometric system 102 (FIG. 1) can be configured to silently signal police if, for example, the left index finger is used for authentication to the ATM machine during a robbery. Otherwise, the right index finger is used for a normal transaction without the need to signal the police. A similar scenario applies to access/facility control.

Another example of silent signal incorporates a voice recognition device. Here, when a certain phrase is used for authentication to either a physical location or at an ATM machine, the police are silently signaled. In addition, it should be apparent to one skilled in the art that any of the biometric devices mentioned above can be used to implement the silent signal of the present invention.

I. Conclusion

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention. This is especially true in light of technology and terms within the relevant art(s) that may be later developed. Thus, the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

What Is Claimed Is:

1. A method for providing user authentication to enterprise resources, comprising the steps of:

(a) setting up a biometric server, said biometric server having stored therein at least one biometric policy that determines whether the user can gain access to the enterprise resources, wherein said biometric policy has associated therewith at least one biometric device;

(b) determining whether the user is authenticated by executing said biometric policy; and

(c) allowing the user access to the enterprise resources if the user passes said biometric policy, otherwise denying access to the user to the enterprise resources.

2. The method claim 1, further comprising the step of enrolling the user for authentication by having the user create a biometric template for each said biometric device, wherein said biometric template includes biometric data unique to the user.

3. The method of claim 1, further comprising forming said biometric policy by selecting one or more said biometric devices that the user must be tested on in order to gain access to the enterprise resources.

4. The method of claim 1, further comprising placing the user within a biometric group, wherein said biometric group defines a set of users with a common characteristic or access privileges.

5. The method of claim 1, wherein step (1) comprises the steps of:

(a) determining initial collections of data stored in said biometric server; and

(b) customizing said collections of data stored in said biometric server.

6. The method of claim 5, wherein step (a) comprises the steps of:

(I) assigning a unique computer ID to each computer in the enterprise;

(ii) assigning a unique biometric device ID to each said biometric device in the enterprise;

(iii) determining which of said biometric devices will be attached to which of said computers by assigning said biometric device IDs to each of said computer IDs;

(iv) forming biometric groups;

(v) creating biometric policies;

(vi) assigning one of said biometric policies to each of said biometric groups;

(vii) assigning a unique user ID to each user who needs to be authenticated;

(viii) putting each of said user IDs into one of said biometric groups; and

(ix) storing said biometric policies, said biometric groups, said biometric device IDs, said user IDs and said computer IDs in said biometric server.

7. The method of claim 2, wherein the step of enrolling the user comprises the steps of:

(a) determining said biometric devices the user must be enrolled in by looking at a list of devices associated with said biometric policy assigned to the user's said biometric group;

(b) creating a biometric template for each of said biometric devices in said list of devices; and

(c) storing each of said created biometric templates in said biometric server.

8. The method of claim 6, wherein step (2) comprises the steps of:

(a) receiving a login request at said biometric server, wherein said login request includes one of said computer IDs and one of said user IDs;

(b) determining which said biometric group said user ID is in;

(c) determining which said biometric policy is assigned to said biometric group;

(d) determining whether said biometric policy can be executed;

(e) returning that the user is not authenticated if the outcome of step (d) is negative;

(f) executing said biometric policy to determine if the user is authenticated; and

(g) returning that the user is authenticated if the outcome of step (f) is positive.

9. The method of claim 8, wherein step (d) comprises the steps of:

I. determining whether said required biometric templates are stored in said biometric server;

ii. determining whether said required biometric device IDs are assigned to said computer ID; and

iii. returning that said biometric policy can be executed if the outcome to both step I and step ii are positive.

10. The method of claim 1, wherein step (1) is performed with an administration station.

11. The method of claim 2, wherein the step of enrolling the user is performed with an enrollment station.

12. The method of claim 8, wherein step (f) comprises the step of testing the user on said biometric devices listed in said list of devices until either the user passes said biometric policy or the user fails said biometric policy.

13. The method of claim 1, wherein said biometric policy is an OR policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said OR policy if the user passes one of said biometric devices in said list of devices.

14. The method of claim 1, wherein said biometric policy is an OR policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said OR policy if the user passes said biometric device while being tested with at least two biometric measurements.

15. The method of claim 1, wherein said biometric policy is an AND policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said AND policy if the user passes all of said biometric devices in said list of devices.

16. The method of claim 1, wherein said biometric policy is an AND policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said AND policy if the user passes said biometric device while being tested with at least two biometric measurements.

17. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with a first biometric device or if the user exceeds a contingent threshold

associated with said first biometric device and the user exceeds a minimum threshold associated with a second biometric device.

18. The method of claim 17, wherein said minimum thresholds and said contingent threshold is set by an administrator.

19. The method of claim 17, wherein said second biometric device is selected based on environmental conditions.

20. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of devices, wherein said list of devices includes only one biometric device, wherein a first biometric measurement and a second biometric measurement are associated with said biometric device, and wherein the user passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with said biometric device and said first biometric measurement or if the user exceeds a contingent threshold associated with said biometric device and said first biometric measurement and the user exceeds a minimum threshold associated with said biometric device and said second biometric measurement.

21. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of devices, wherein said list of devices includes at least two different biometric devices, wherein a random biometric device is determined from said list of devices, and wherein the user passes said RANDOM policy if the user passes said random biometric device.

22. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of devices, wherein said list of devices includes only one biometric device, wherein a random biometric measurement is determined from one or more biometric measurements, and wherein the user

passes said RANDOM policy if the user passes said biometric device while being tested with said random biometric measurement.

23. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of devices, wherein said list of devices includes at least two different biometric devices, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested on one or more of said biometric devices in said list of devices.

24. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of devices, wherein said list of devices includes only one biometric device, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested with one or more biometric measurements on said biometric device in said list of devices.

25. The method of claim 1, wherein said biometric policy is an OR policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said OR policy if the user passes one of said biometric policies in said list of biometric policies.

26. The method of claim 1, wherein said biometric policy is an AND policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said AND policy if the user passes all of said biometric policies in said list of biometric policies.

27. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user

passes said CONTINGENT policy if either the user exceeds a minimum threshold associated with a first biometric policy or if the user exceeds a contingent threshold associated with said first biometric policy and the user exceeds a minimum threshold associated with a second biometric policy.

28. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, wherein a random biometric policy is determined from said list of biometric policies, and wherein the user passes said RANDOM policy if the user passes said random biometric policy.

29. The method of claim 1, wherein said biometric policy is a THRESHOLD policy having a list of biometric policies, wherein said list of biometric policies includes at least two biometric policies, and wherein the user passes said THRESHOLD policy if the user exceeds a total threshold while being tested on one or more of said biometric policies in said list of biometric policies.

30. The method of claim 1, wherein said biometric policy is an OR policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said OR policy if the user passes one of said elements in said list of policies or devices.

31. The method of claim 1, wherein said biometric policy is an AND policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said AND policy if the user passes all of said elements in said list of policies or devices.

32. The method of claim 1, wherein said biometric policy is a CONTINGENT policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, and wherein the user passes said

CONTINGENT policy if either the user exceeds a minimum threshold associated with a first element or if the user exceeds a contingent threshold associated with said first element and the user exceeds a minimum threshold associated with a second element.

33. The method of claim 1, wherein said biometric policy is a RANDOM policy having a list of policies or devices, wherein said list of policies or devices includes at least two elements, wherein a random element is determined from said elements in said list of policies or devices, and wherein the user passes said RANDOM policy if the user passes said random element.

34. The method of claim 1, further comprising having a timeout value associated with said biometric device.

35. A method of storing biometric templates in a hierarchical structure throughout an enterprise, the enterprise having multiple locations, comprising the steps of:

determining a corporate location;

storing all of the biometric templates associated with a group of users at said corporate location;

dividing all of the remaining locations into multiple logical groupings, wherein each logical grouping is associated with a subset of said group of users;

selecting a top level location in each of said logical groupings;

storing at said top level location for each logical grouping all of the biometric templates associated with said subset of users; and

storing at a bottom level location for each of said logical groupings all of said biometric templates associated with a further subset of said subset of users.

36. A method of storing digital certificates in a hierarchical structure throughout an enterprise, the enterprise having multiple locations, comprising the steps of:

determining a corporate location;

storing all of the digital certificates associated with a group of users at said corporate location;

dividing all of the remaining locations into multiple logical groupings, wherein each logical grouping is associated with a subset of said group of users;

selecting a top level location in each of said logical groupings;

storing at said top level location for each logical grouping all of the digital certificates associated with said subset of users; and

storing at a bottom level location for each of said logical groupings all of said digital certificates associated with a further subset of said subset of users.

37. A system for controlling access to enterprise resources, comprising:

a biometric server having stored therein biometric data related to a plurality of users and at least one biometric policy that determines whether said users can gain access to the enterprise resources;

at least one computer connected to said biometric server;

a plurality of biometric devices, wherein said biometric policy has associated therewith at least one of said plurality of biometric devices; and

wherein said biometric server includes means for determining whether said user can access said enterprise resources, wherein said user gains access to the enterprise resources by passing said biometric policy.

38. The system of claim 37, further comprising means for enrolling each of said users, wherein said means for enrolling includes creating a biometric

template for each of said plurality of biometric devices, wherein said biometric template includes biometric data unique to a particular user.

39. The system of claim 37, further comprising means for creating biometric policies and biometric groups, wherein each said biometric groups includes one or more users.

40. The system of claim 39, wherein said biometric group defines one or more users that are allowed access to the same subset of enterprise resources.

41. The system of claim 37, further includes a communication means for connecting said biometric server to one or more remote computers.

42. The system of claim 37, further comprising a secondary server that duplicates all data within said biometric server.

43. The system of claim 37, wherein said biometric server further stores biometric device ID's, User ID's, Computer ID's and Application ID's.

44. The system of claim 37, wherein said means for determining is implemented as an object.

45. The system of claim 37, further comprises a graphical user interface that allows an administrator to create biometric groups and define biometric policies.

46. The system of claim 37, further comprising a roaming profile server having one or more user profiles, wherein said biometric server is utilized to access each of said user profiles.

47. The system of claim 37, wherein said computer is a phone.

48. The system of claim 37, wherein said computer is an ATM machine.

49. The system of claim 37, wherein said computer is attached to a physical location.

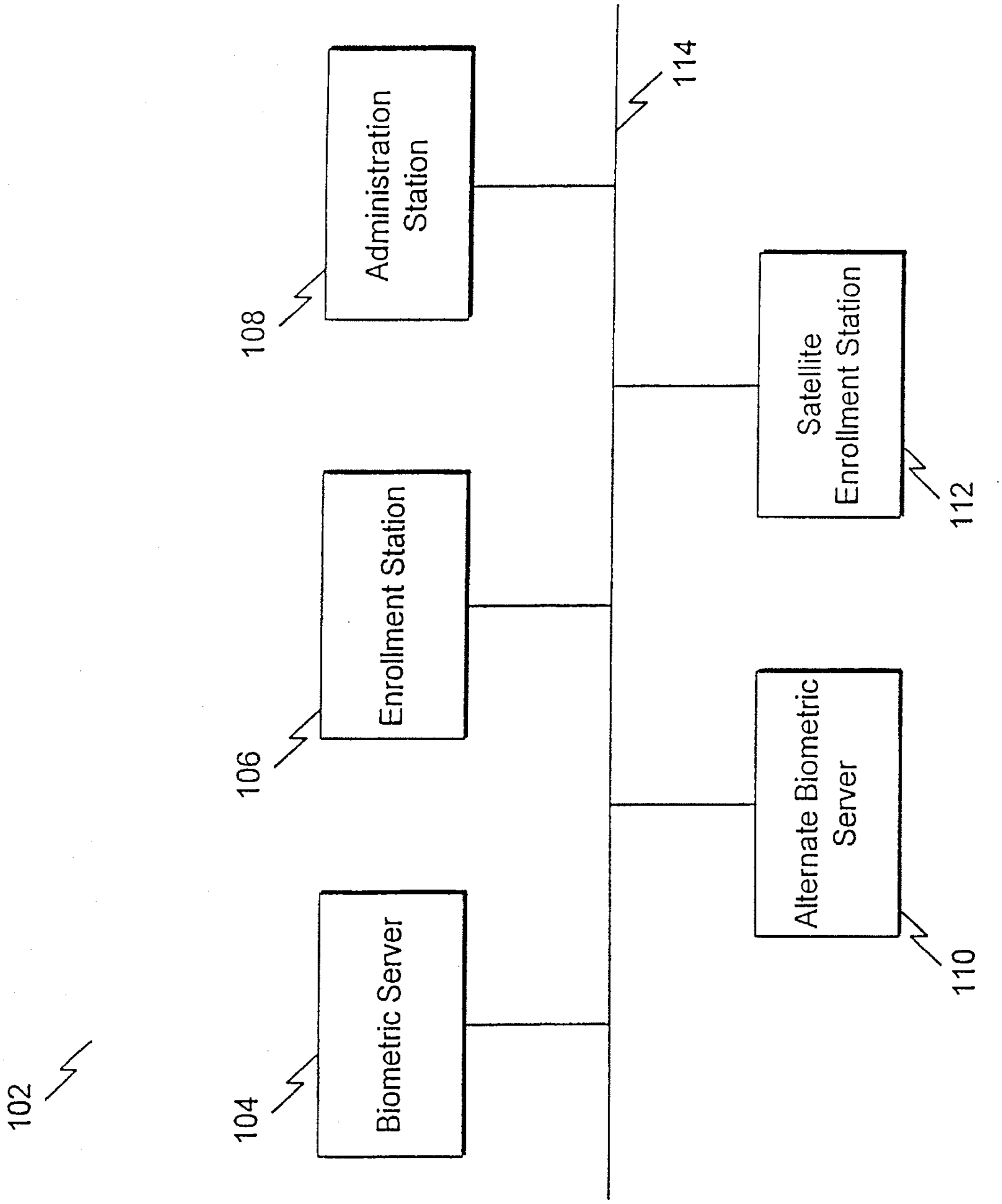

102
104
Biometric Server
106
Enrollment Station
108
Administration Station
110
Alternate Biometric Server
112
Satellite Enrollment Station
114

FIG. 1

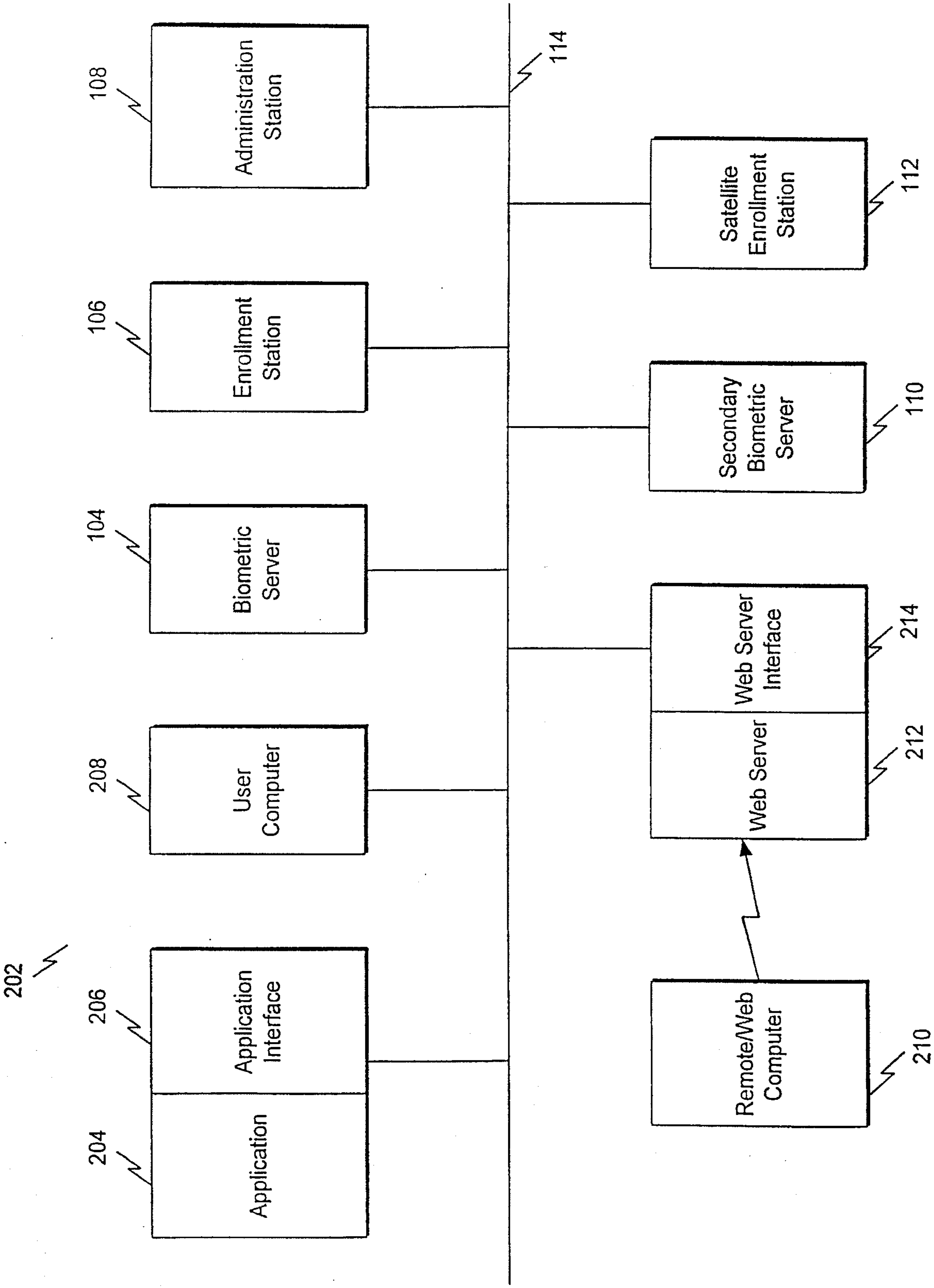

114
108
Administration Station
112
Satellite Enrollment Station
106
Enrollment Station
110
Secondary Biometric Server
104
Biometric Server
214
Web Server Interface
212
Web Server
208
User Computer
202
206
Application Interface
204
Application
210
Remote/Web Computer

FIG.2

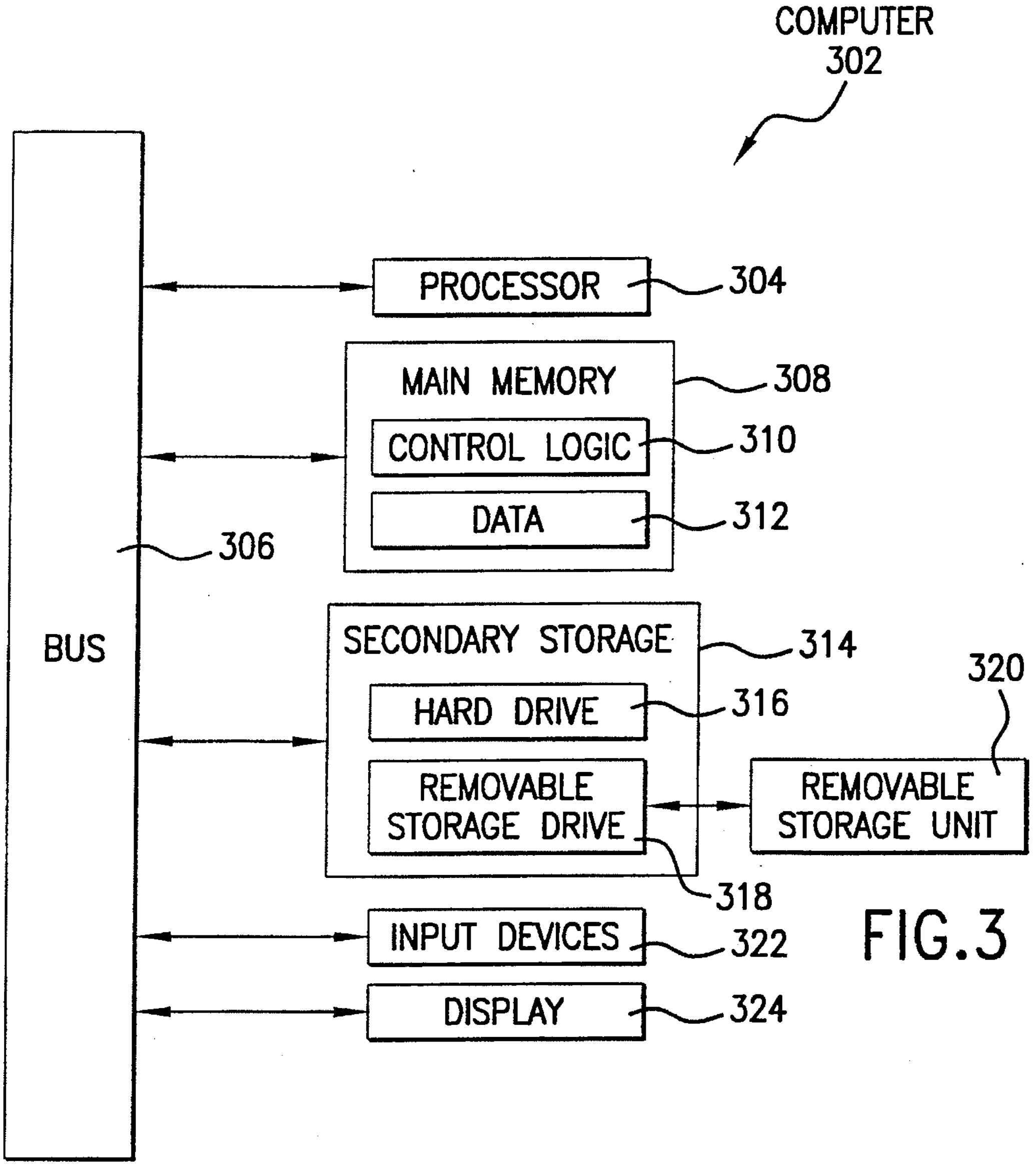

COMPUTER
302
PROCESSOR
304
MAIN MEMORY
308
CONTROL LOGIC
310
DATA
312
306
BUS
SECONDARY STORAGE
314
HARD DRIVE
316
320
REMOVABLE STORAGE DRIVE
REMOVABLE STORAGE UNIT
318
INPUT DEVICES
322
DISPLAY
324

FIG.3

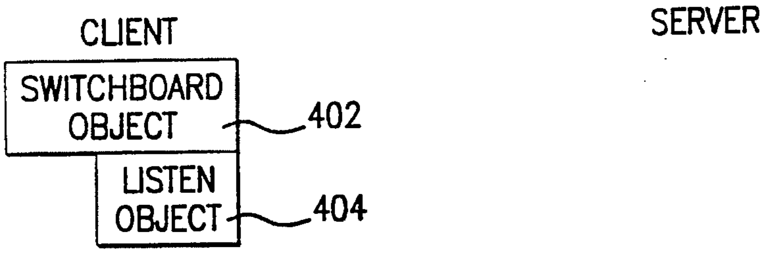


FIG. 4A

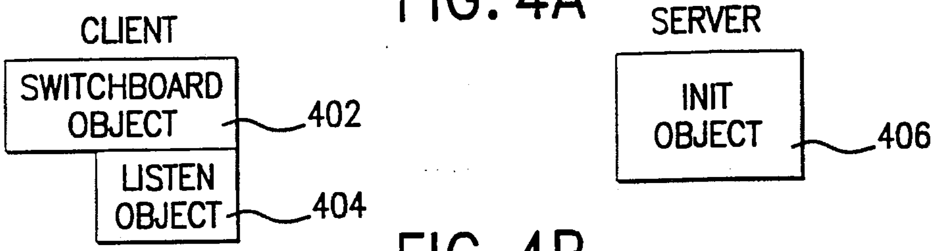


FIG. 4B

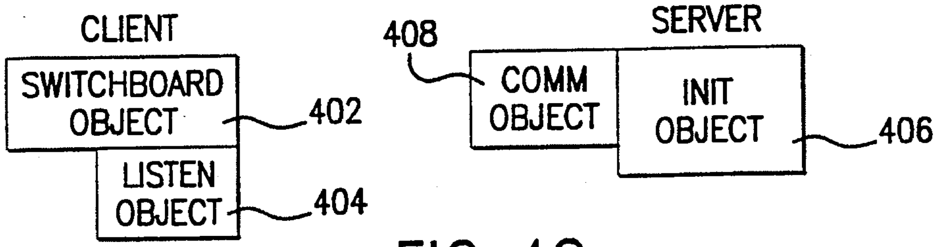


FIG. 4C

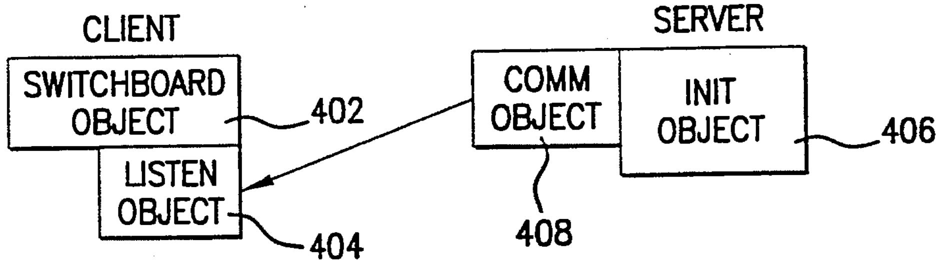


FIG. 4D

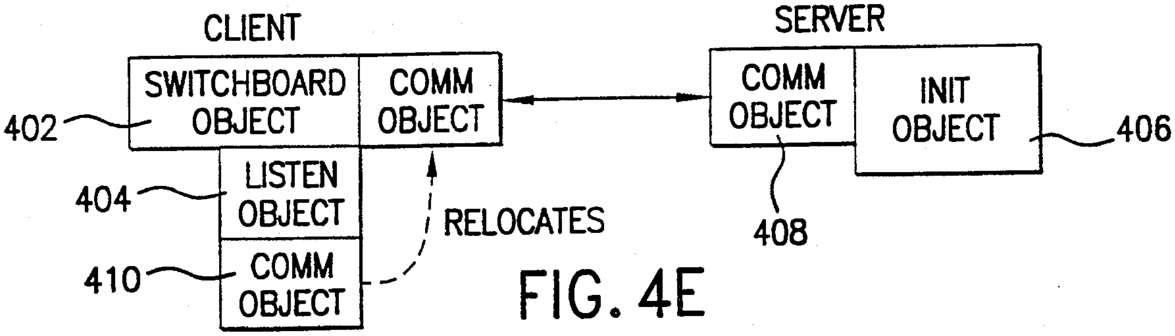


FIG. 4E

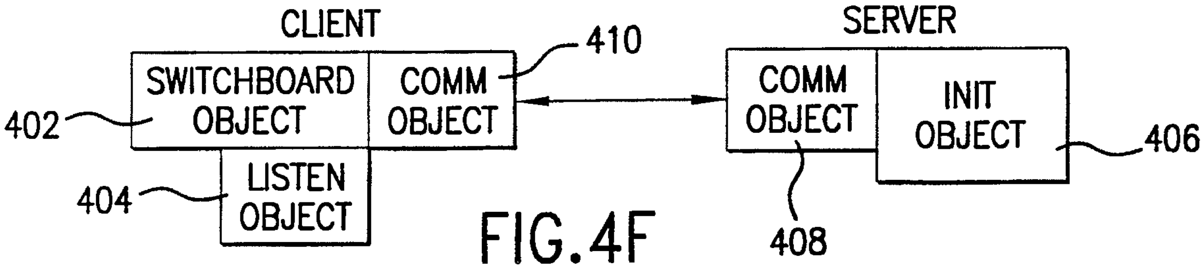


FIG.4F

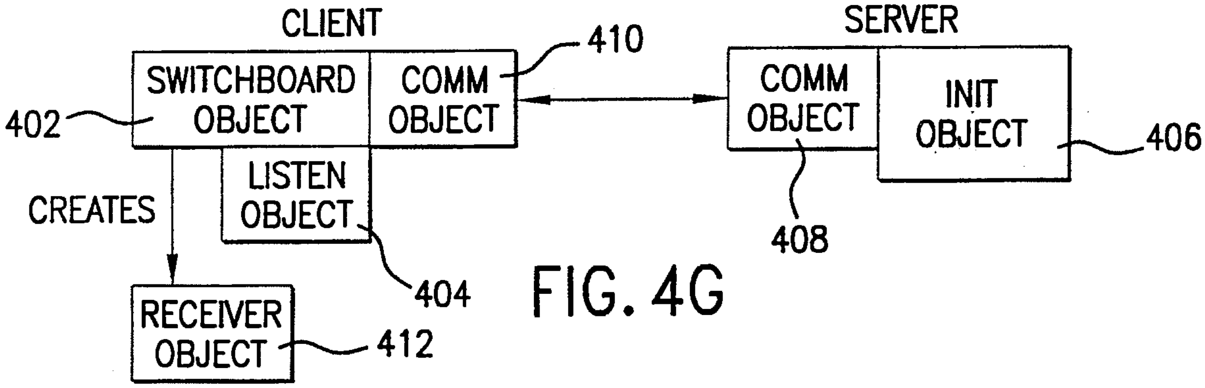


FIG. 4G

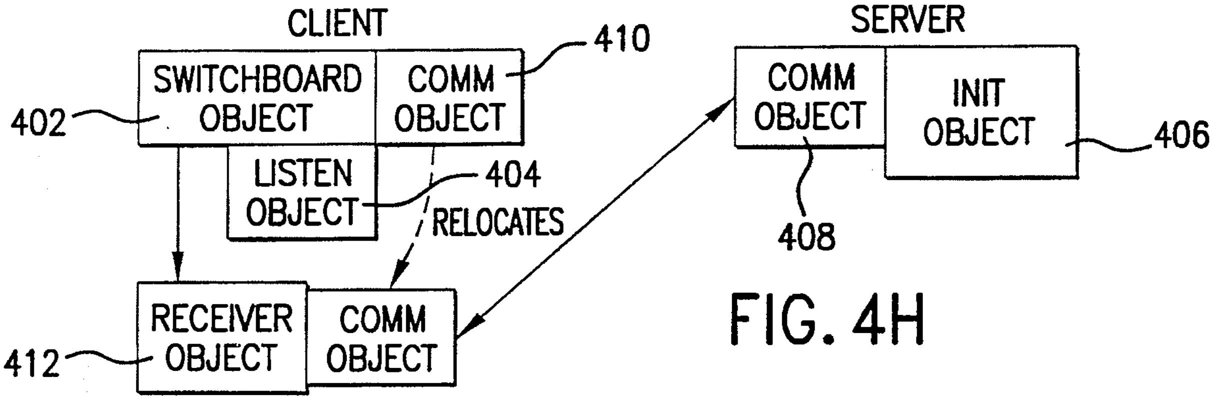


FIG. 4H

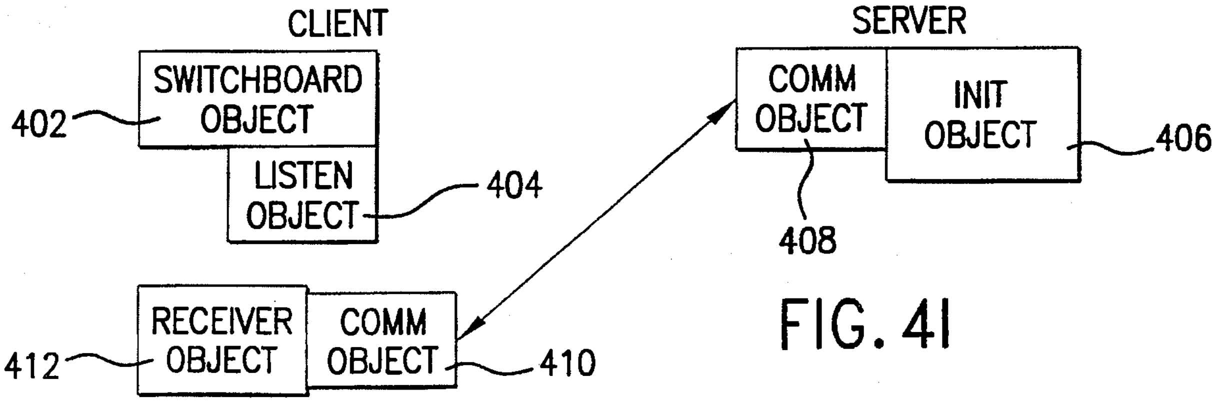


FIG. 4I

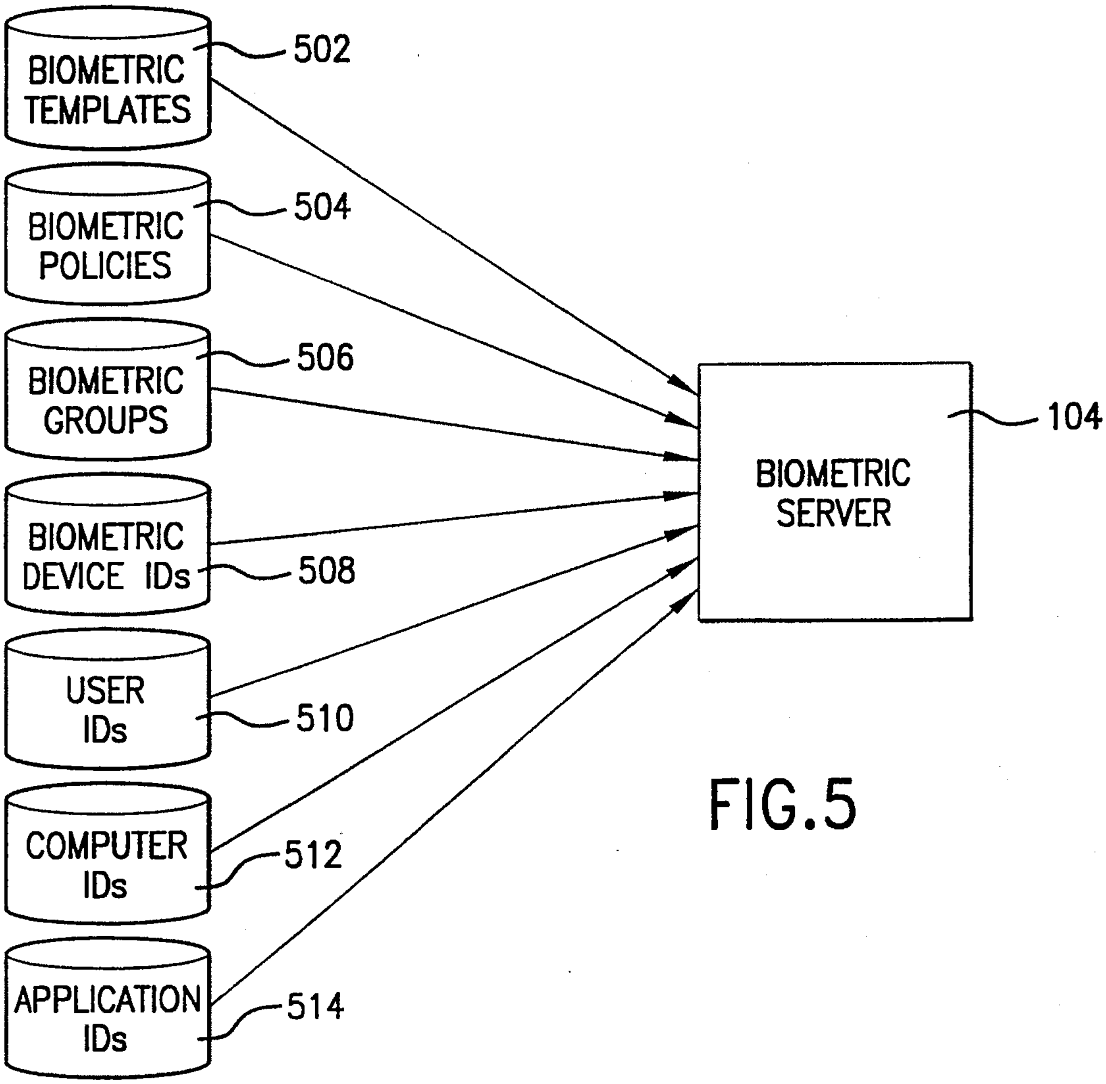

BIOMETRIC TEMPLATES
502
BIOMETRIC POLICIES
504
BIOMETRIC GROUPS
506
BIOMETRIC DEVICE IDs
508
USER IDs
510
COMPUTER IDs
512
APPLICATION IDs
514
BIOMETRIC SERVER
104

FIG.5

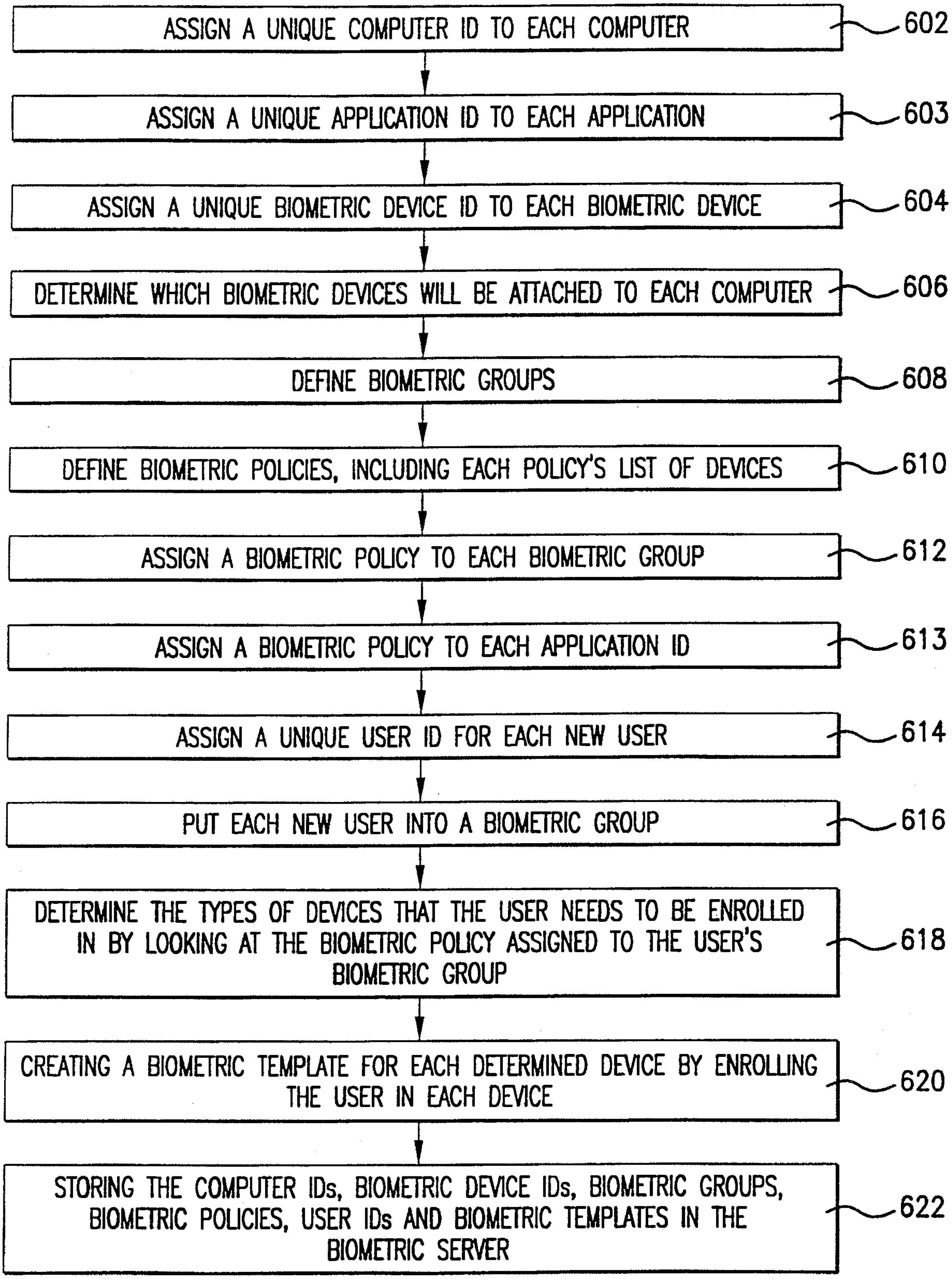

ASSIGN A UNIQUE COMPUTER ID TO EACH COMPUTER
602
ASSIGN A UNIQUE APPLICATION ID TO EACH APPLICATION
603
ASSIGN A UNIQUE BIOMETRIC DEVICE ID TO EACH BIOMETRIC DEVICE
604
DETERMINE WHICH BIOMETRIC DEVICES WILL BE ATTACHED TO EACH COMPUTER
606
DEFINE BIOMETRIC GROUPS
608
DEFINE BIOMETRIC POLICIES, INCLUDING EACH POLICY'S LIST OF DEVICES
610
ASSIGN A BIOMETRIC POLICY TO EACH BIOMETRIC GROUP
612
ASSIGN A BIOMETRIC POLICY TO EACH APPLICATION ID
613
ASSIGN A UNIQUE USER ID FOR EACH NEW USER
614
PUT EACH NEW USER INTO A BIOMETRIC GROUP
616
DETERMINE THE TYPES OF DEVICES THAT THE USER NEEDS TO BE ENROLLED IN BY LOOKING AT THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP
618
CREATING A BIOMETRIC TEMPLATE FOR EACH DETERMINED DEVICE BY ENROLLING THE USER IN EACH DEVICE
620
STORING THE COMPUTER IDs, BIOMETRIC DEVICE IDs, BIOMETRIC GROUPS, BIOMETRIC POLICIES, USER IDs AND BIOMETRIC TEMPLATES IN THE BIOMETRIC SERVER
622

FIG.6

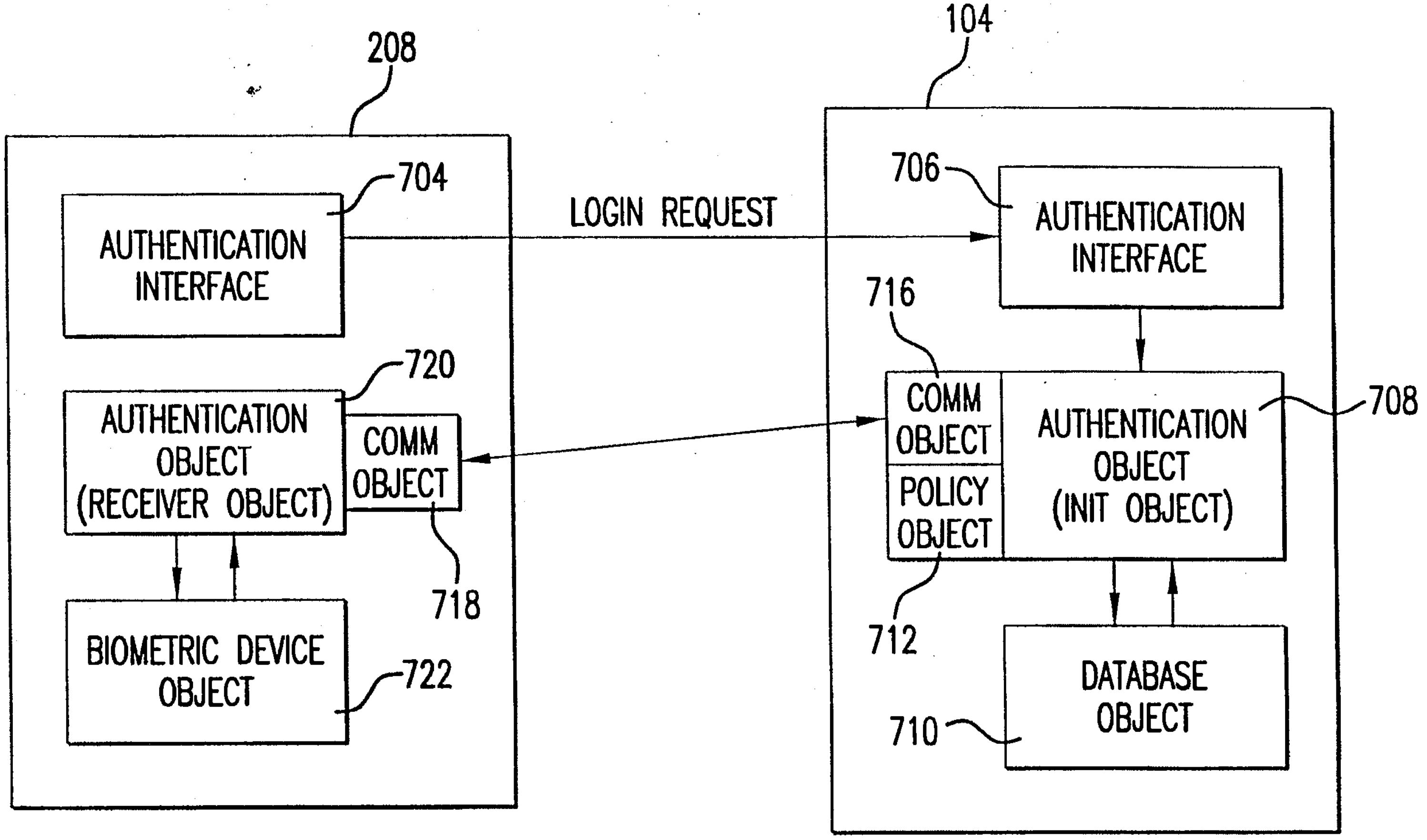

208
104
704
AUTHENTICATION INTERFACE
LOGIN REQUEST
706
AUTHENTICATION INTERFACE
716
720
AUTHENTICATION OBJECT (RECEIVER OBJECT)
COMM OBJECT
718
COMM OBJECT
POLICY OBJECT
AUTHENTICATION OBJECT (INIT OBJECT)
708
712
BIOMETRIC DEVICE OBJECT
722
DATABASE OBJECT
710

FIG.7

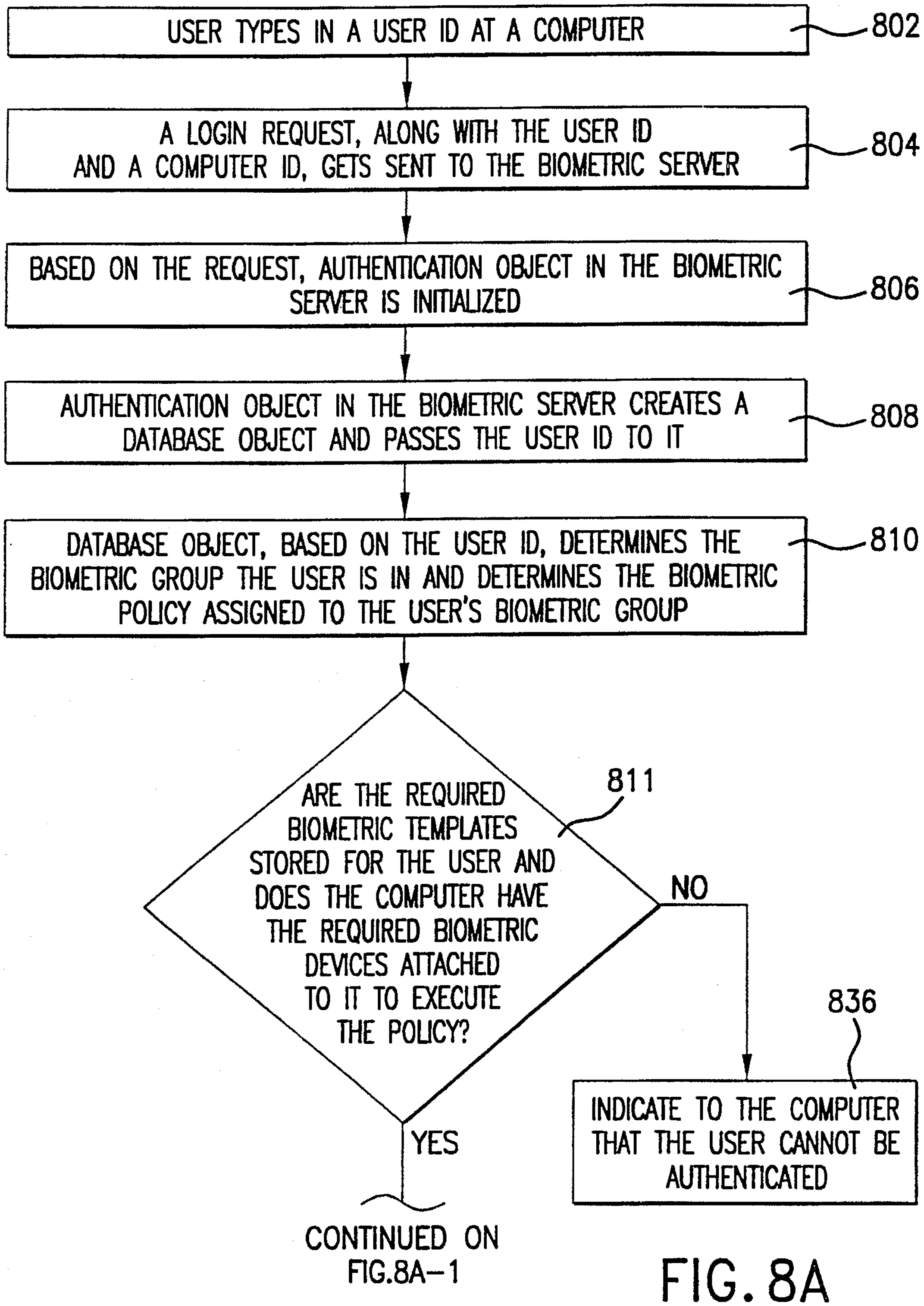

USER TYPES IN A USER ID AT A COMPUTER
802
A LOGIN REQUEST, ALONG WITH THE USER ID AND A COMPUTER ID, GETS SENT TO THE BIOMETRIC SERVER
804
BASED ON THE REQUEST, AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER IS INITIALIZED
806
AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER CREATES A DATABASE OBJECT AND PASSES THE USER ID TO IT
808
DATABASE OBJECT, BASED ON THE USER ID, DETERMINES THE BIOMETRIC GROUP THE USER IS IN AND DETERMINES THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP
810
ARE THE REQUIRED BIOMETRIC TEMPLATES STORED FOR THE USER AND DOES THE COMPUTER HAVE THE REQUIRED BIOMETRIC DEVICES ATTACHED TO IT TO EXECUTE THE POLICY?
811
NO
836
INDICATE TO THE COMPUTER THAT THE USER CANNOT BE AUTHENTICATED
YES
CONTINUED ON FIG.8A-1

FIG.8A

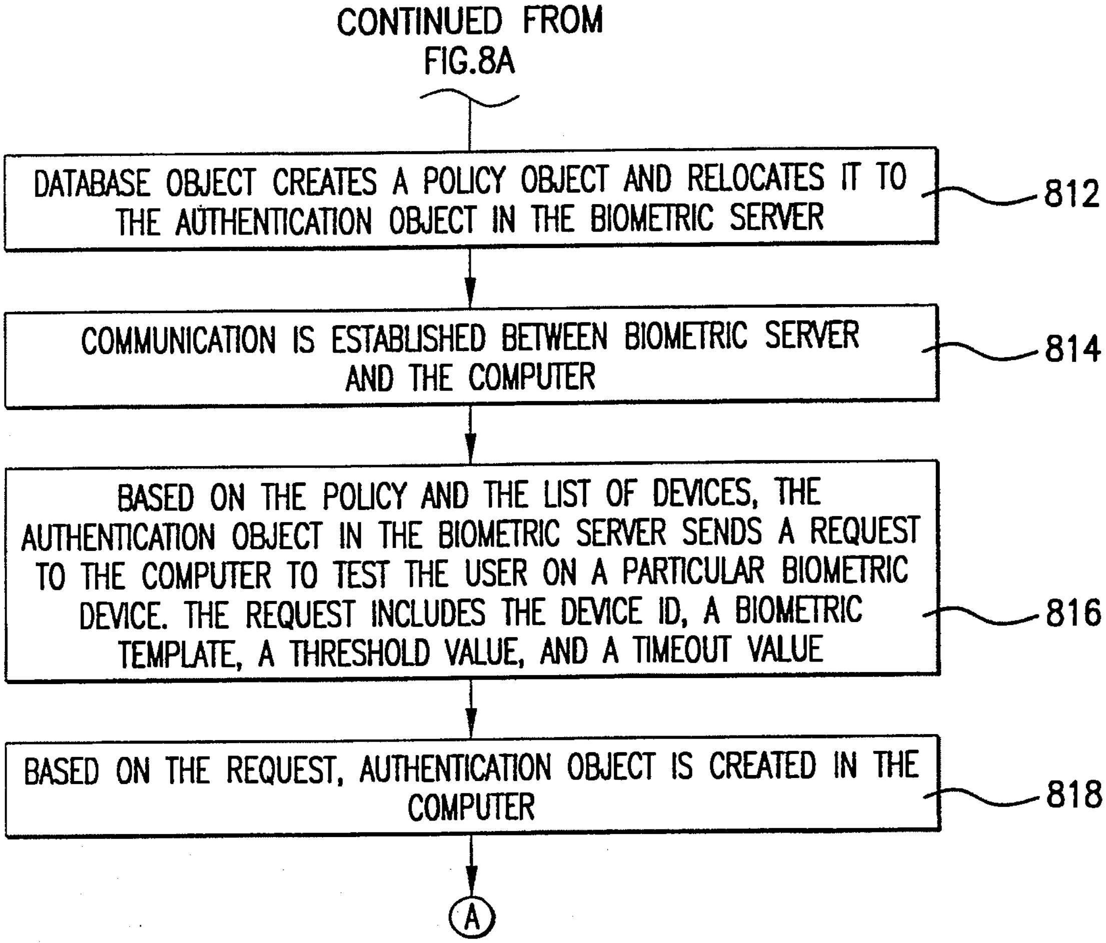

CONTINUED FROM FIG.8A
DATABASE OBJECT CREATES A POLICY OBJECT AND RELOCATES IT TO THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER
812
COMMUNICATION IS ESTABLISHED BETWEEN BIOMETRIC SERVER AND THE COMPUTER
814
BASED ON THE POLICY AND THE LIST OF DEVICES, THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER SENDS A REQUEST TO THE COMPUTER TO TEST THE USER ON A PARTICULAR BIOMETRIC DEVICE. THE REQUEST INCLUDES THE DEVICE ID, A BIOMETRIC TEMPLATE, A THRESHOLD VALUE, AND A TIMEOUT VALUE
816
BASED ON THE REQUEST, AUTHENTICATION OBJECT IS CREATED IN THE COMPUTER
818
A

FIG. 8A-1

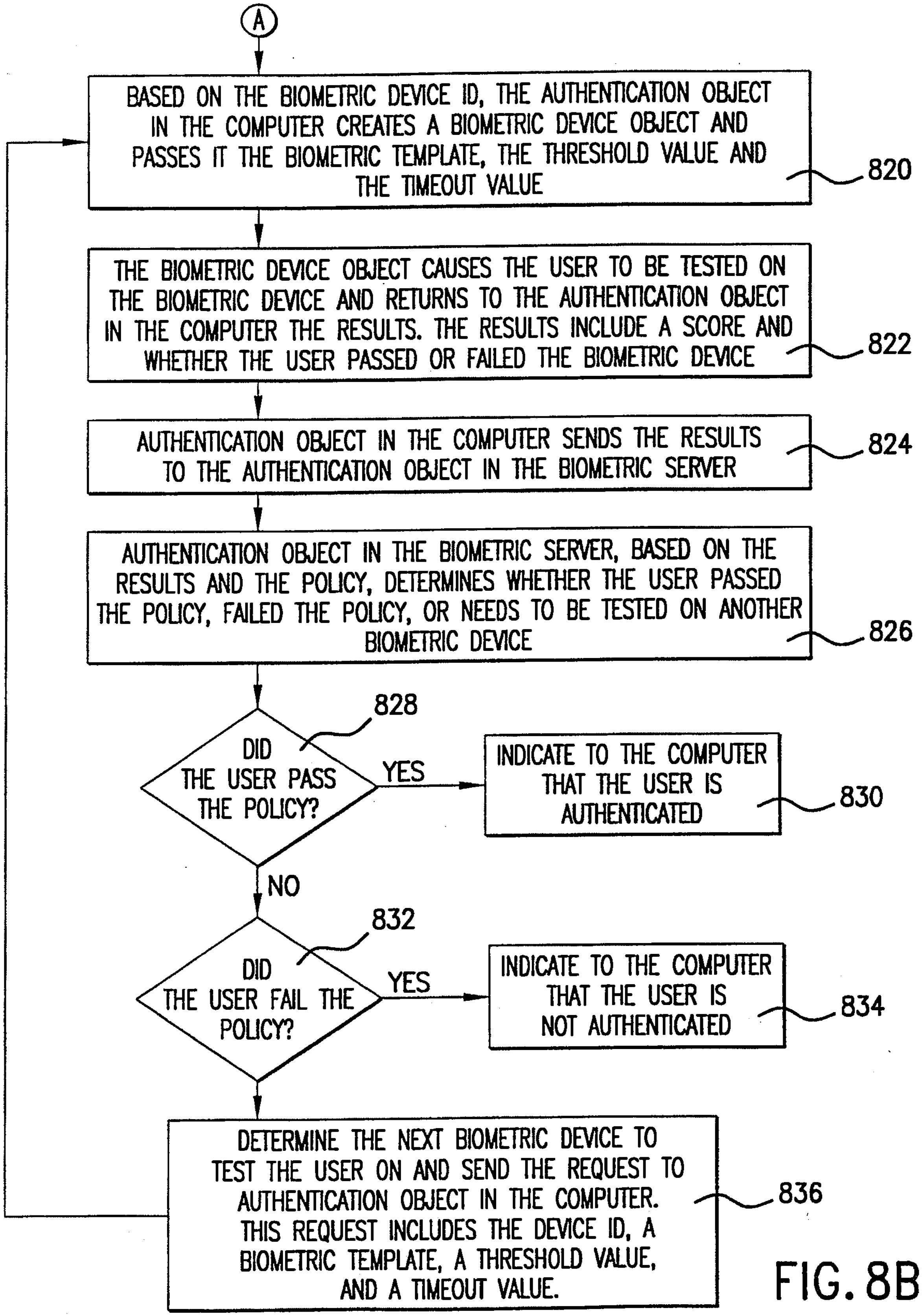

A
BASED ON THE BIOMETRIC DEVICE ID, THE AUTHENTICATION OBJECT IN THE COMPUTER CREATES A BIOMETRIC DEVICE OBJECT AND PASSES IT THE BIOMETRIC TEMPLATE, THE THRESHOLD VALUE AND THE TIMEOUT VALUE
820
THE BIOMETRIC DEVICE OBJECT CAUSES THE USER TO BE TESTED ON THE BIOMETRIC DEVICE AND RETURNS TO THE AUTHENTICATION OBJECT IN THE COMPUTER THE RESULTS. THE RESULTS INCLUDE A SCORE AND WHETHER THE USER PASSED OR FAILED THE BIOMETRIC DEVICE
822
AUTHENTICATION OBJECT IN THE COMPUTER SENDS THE RESULTS TO THE AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER
824
AUTHENTICATION OBJECT IN THE BIOMETRIC SERVER, BASED ON THE RESULTS AND THE POLICY, DETERMINES WHETHER THE USER PASSED THE POLICY, FAILED THE POLICY, OR NEEDS TO BE TESTED ON ANOTHER BIOMETRIC DEVICE
826
828
DID THE USER PASS THE POLICY?
YES
INDICATE TO THE COMPUTER THAT THE USER IS AUTHENTICATED
830
NO
832
DID THE USER FAIL THE POLICY?
YES
INDICATE TO THE COMPUTER THAT THE USER IS NOT AUTHENTICATED
834
DETERMINE THE NEXT BIOMETRIC DEVICE TO TEST THE USER ON AND SEND THE REQUEST TO AUTHENTICATION OBJECT IN THE COMPUTER. THIS REQUEST INCLUDES THE DEVICE ID, A BIOMETRIC TEMPLATE, A THRESHOLD VALUE, AND A TIMEOUT VALUE.
836

FIG. 8B

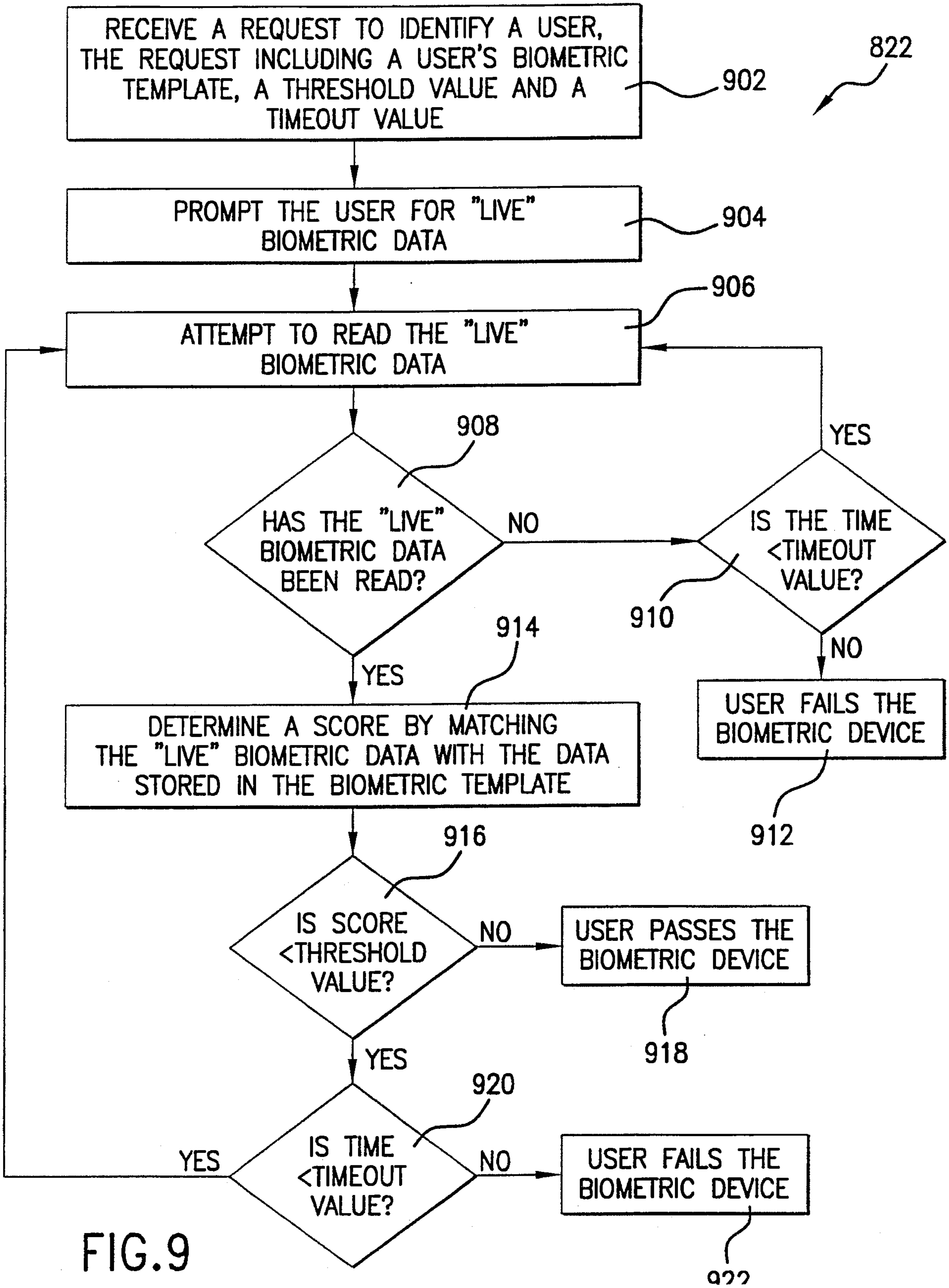

RECEIVE A REQUEST TO IDENTIFY A USER, THE REQUEST INCLUDING A USER'S BIOMETRIC TEMPLATE, A THRESHOLD VALUE AND A TIMEOUT VALUE
902
822
PROMPT THE USER FOR "LIVE" BIOMETRIC DATA
904
906
ATTEMPT TO READ THE "LIVE" BIOMETRIC DATA
908
HAS THE "LIVE" BIOMETRIC DATA BEEN READ?
NO
YES
IS THE TIME <TIMEOUT VALUE?
910
NO
USER FAILS THE BIOMETRIC DEVICE
912
914
YES
DETERMINE A SCORE BY MATCHING THE "LIVE" BIOMETRIC DATA WITH THE DATA STORED IN THE BIOMETRIC TEMPLATE
916
IS SCORE <THRESHOLD VALUE?
NO
USER PASSES THE BIOMETRIC DEVICE
918
YES
920
IS TIME <TIMEOUT VALUE?
YES
NO
USER FAILS THE BIOMETRIC DEVICE
922

FIG.9

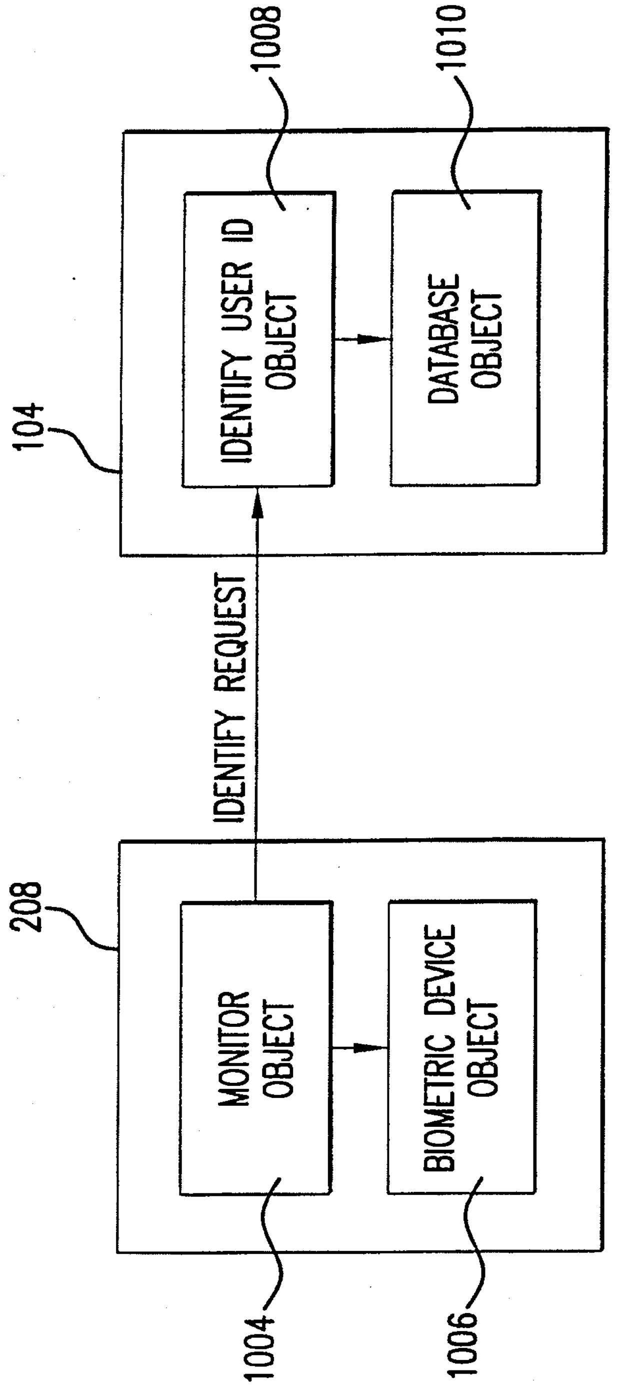

104
IDENTIFY USER ID OBJECT
1008
DATABASE OBJECT
1010
IDENTIFY REQUEST
208
MONITOR OBJECT
1004
BIOMETRIC DEVICE OBJECT
1006

FIG.10

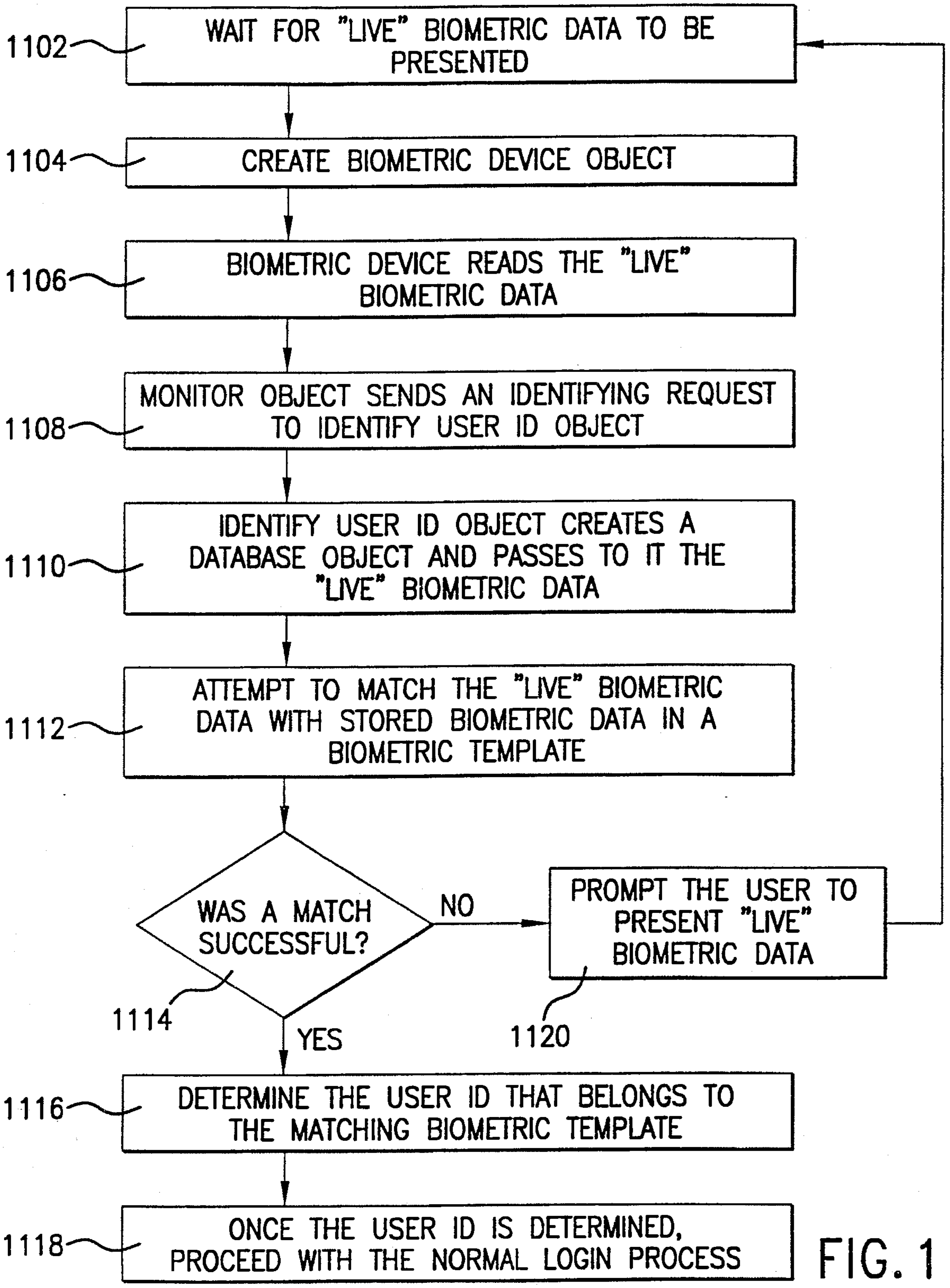

1102
WAIT FOR "LIVE" BIOMETRIC DATA TO BE PRESENTED
1104
CREATE BIOMETRIC DEVICE OBJECT
1106
BIOMETRIC DEVICE READS THE "LIVE" BIOMETRIC DATA
1108
MONITOR OBJECT SENDS AN IDENTIFYING REQUEST TO IDENTIFY USER ID OBJECT
1110
IDENTIFY USER ID OBJECT CREATES A DATABASE OBJECT AND PASSES TO IT THE "LIVE" BIOMETRIC DATA
1112
ATTEMPT TO MATCH THE "LIVE" BIOMETRIC DATA WITH STORED BIOMETRIC DATA IN A BIOMETRIC TEMPLATE
WAS A MATCH SUCCESSFUL?
1114
NO
PROMPT THE USER TO PRESENT "LIVE" BIOMETRIC DATA
1120
YES
1116
DETERMINE THE USER ID THAT BELONGS TO THE MATCHING BIOMETRIC TEMPLATE
1118
ONCE THE USER ID IS DETERMINED, PROCEED WITH THE NORMAL LOGIN PROCESS

FIG. 11

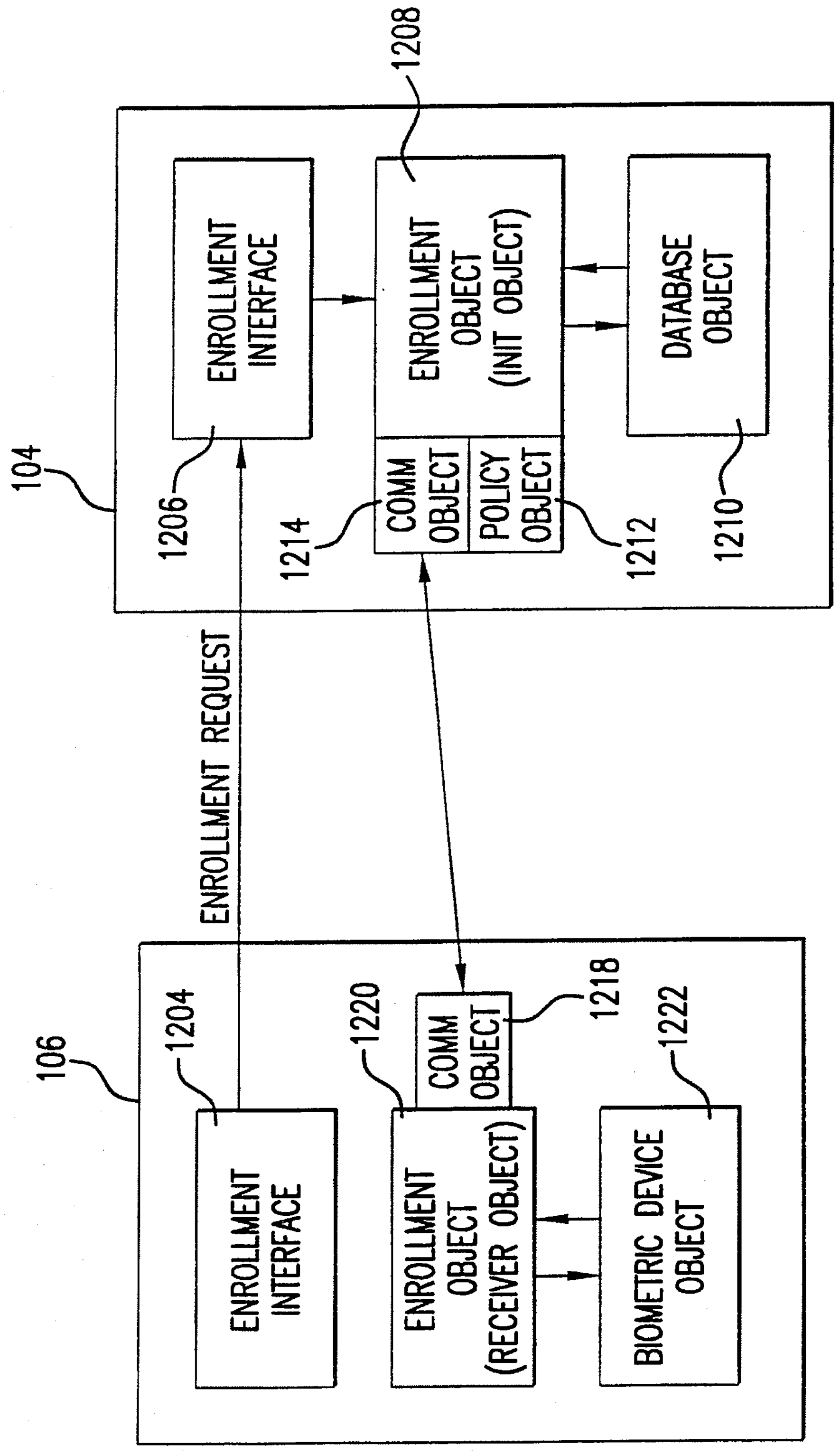

106
1204
ENROLLMENT INTERFACE
1220
ENROLLMENT OBJECT (RECEIVER OBJECT)
COMM OBJECT
1218
1222
BIOMETRIC DEVICE OBJECT
ENROLLMENT REQUEST
104
1206
ENROLLMENT INTERFACE
1214
COMM OBJECT
POLICY OBJECT
1212
ENROLLMENT OBJECT (INIT OBJECT)
1208
DATABASE OBJECT
1210

FIG. 12

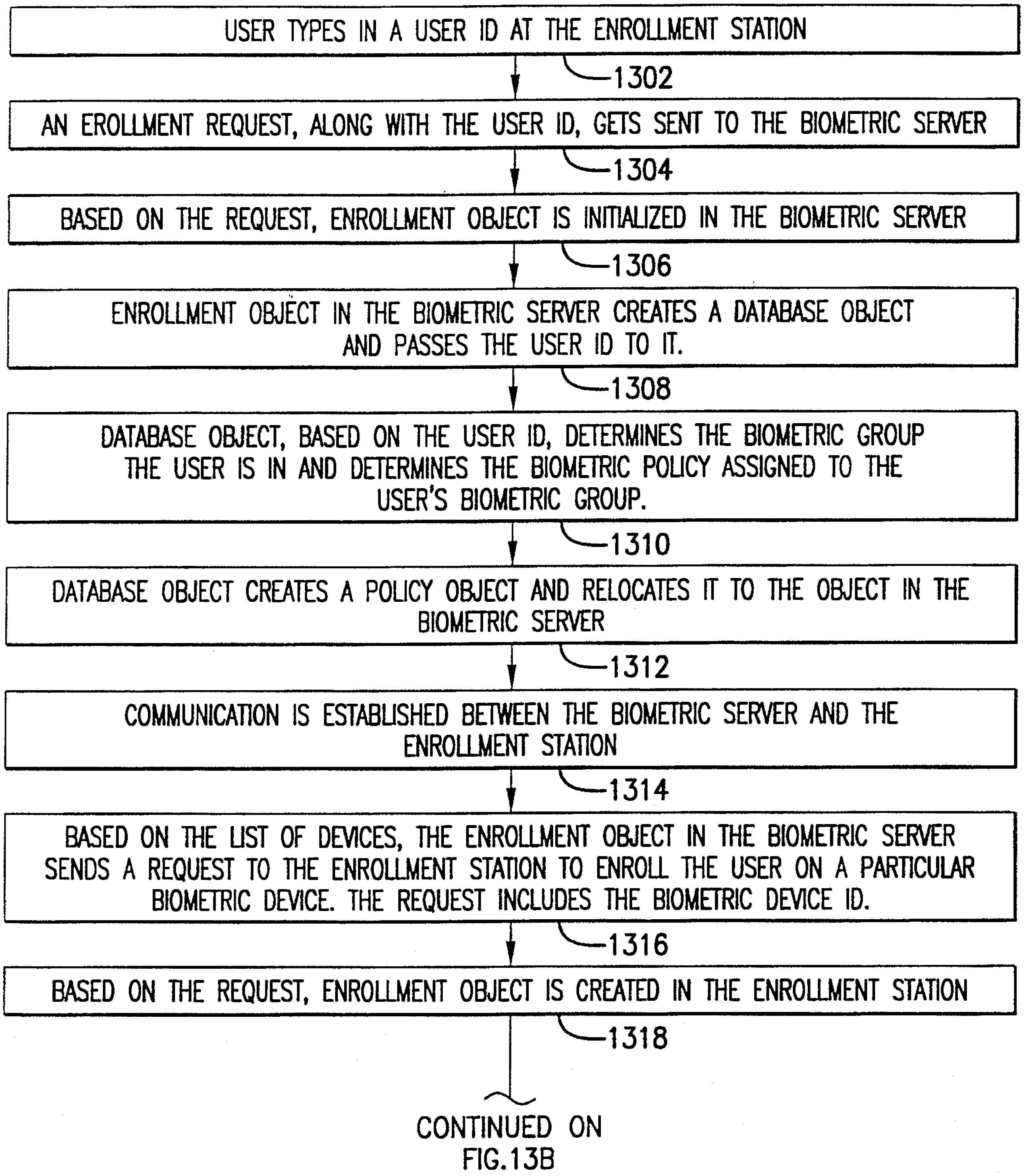

USER TYPES IN A USER ID AT THE ENROLLMENT STATION
1302
AN EROLLMENT REQUEST, ALONG WITH THE USER ID, GETS SENT TO THE BIOMETRIC SERVER
1304
BASED ON THE REQUEST, ENROLLMENT OBJECT IS INITIALIZED IN THE BIOMETRIC SERVER
1306
ENROLLMENT OBJECT IN THE BIOMETRIC SERVER CREATES A DATABASE OBJECT AND PASSES THE USER ID TO IT.
1308
DATABASE OBJECT, BASED ON THE USER ID, DETERMINES THE BIOMETRIC GROUP THE USER IS IN AND DETERMINES THE BIOMETRIC POLICY ASSIGNED TO THE USER'S BIOMETRIC GROUP.
1310
DATABASE OBJECT CREATES A POLICY OBJECT AND RELOCATES IT TO THE OBJECT IN THE BIOMETRIC SERVER
1312
COMMUNICATION IS ESTABLISHED BETWEEN THE BIOMETRIC SERVER AND THE ENROLLMENT STATION
1314
BASED ON THE LIST OF DEVICES, THE ENROLLMENT OBJECT IN THE BIOMETRIC SERVER SENDS A REQUEST TO THE ENROLLMENT STATION TO ENROLL THE USER ON A PARTICULAR BIOMETRIC DEVICE. THE REQUEST INCLUDES THE BIOMETRIC DEVICE ID.
1316
BASED ON THE REQUEST, ENROLLMENT OBJECT IS CREATED IN THE ENROLLMENT STATION
1318
CONTINUED ON FIG.13B

FIG. 13A

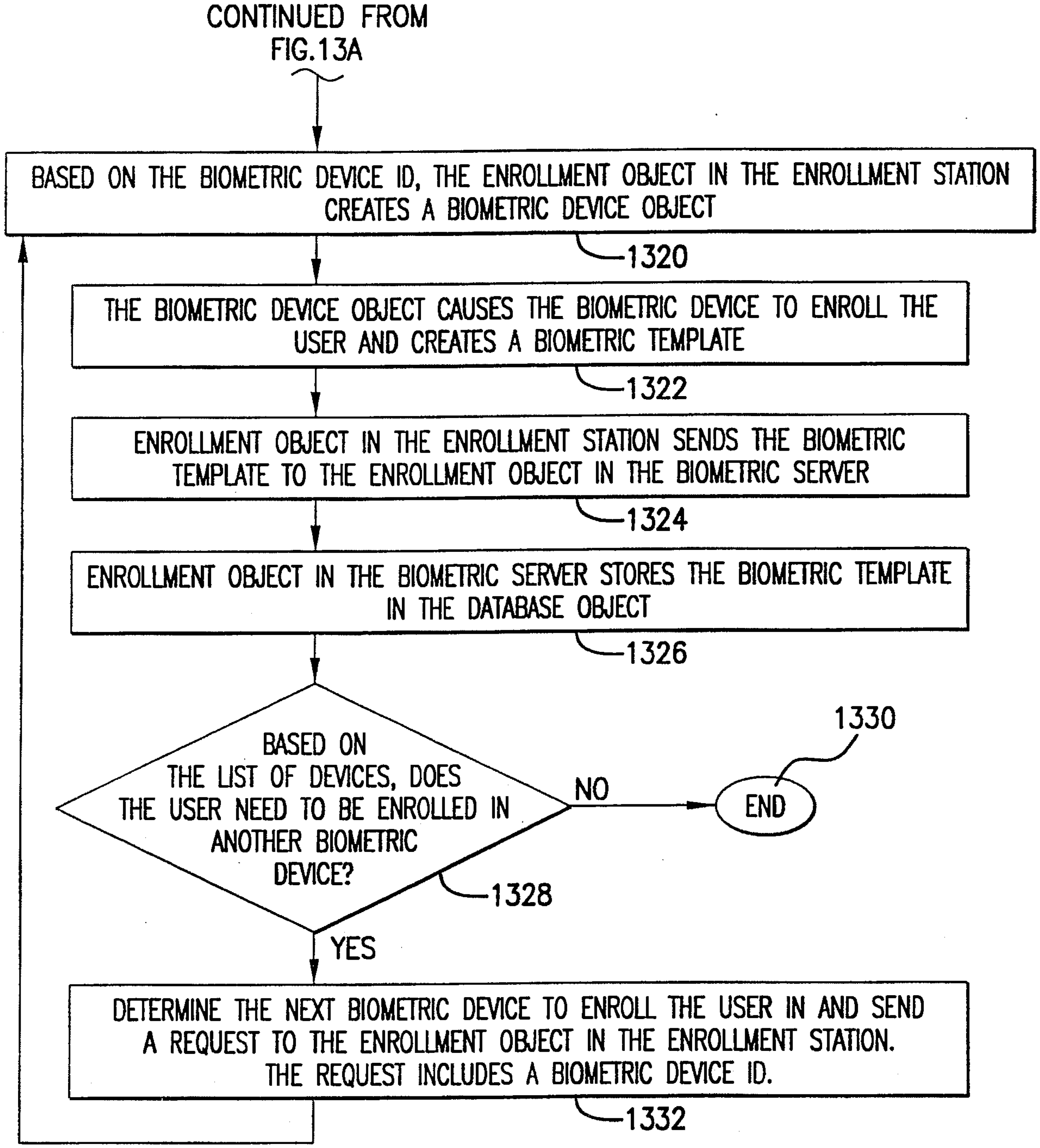

CONTINUED FROM FIG.13A
BASED ON THE BIOMETRIC DEVICE ID, THE ENROLLMENT OBJECT IN THE ENROLLMENT STATION CREATES A BIOMETRIC DEVICE OBJECT
1320
THE BIOMETRIC DEVICE OBJECT CAUSES THE BIOMETRIC DEVICE TO ENROLL THE USER AND CREATES A BIOMETRIC TEMPLATE
1322
ENROLLMENT OBJECT IN THE ENROLLMENT STATION SENDS THE BIOMETRIC TEMPLATE TO THE ENROLLMENT OBJECT IN THE BIOMETRIC SERVER
1324
ENROLLMENT OBJECT IN THE BIOMETRIC SERVER STORES THE BIOMETRIC TEMPLATE IN THE DATABASE OBJECT
1326
BASED ON THE LIST OF DEVICES, DOES THE USER NEED TO BE ENROLLED IN ANOTHER BIOMETRIC DEVICE?
1328
NO
END
1330
YES
DETERMINE THE NEXT BIOMETRIC DEVICE TO ENROLL THE USER IN AND SEND A REQUEST TO THE ENROLLMENT OBJECT IN THE ENROLLMENT STATION. THE REQUEST INCLUDES A BIOMETRIC DEVICE ID.
1332

FIG. 13B

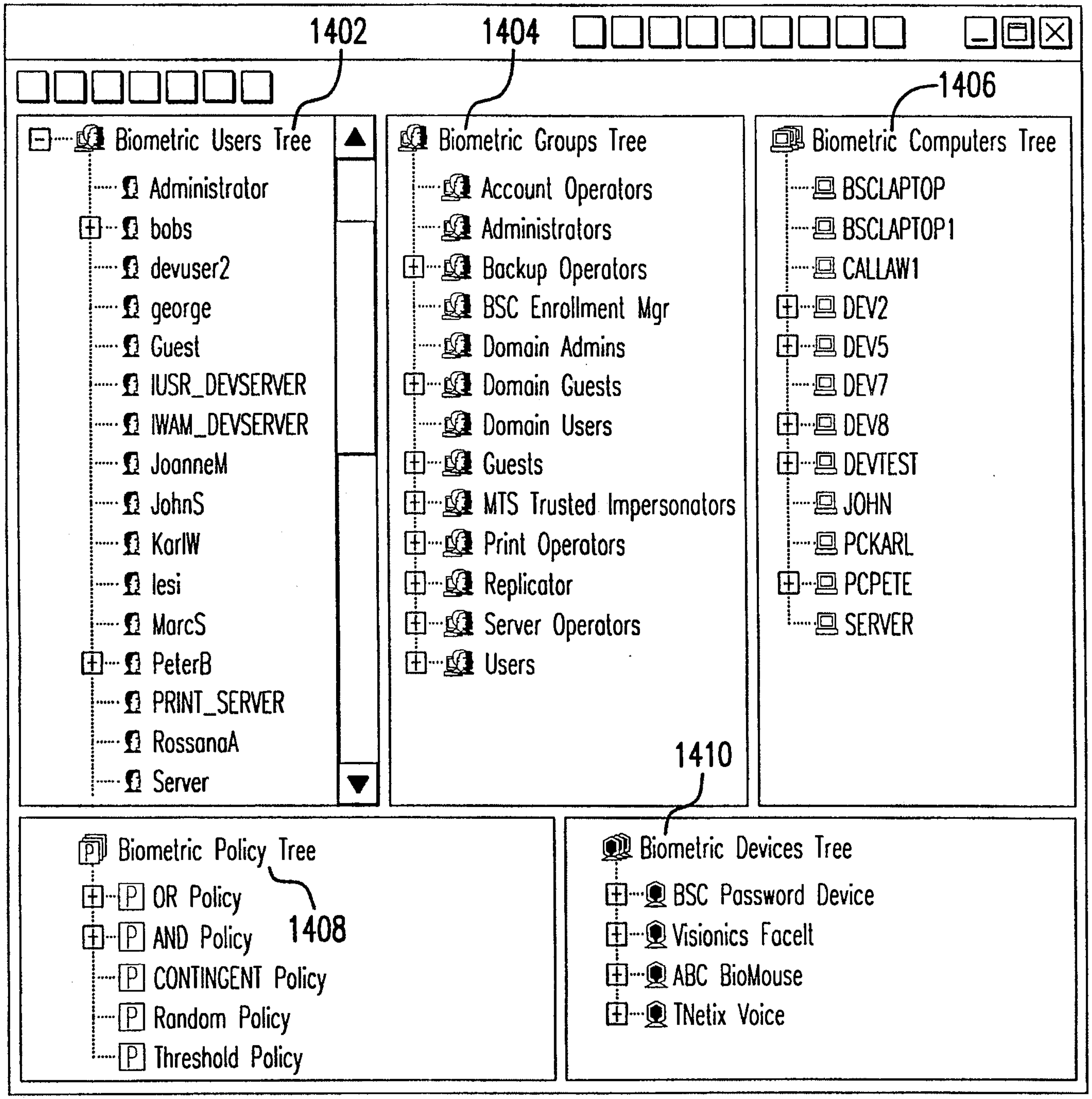

1402
1404
1406
Biometric Users Tree
Administrator
bobs
devuser2
george
Guest
IUSR_DEVSERVER
IWAM_DEVSERVER
JoanneM
JohnS
KarlW
lesi
MarcS
PeterB
PRINT_SERVER
RossanaA
Server
Biometric Groups Tree
Account Operators
Administrators
Backup Operators
BSC Enrollment Mgr
Domain Admins
Domain Guests
Domain Users
Guests
MTS Trusted Impersonators
Print Operators
Replicator
Server Operators
Users
Biometric Computers Tree
BSCLAPTOP
BSCLAPTOP1
CALLAW1
DEV2
DEV5
DEV7
DEV8
DEVTEST
JOHN
PCKARL
PCPETE
SERVER
1410
Biometric Policy Tree
1408
OR Policy
AND Policy
CONTINGENT Policy
Random Policy
Threshold Policy
Biometric Devices Tree
BSC Password Device
Visionics FaceIt
ABC BioMouse
TNetix Voice

FIG. 14

1502

204

208 202 1504 1506

	BULLETIN BOARD	EMAIL	SALES REPORTS	PATIENT/ CLIENT RECORDS	PRODUCT DEVELOP-MENT	USER COMPUTERS	NETWORK SYSTEM	INTERNET ACCESS	DIAL-IN ACCESS
PASSWORD	✓								✓
FINGERPRINT		M	M	H	H		M	M	M
VOICE RECOGNITION			L				L	L	L
FACIAL IMAGE				M					
SIGNATURE						M			
SMART CARD						✓			

FIG. 15

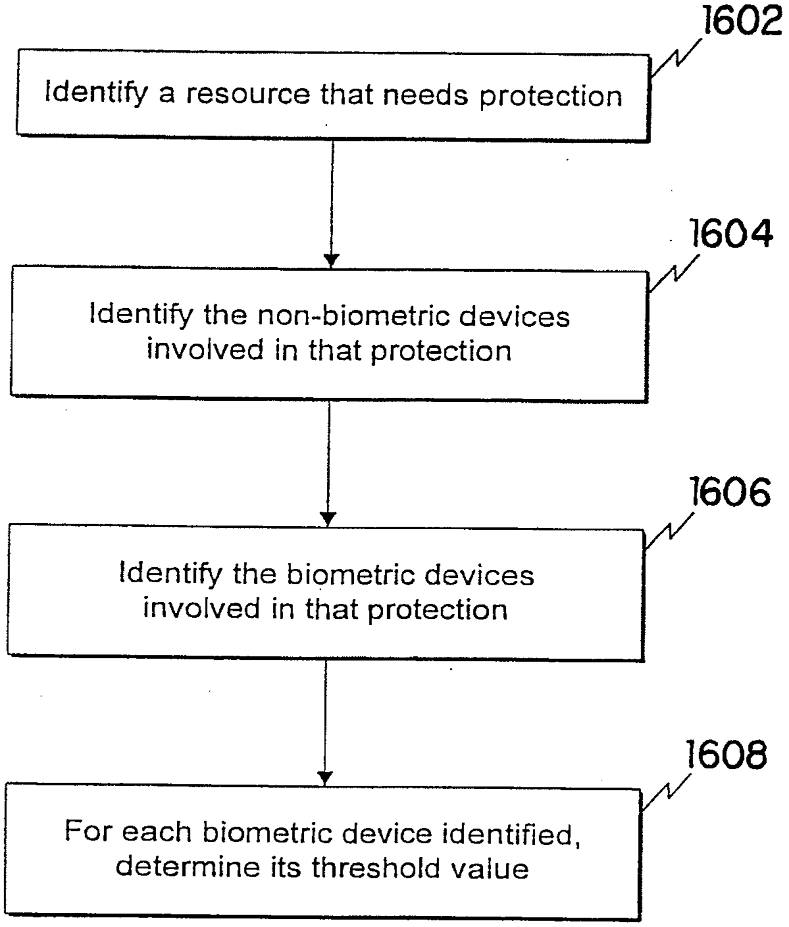

1602
Identify a resource that needs protection
1604
Identify the non-biometric devices involved in that protection
1606
Identify the biometric devices involved in that protection
1608
For each biometric device identified, determine its threshold value

FIG. 16

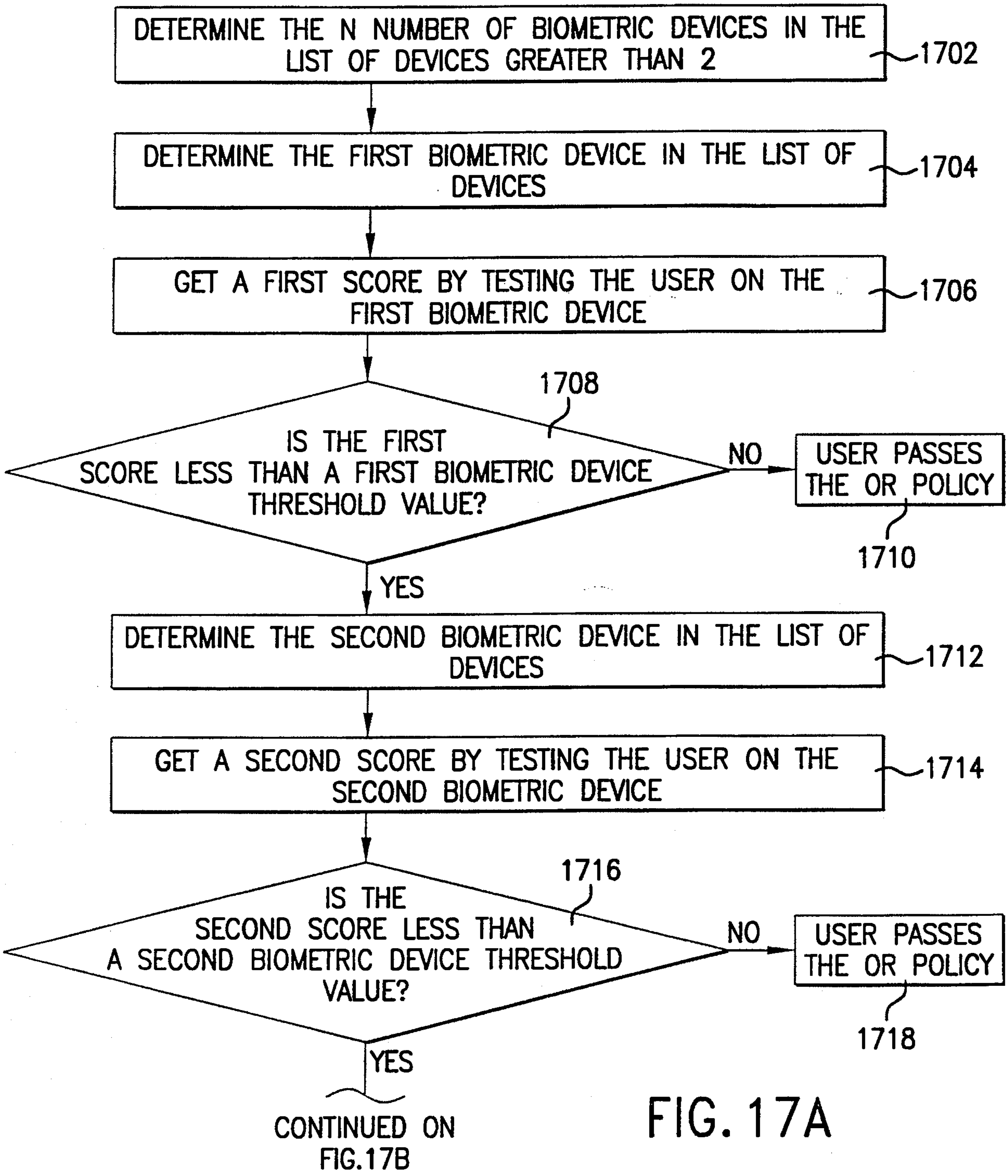

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 2
1702
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
1704
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
1706
1708
IS THE FIRST SCORE LESS THAN A FIRST BIOMETRIC DEVICE THRESHOLD VALUE?
NO
USER PASSES THE OR POLICY
1710
YES
DETERMINE THE SECOND BIOMETRIC DEVICE IN THE LIST OF DEVICES
1712
GET A SECOND SCORE BY TESTING THE USER ON THE SECOND BIOMETRIC DEVICE
1714
1716
IS THE SECOND SCORE LESS THAN A SECOND BIOMETRIC DEVICE THRESHOLD VALUE?
NO
USER PASSES THE OR POLICY
1718
YES
CONTINUED ON FIG.17B

FIG. 17A

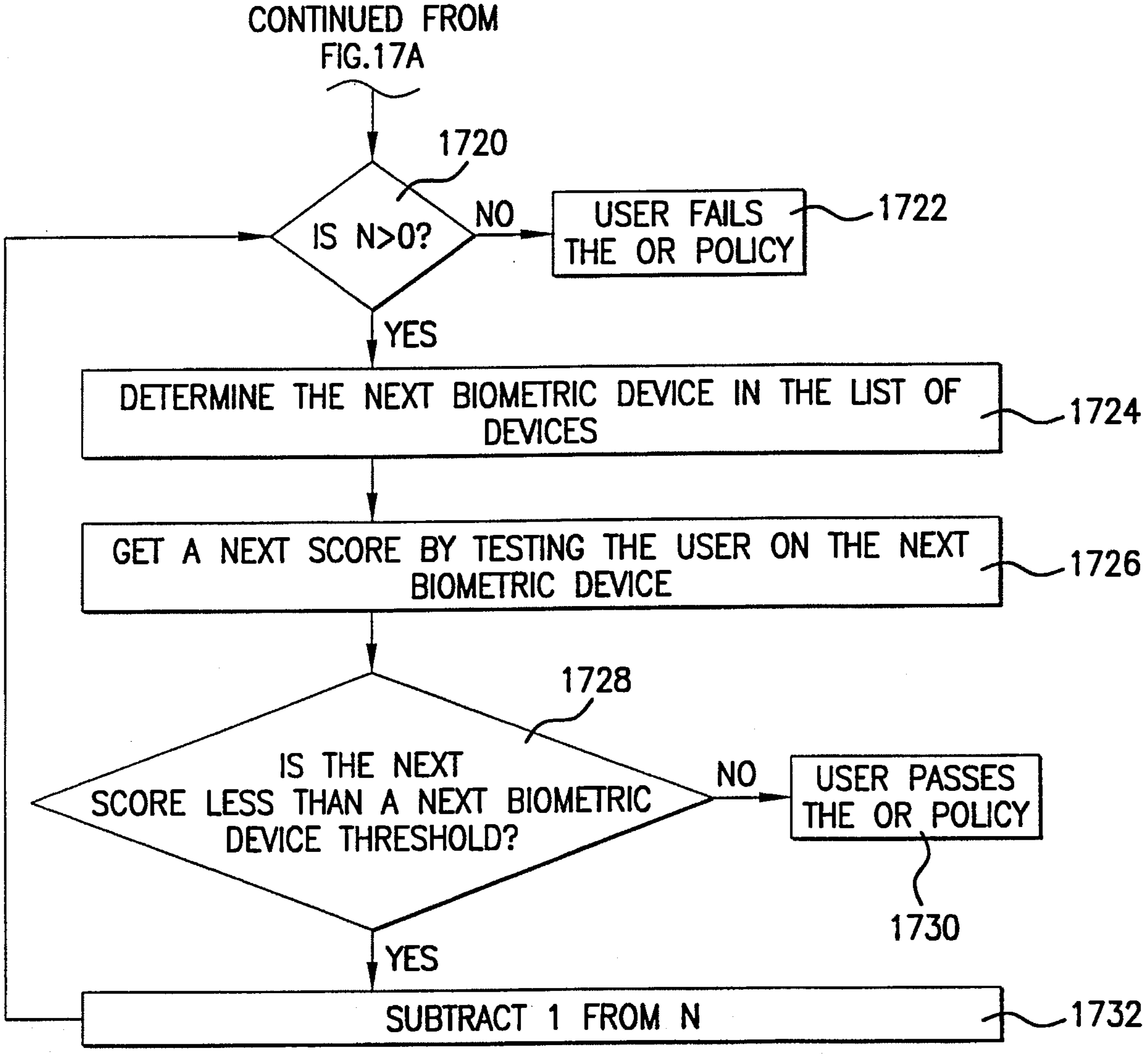

CONTINUED FROM FIG.17A
1720
IS N>0?
NO
USER FAILS THE OR POLICY
1722
YES
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
1724
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
1726
1728
IS THE NEXT SCORE LESS THAN A NEXT BIOMETRIC DEVICE THRESHOLD?
NO
USER PASSES THE OR POLICY
1730
YES
SUBTRACT 1 FROM N
1732

FIG. 17B

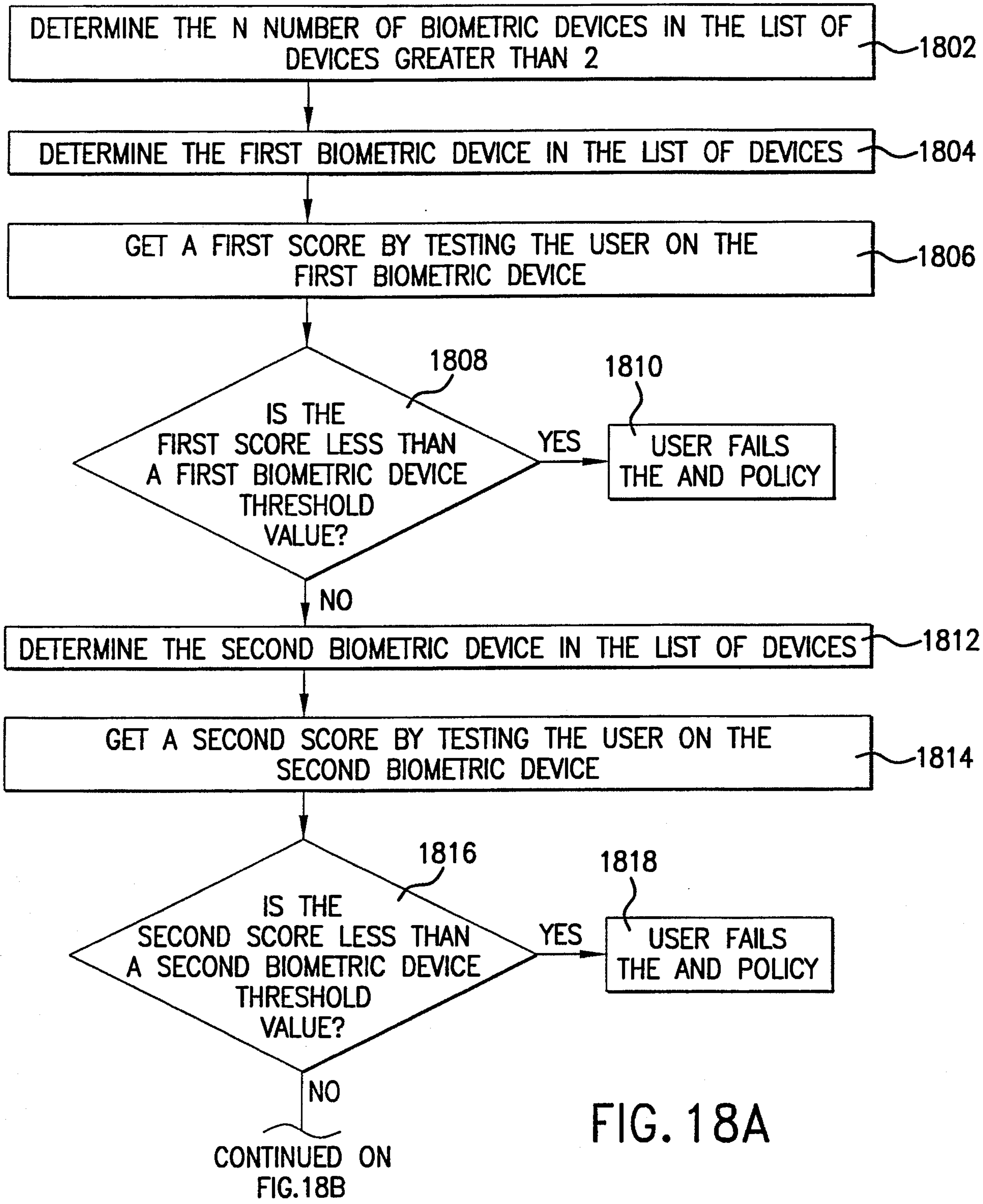

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 2
1802
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
1804
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
1806
1808
IS THE FIRST SCORE LESS THAN A FIRST BIOMETRIC DEVICE THRESHOLD VALUE?
YES
1810
USER FAILS THE AND POLICY
NO
DETERMINE THE SECOND BIOMETRIC DEVICE IN THE LIST OF DEVICES
1812
GET A SECOND SCORE BY TESTING THE USER ON THE SECOND BIOMETRIC DEVICE
1814
1816
IS THE SECOND SCORE LESS THAN A SECOND BIOMETRIC DEVICE THRESHOLD VALUE?
YES
1818
USER FAILS THE AND POLICY
NO
CONTINUED ON FIG.18B

FIG. 18A

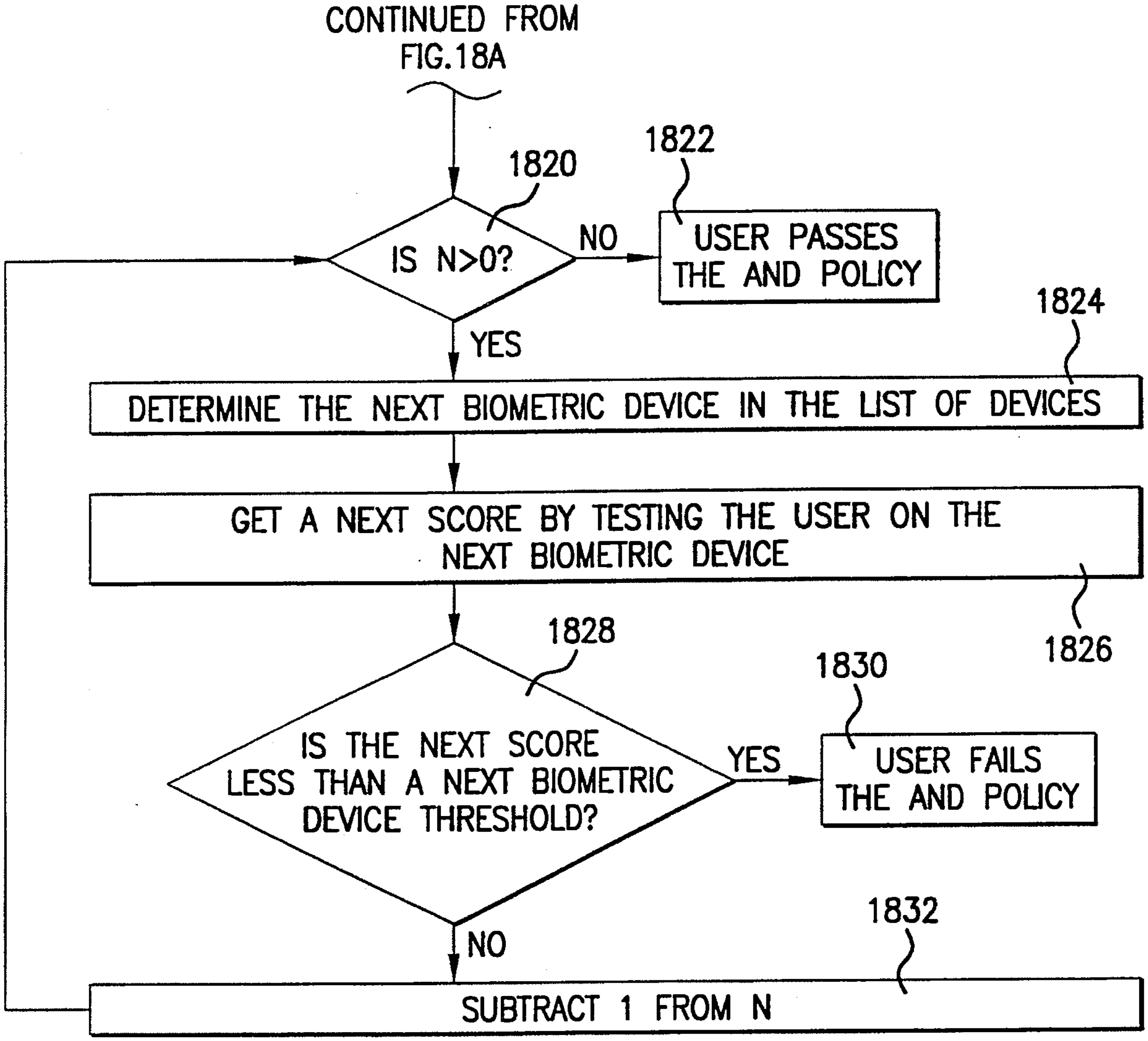

CONTINUED FROM FIG.18A
1820
1822
IS N>0?
NO
USER PASSES THE AND POLICY
YES
1824
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
1826
1828
1830
IS THE NEXT SCORE LESS THAN A NEXT BIOMETRIC DEVICE THRESHOLD?
YES
USER FAILS THE AND POLICY
NO
1832
SUBTRACT 1 FROM N

FIG. 18B

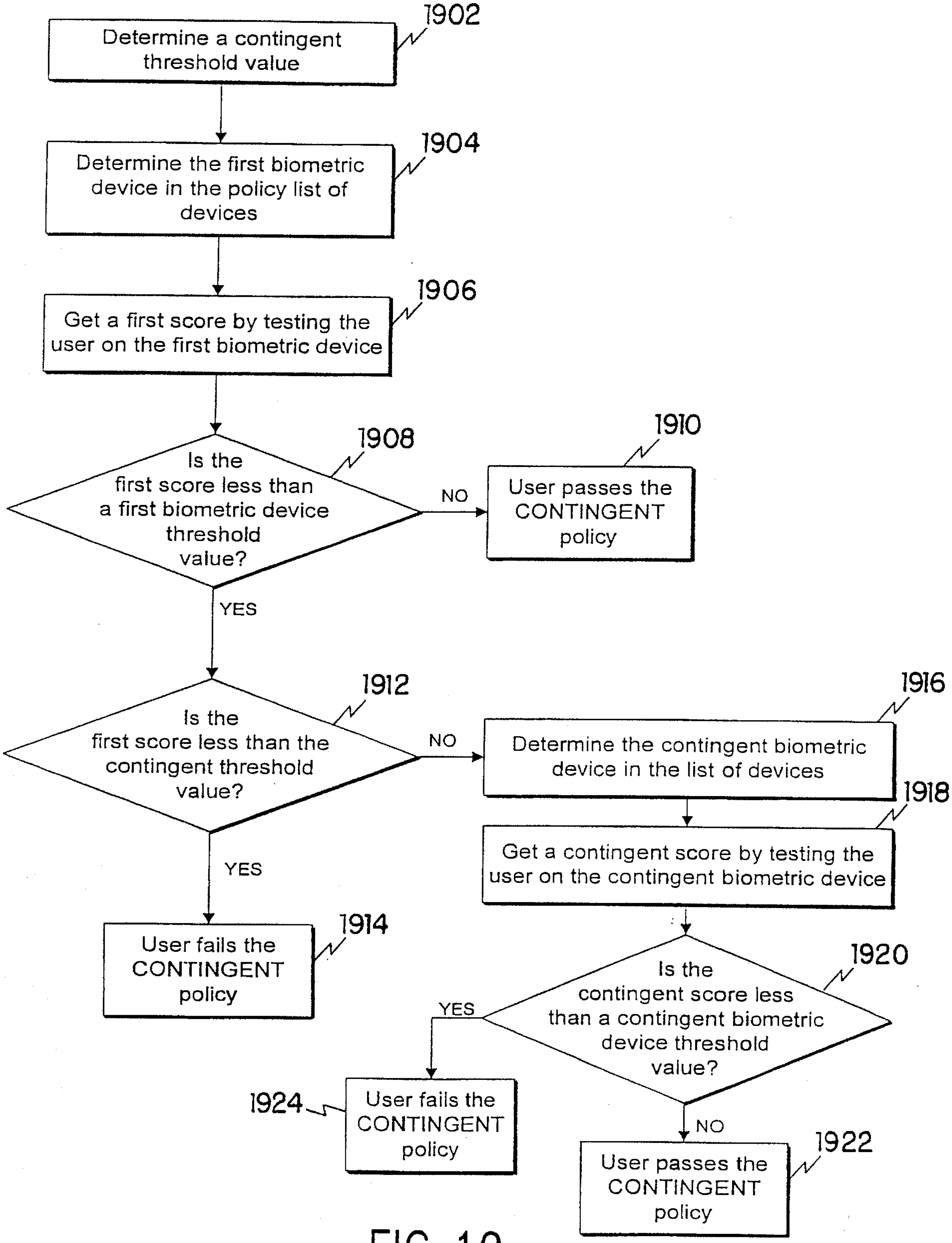

1902
Determine a contingent threshold value
1904
Determine the first biometric device in the policy list of devices
1906
Get a first score by testing the user on the first biometric device
1908
Is the first score less than a first biometric device threshold value?
NO
1910
User passes the CONTINGENT policy
YES
1912
Is the first score less than the contingent threshold value?
NO
1916
Determine the contingent biometric device in the list of devices
1918
Get a contingent score by testing the user on the contingent biometric device
YES
1914
User fails the CONTINGENT policy
1920
Is the contingent score less than a contingent biometric device threshold value?
YES
1924
User fails the CONTINGENT policy
NO
1922
User passes the CONTINGENT policy

FIG. 19

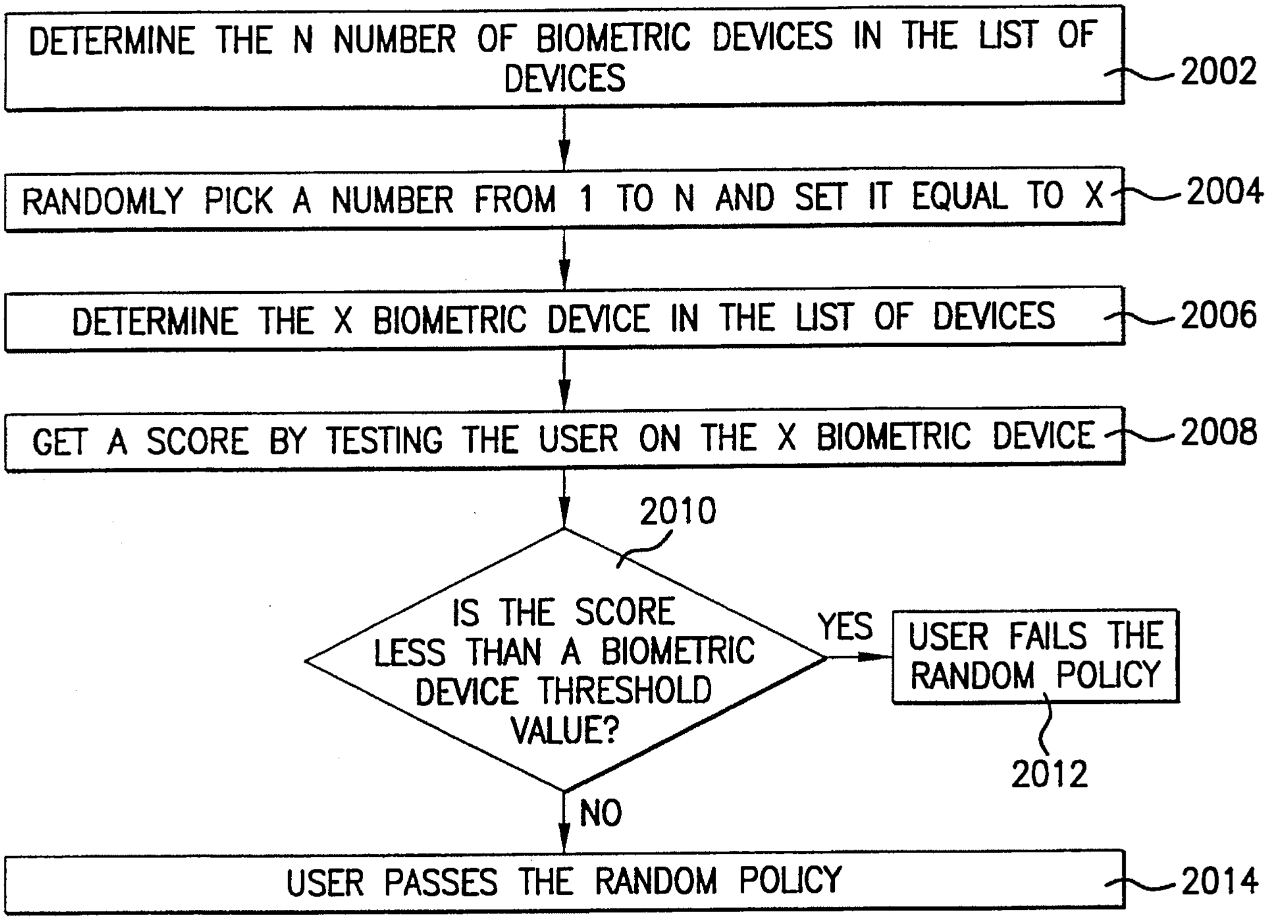

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES
2002
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2004
DETERMINE THE X BIOMETRIC DEVICE IN THE LIST OF DEVICES
2006
GET A SCORE BY TESTING THE USER ON THE X BIOMETRIC DEVICE
2008
2010
IS THE SCORE LESS THAN A BIOMETRIC DEVICE THRESHOLD VALUE?
YES
USER FAILS THE RANDOM POLICY
2012
NO
USER PASSES THE RANDOM POLICY
2014

FIG. 20

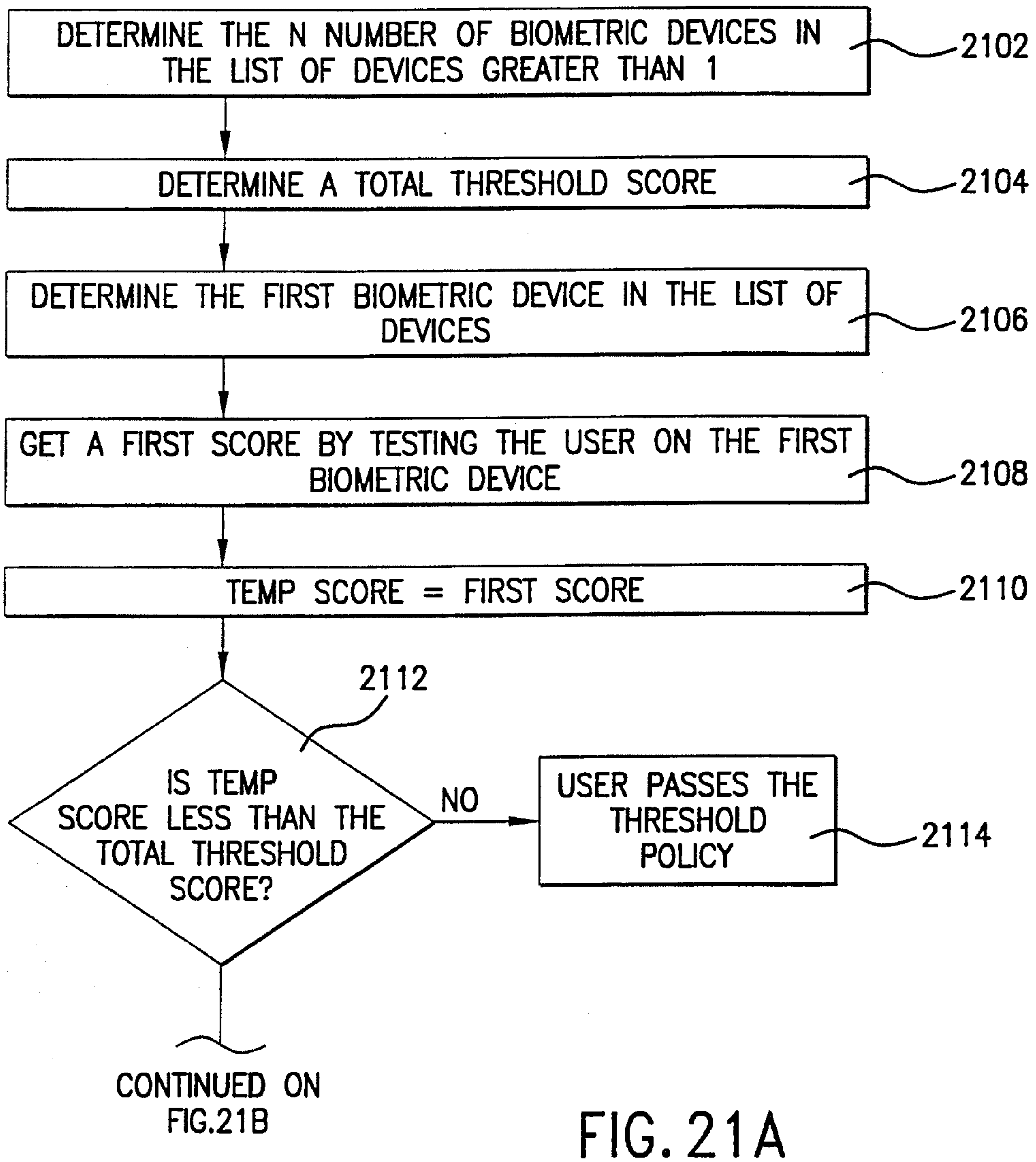

DETERMINE THE N NUMBER OF BIOMETRIC DEVICES IN THE LIST OF DEVICES GREATER THAN 1
2102
DETERMINE A TOTAL THRESHOLD SCORE
2104
DETERMINE THE FIRST BIOMETRIC DEVICE IN THE LIST OF DEVICES
2106
GET A FIRST SCORE BY TESTING THE USER ON THE FIRST BIOMETRIC DEVICE
2108
TEMP SCORE = FIRST SCORE
2110
2112
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY
2114
CONTINUED ON FIG.21B

FIG. 21A

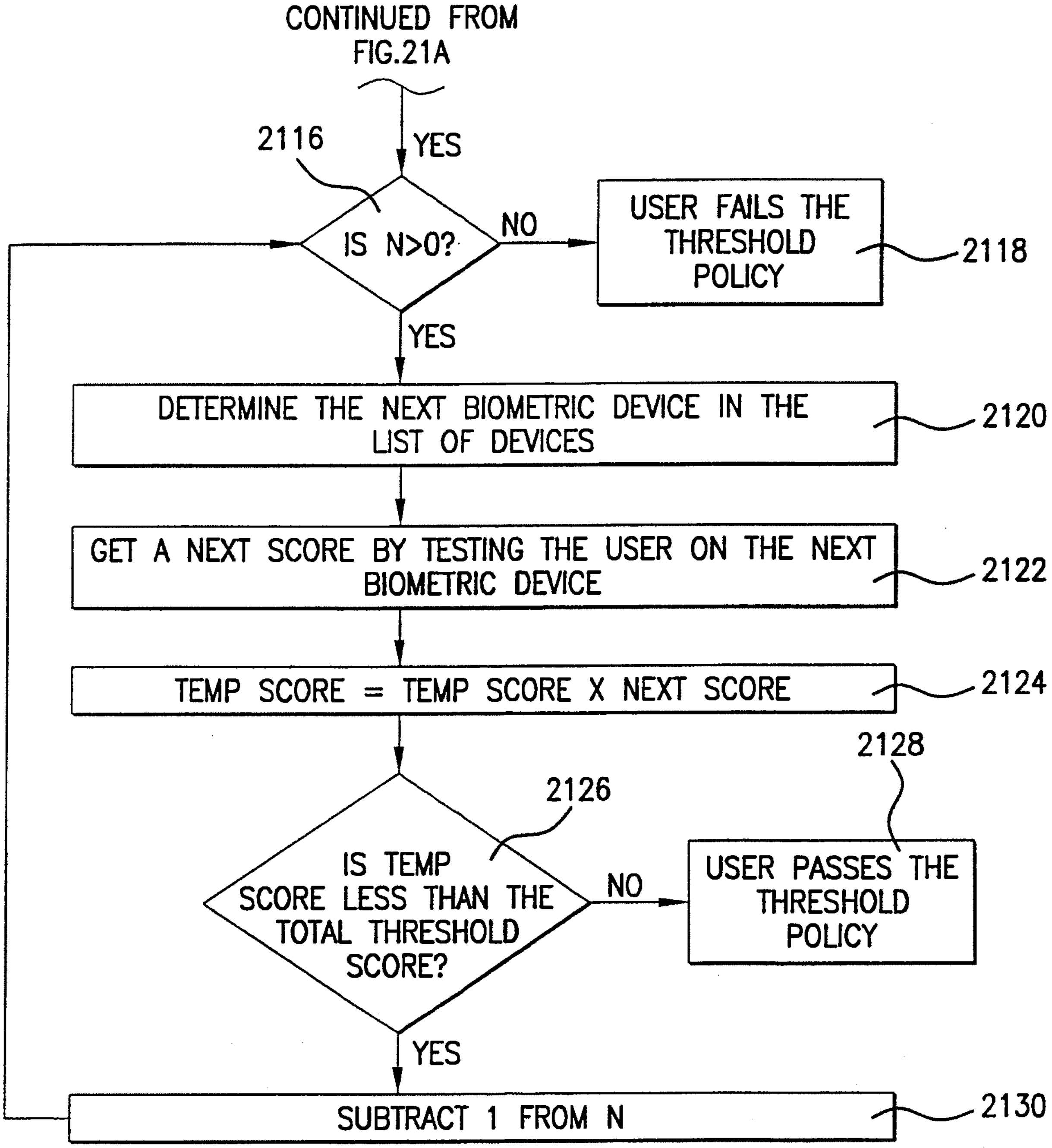

CONTINUED FROM FIG.21A
YES
2116
IS N>0?
NO
USER FAILS THE THRESHOLD POLICY
2118
YES
DETERMINE THE NEXT BIOMETRIC DEVICE IN THE LIST OF DEVICES
2120
GET A NEXT SCORE BY TESTING THE USER ON THE NEXT BIOMETRIC DEVICE
2122
TEMP SCORE = TEMP SCORE X NEXT SCORE
2124
2128
2126
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY
YES
SUBTRACT 1 FROM N
2130

FIG. 21B

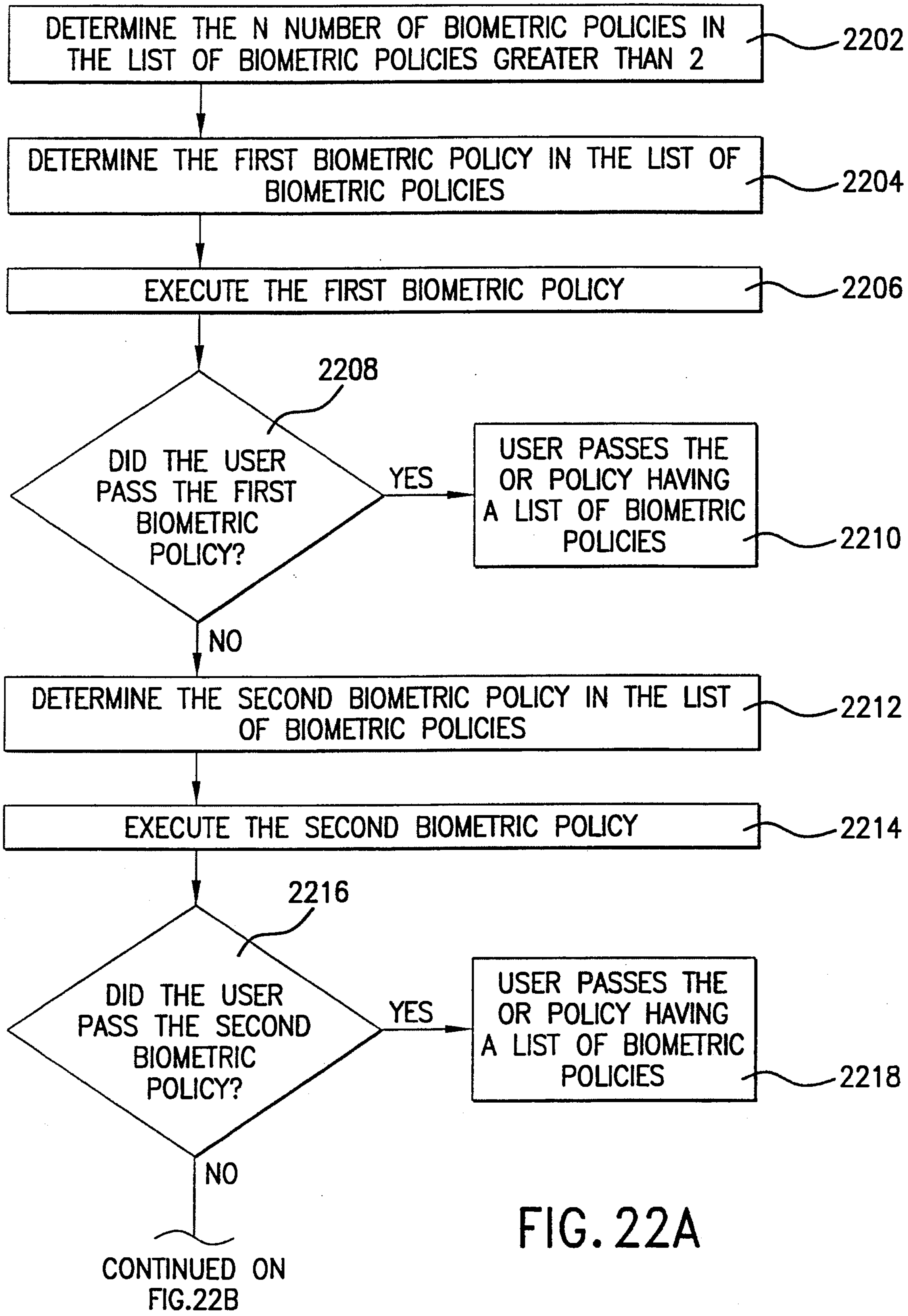

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 2
2202
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2204
EXECUTE THE FIRST BIOMETRIC POLICY
2206
2208
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2210
NO
DETERMINE THE SECOND BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2212
EXECUTE THE SECOND BIOMETRIC POLICY
2214
2216
DID THE USER PASS THE SECOND BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2218
NO
CONTINUED ON FIG.22B

FIG. 22A

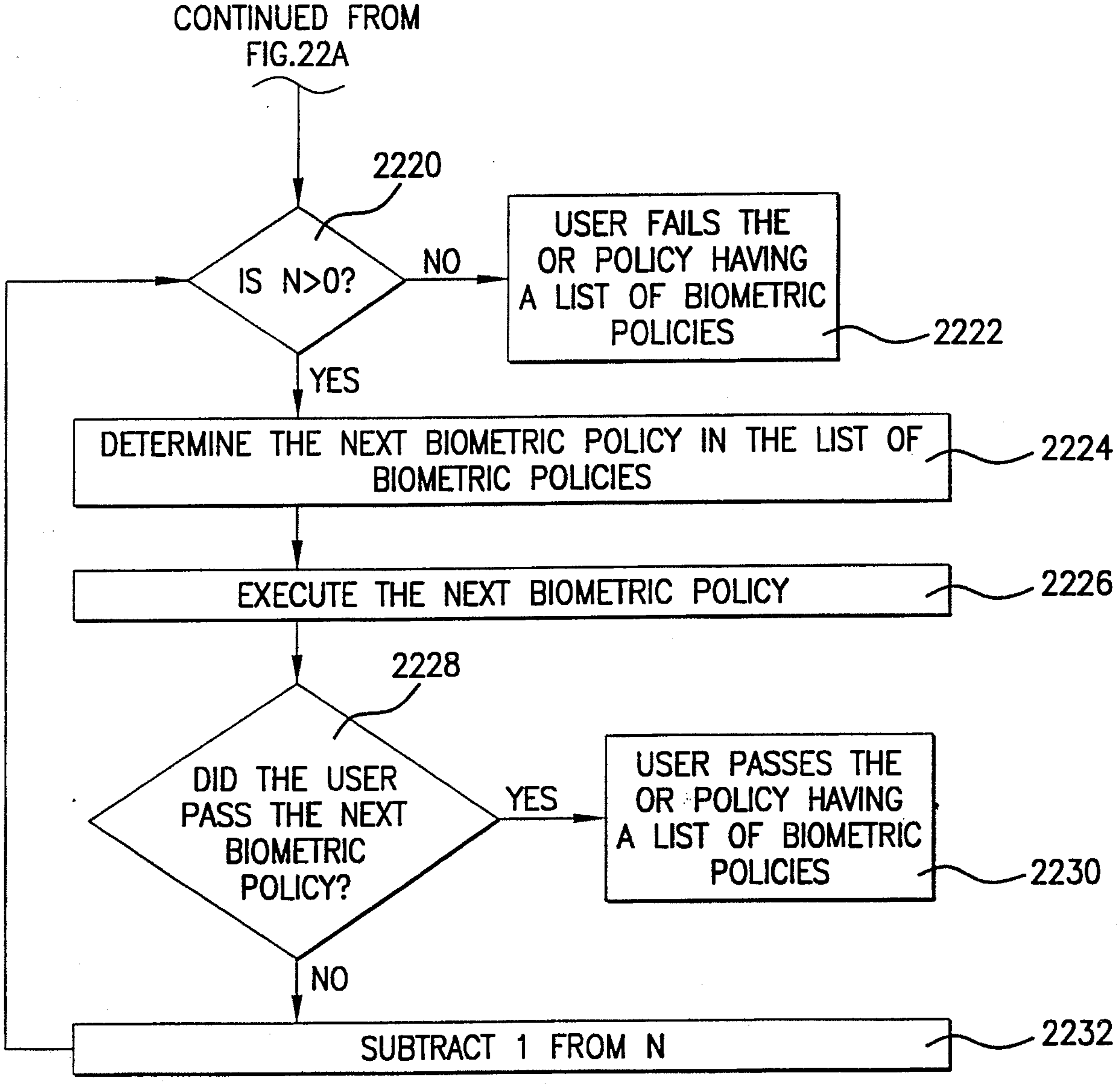

CONTINUED FROM FIG.22A
2220
IS N>0?
NO
USER FAILS THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2222
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2224
EXECUTE THE NEXT BIOMETRIC POLICY
2226
2228
DID THE USER PASS THE NEXT BIOMETRIC POLICY?
YES
USER PASSES THE OR POLICY HAVING A LIST OF BIOMETRIC POLICIES
2230
NO
SUBTRACT 1 FROM N
2232

FIG. 22B

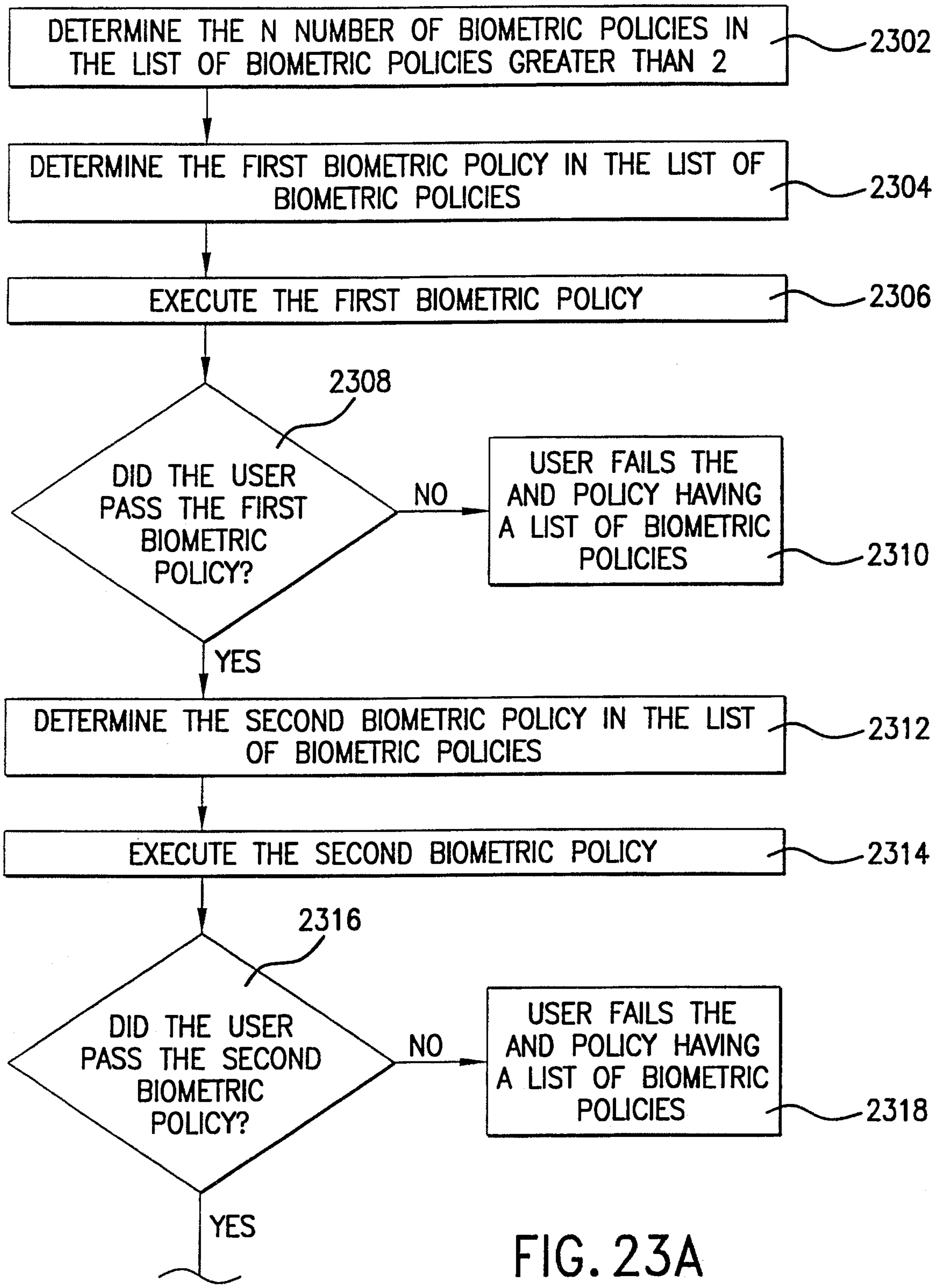

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 2
2302
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2304
EXECUTE THE FIRST BIOMETRIC POLICY
2306
2308
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2310
YES
DETERMINE THE SECOND BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2312
EXECUTE THE SECOND BIOMETRIC POLICY
2314
2316
DID THE USER PASS THE SECOND BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2318
YES

FIG. 23A

CONTINUED ON FIG.23B

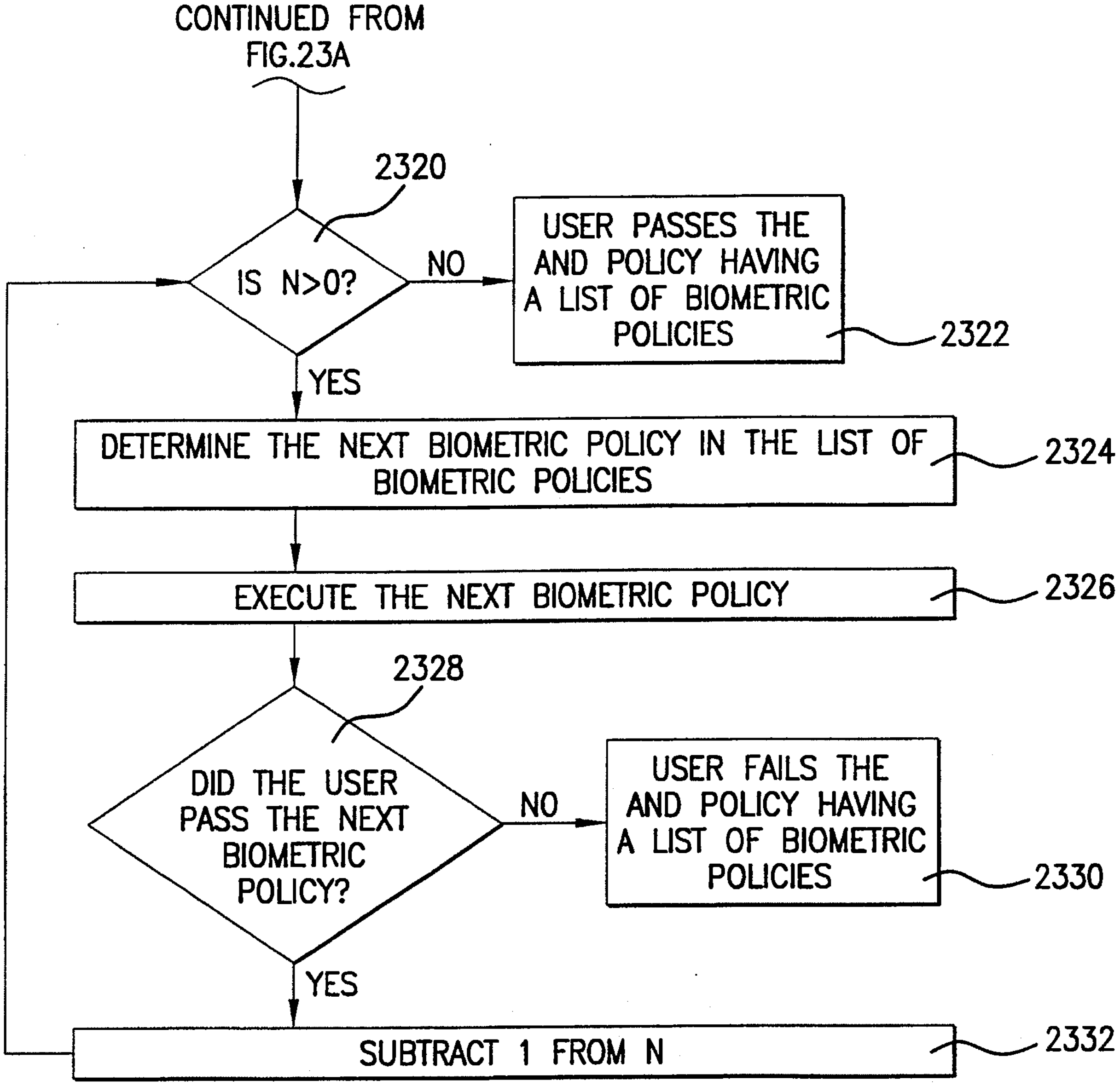

CONTINUED FROM FIG.23A
2320
IS N>0?
NO
USER PASSES THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2322
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2324
EXECUTE THE NEXT BIOMETRIC POLICY
2326
2328
DID THE USER PASS THE NEXT BIOMETRIC POLICY?
NO
USER FAILS THE AND POLICY HAVING A LIST OF BIOMETRIC POLICIES
2330
YES
SUBTRACT 1 FROM N
2332

FIG. 23B

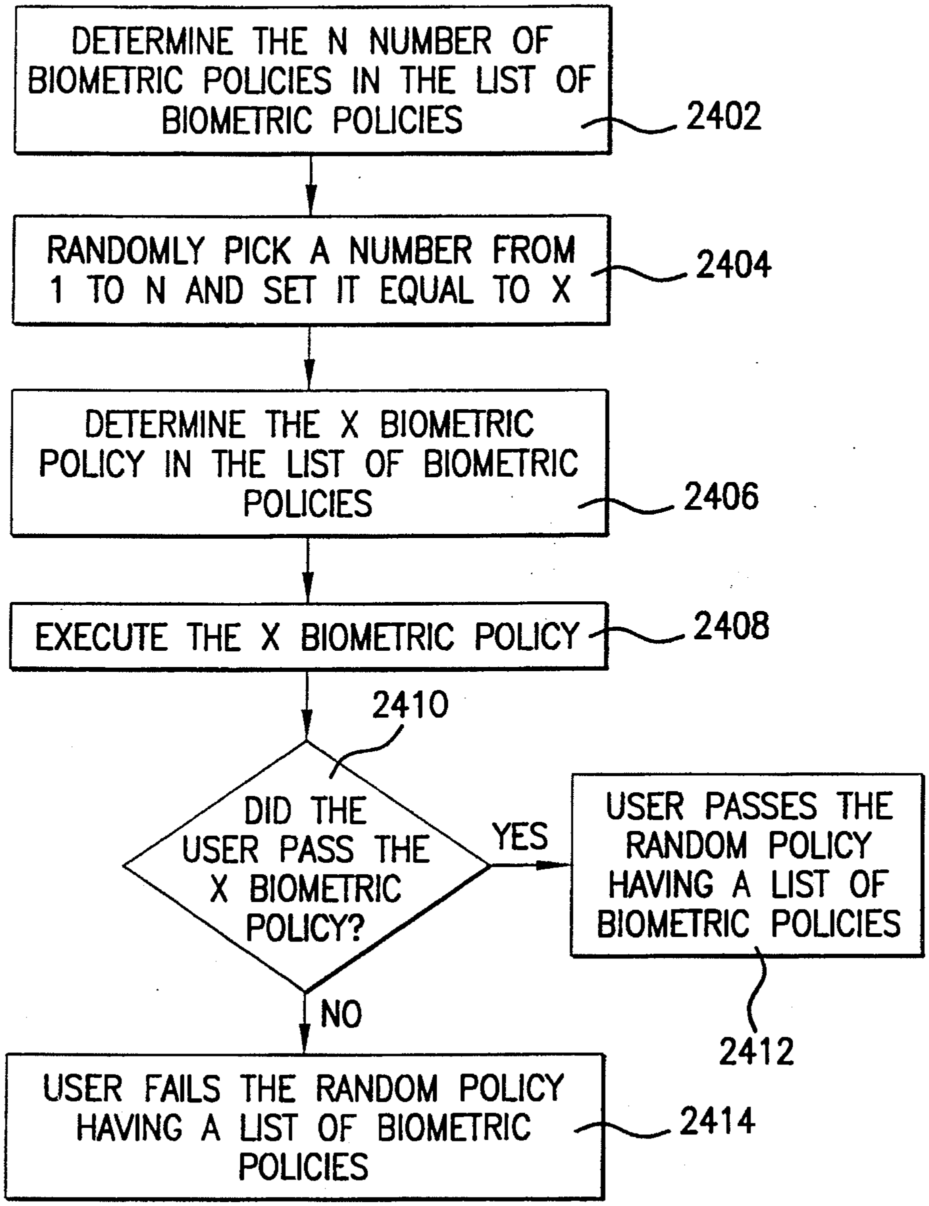
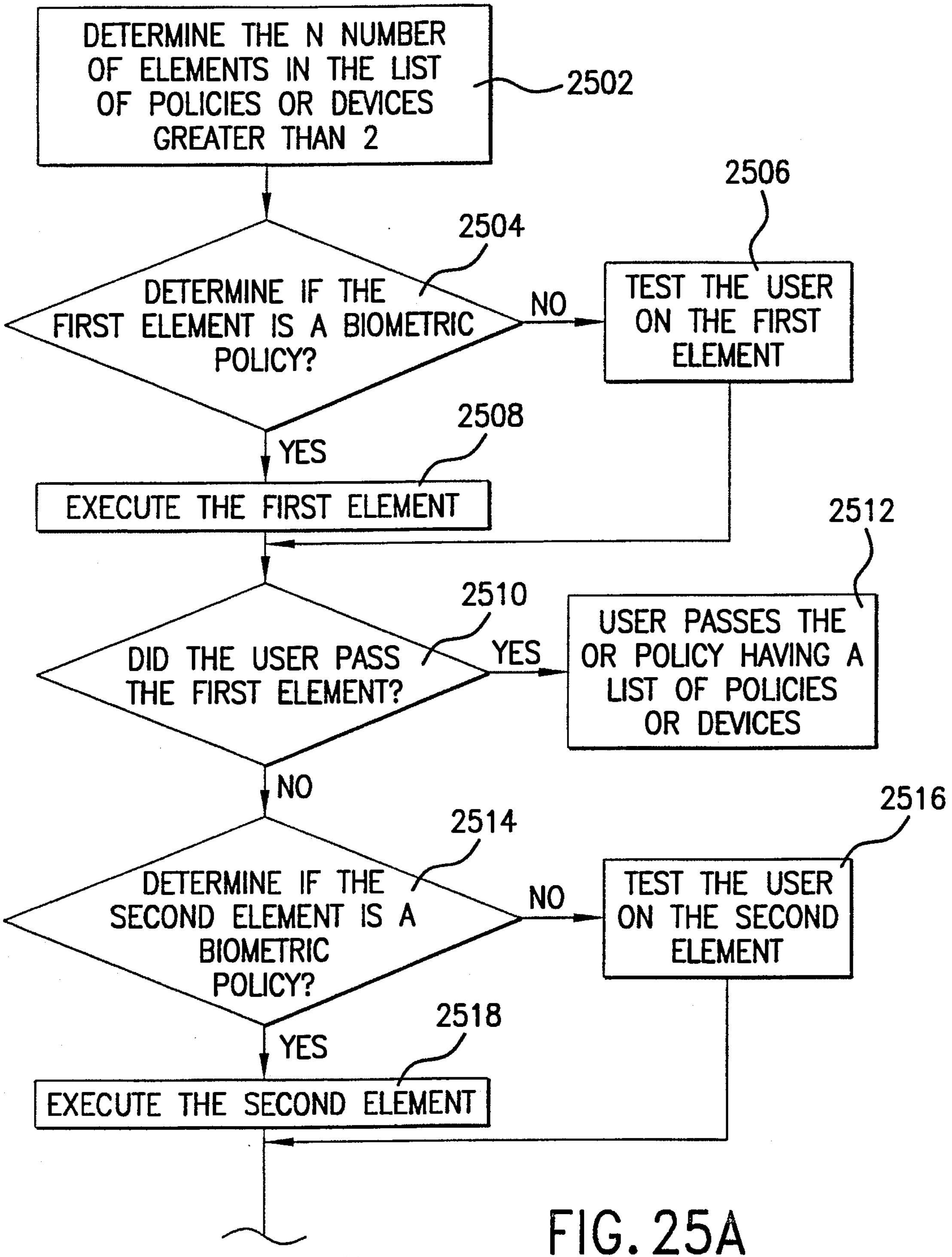

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES
2402
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2404
DETERMINE THE X BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
2406
EXECUTE THE X BIOMETRIC POLICY
2408
2410
DID THE USER PASS THE X BIOMETRIC POLICY?
YES
USER PASSES THE RANDOM POLICY HAVING A LIST OF BIOMETRIC POLICIES
2412
NO
USER FAILS THE RANDOM POLICY HAVING A LIST OF BIOMETRIC POLICIES
2414

FIG. 24


DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 2
2502
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
2504
NO
TEST THE USER ON THE FIRST ELEMENT
2506
YES
EXECUTE THE FIRST ELEMENT
2508
DID THE USER PASS THE FIRST ELEMENT?
2510
YES
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
2512
NO
DETERMINE IF THE SECOND ELEMENT IS A BIOMETRIC POLICY?
2514
NO
TEST THE USER ON THE SECOND ELEMENT
2516
YES
EXECUTE THE SECOND ELEMENT
2518

CONTINUED ON FIG.25B

FIG. 25A

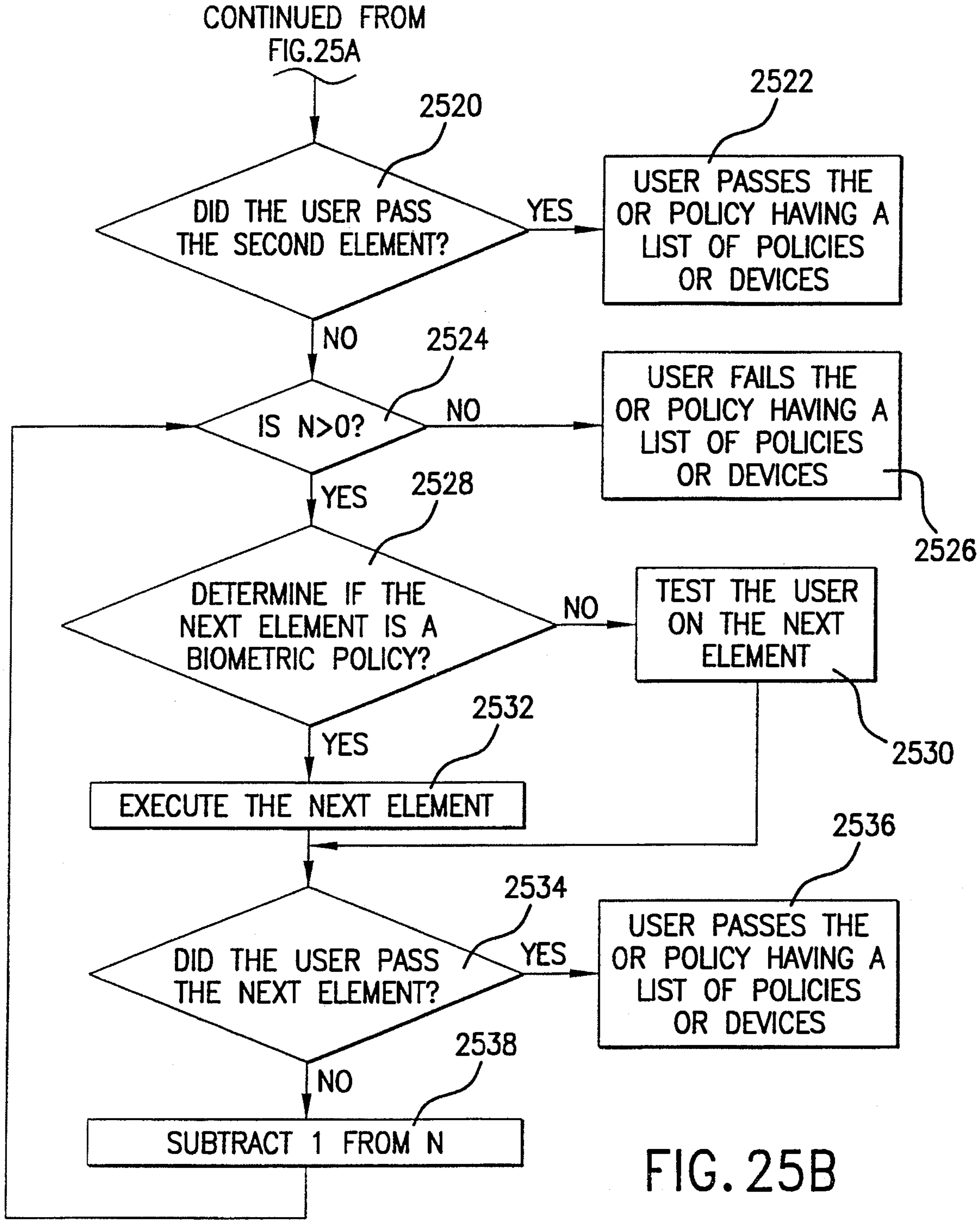
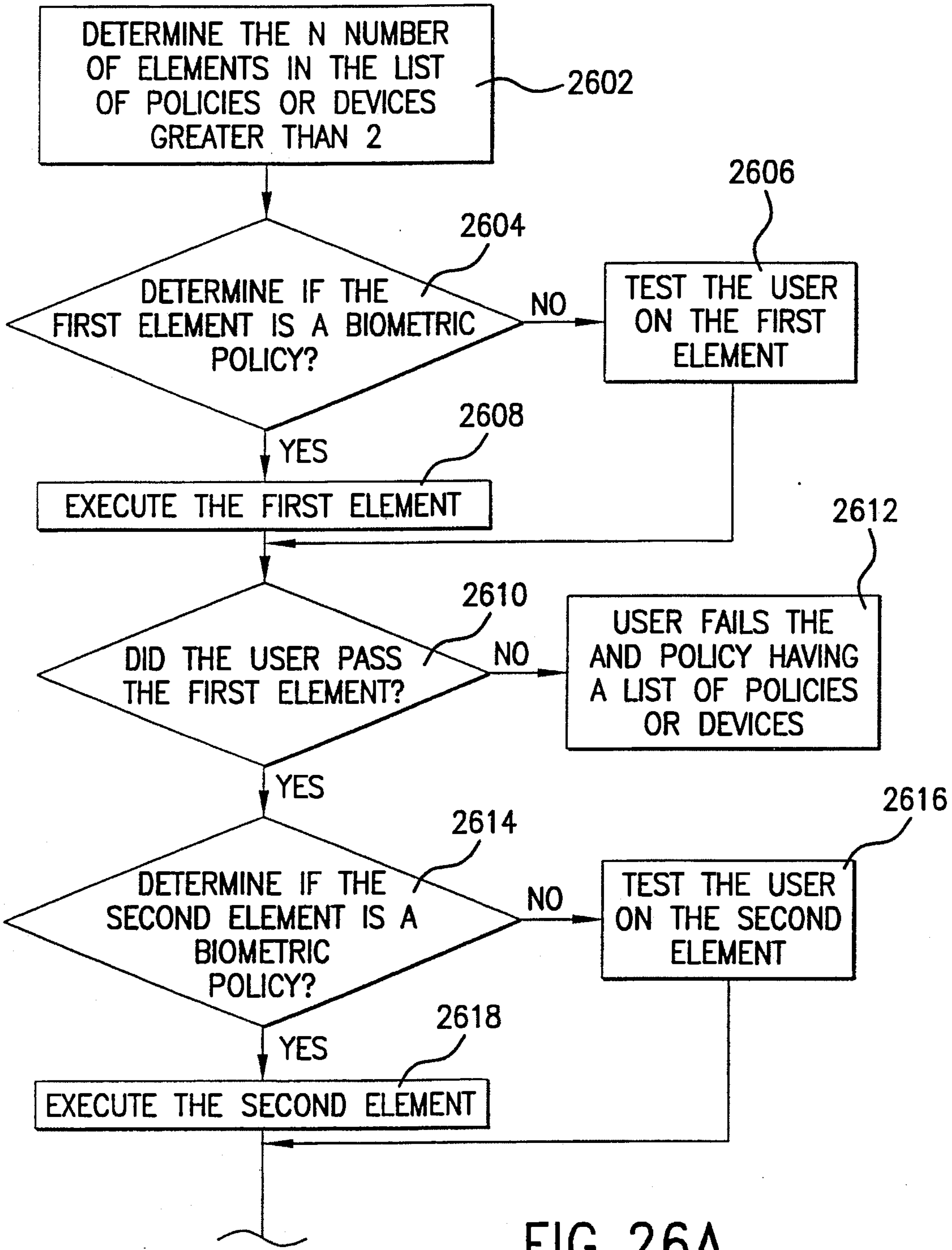

CONTINUED FROM FIG.25A
2520
DID THE USER PASS THE SECOND ELEMENT?
YES
2522
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
2524
IS N>0?
NO
USER FAILS THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
2526
YES
2528
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE NEXT ELEMENT
2530
YES
2532
EXECUTE THE NEXT ELEMENT
2536
2534
DID THE USER PASS THE NEXT ELEMENT?
YES
USER PASSES THE OR POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
2538
SUBTRACT 1 FROM N

FIG. 25B


DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 2
2602
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
2604
NO
TEST THE USER ON THE FIRST ELEMENT
2606
YES
EXECUTE THE FIRST ELEMENT
2608
DID THE USER PASS THE FIRST ELEMENT?
2610
NO
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
2612
YES
DETERMINE IF THE SECOND ELEMENT IS A BIOMETRIC POLICY?
2614
NO
TEST THE USER ON THE SECOND ELEMENT
2616
YES
EXECUTE THE SECOND ELEMENT
2618

CONTINUED ON FIG.26B

FIG. 26A

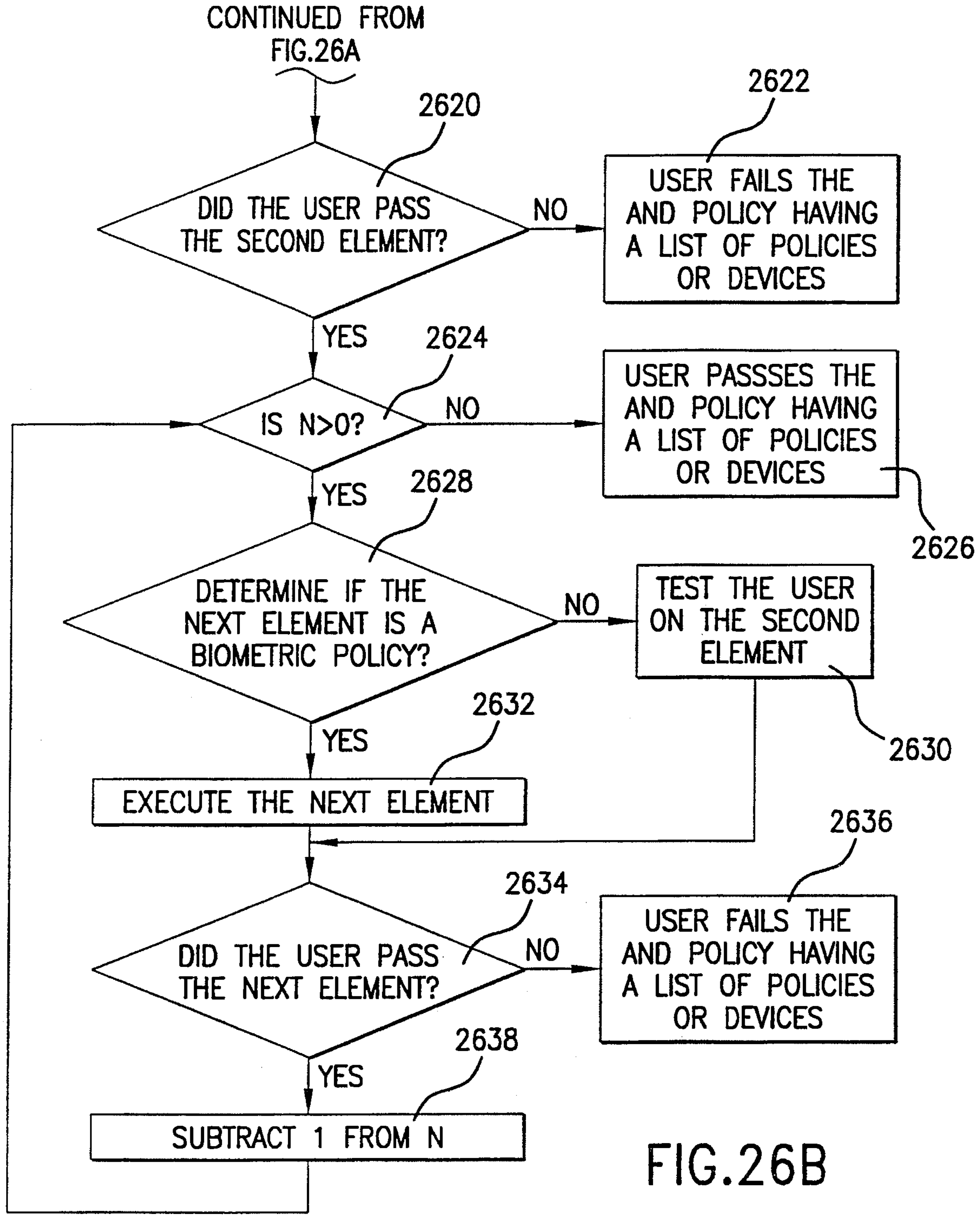

CONTINUED FROM FIG.26A
2620
DID THE USER PASS THE SECOND ELEMENT?
NO
2622
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
YES
2624
IS N>0?
NO
USER PASSSES THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
2626
YES
2628
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE SECOND ELEMENT
2630
YES
2632
EXECUTE THE NEXT ELEMENT
2636
2634
DID THE USER PASS THE NEXT ELEMENT?
NO
USER FAILS THE AND POLICY HAVING A LIST OF POLICIES OR DEVICES
2638
YES
SUBTRACT 1 FROM N

FIG.26B

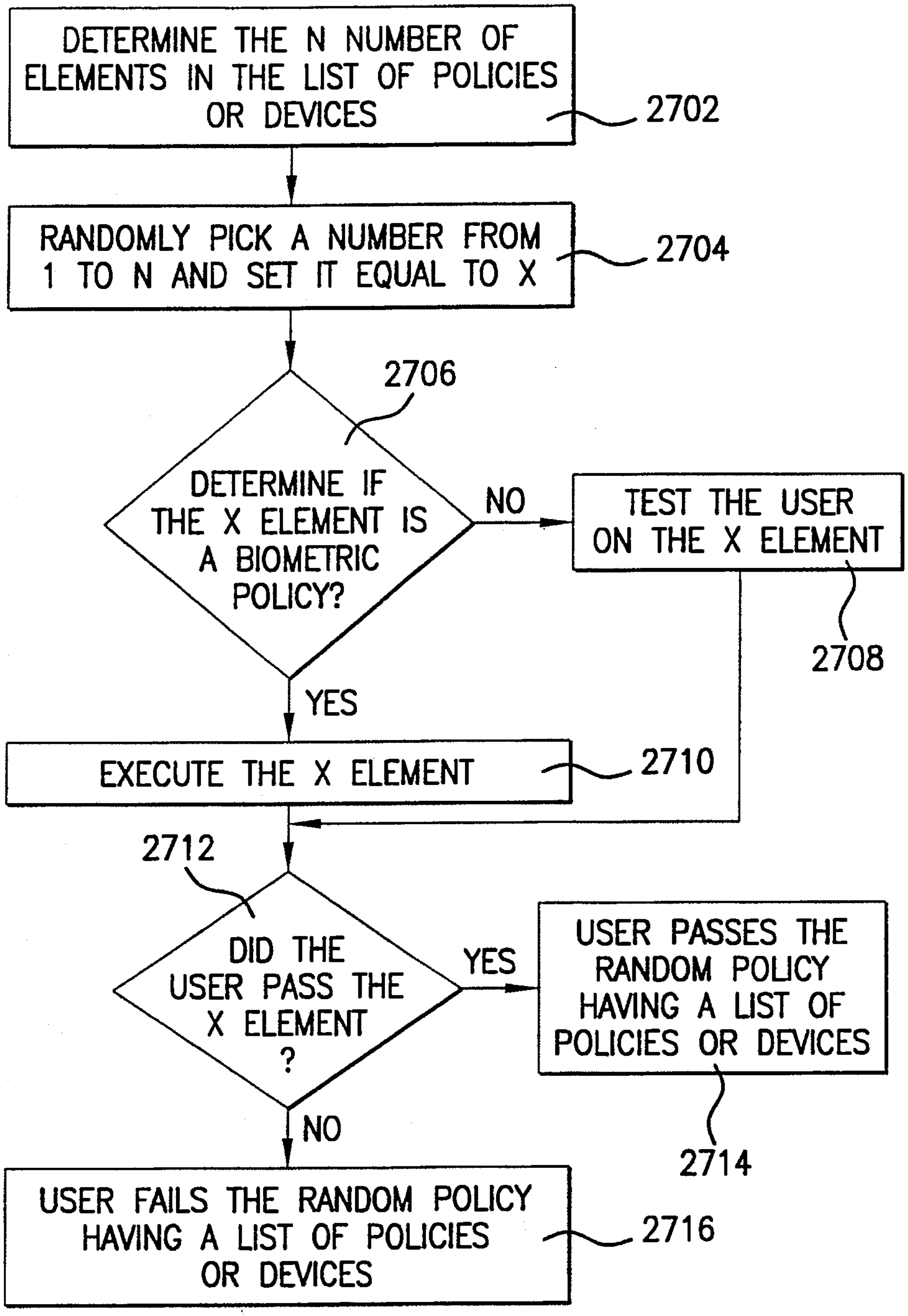

DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES
2702
RANDOMLY PICK A NUMBER FROM 1 TO N AND SET IT EQUAL TO X
2704
2706
DETERMINE IF THE X ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE X ELEMENT
2708
YES
EXECUTE THE X ELEMENT
2710
2712
DID THE USER PASS THE X ELEMENT ?
YES
USER PASSES THE RANDOM POLICY HAVING A LIST OF POLICIES OR DEVICES
2714
NO
USER FAILS THE RANDOM POLICY HAVING A LIST OF POLICIES OR DEVICES
2716

FIG. 27

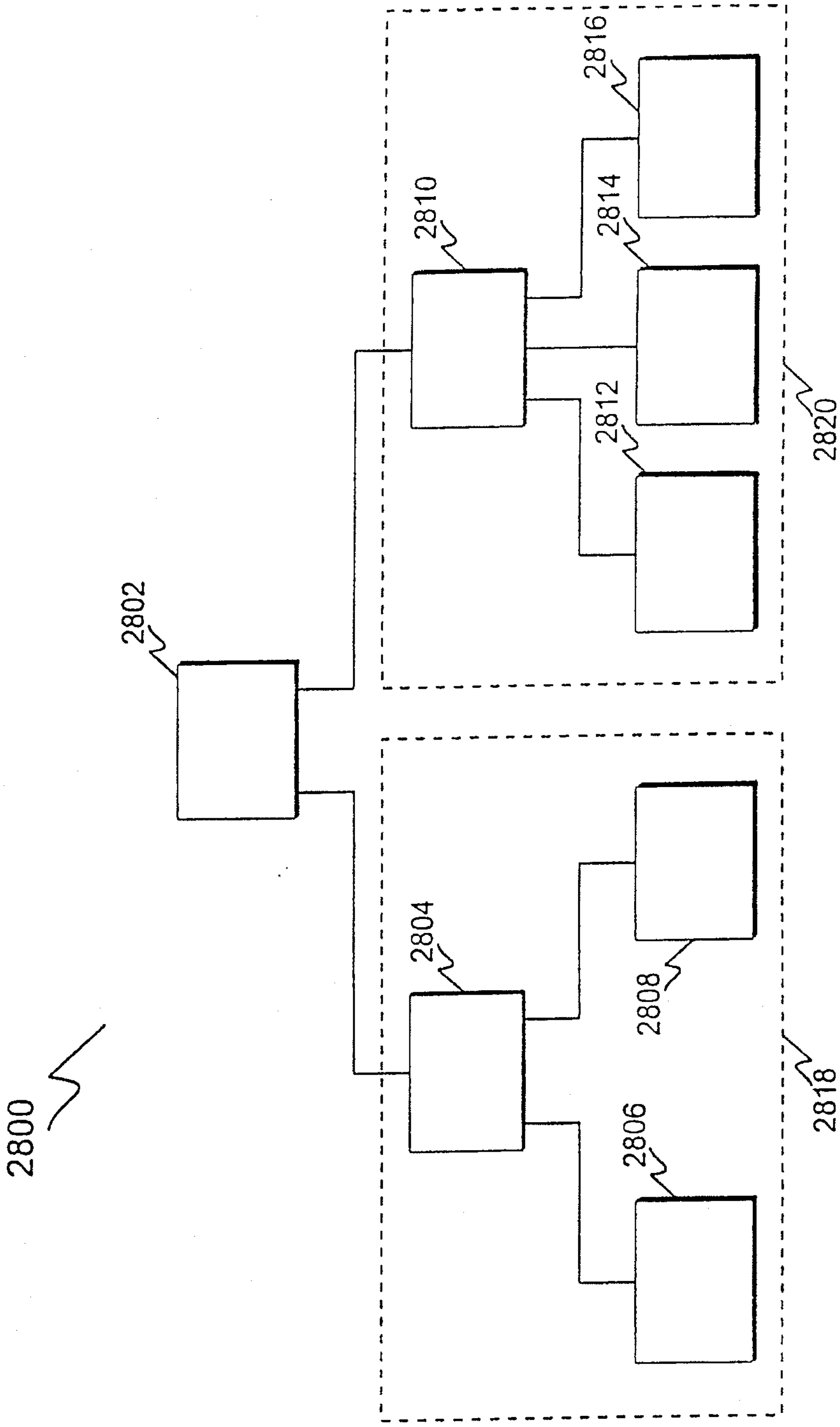


FIG. 28

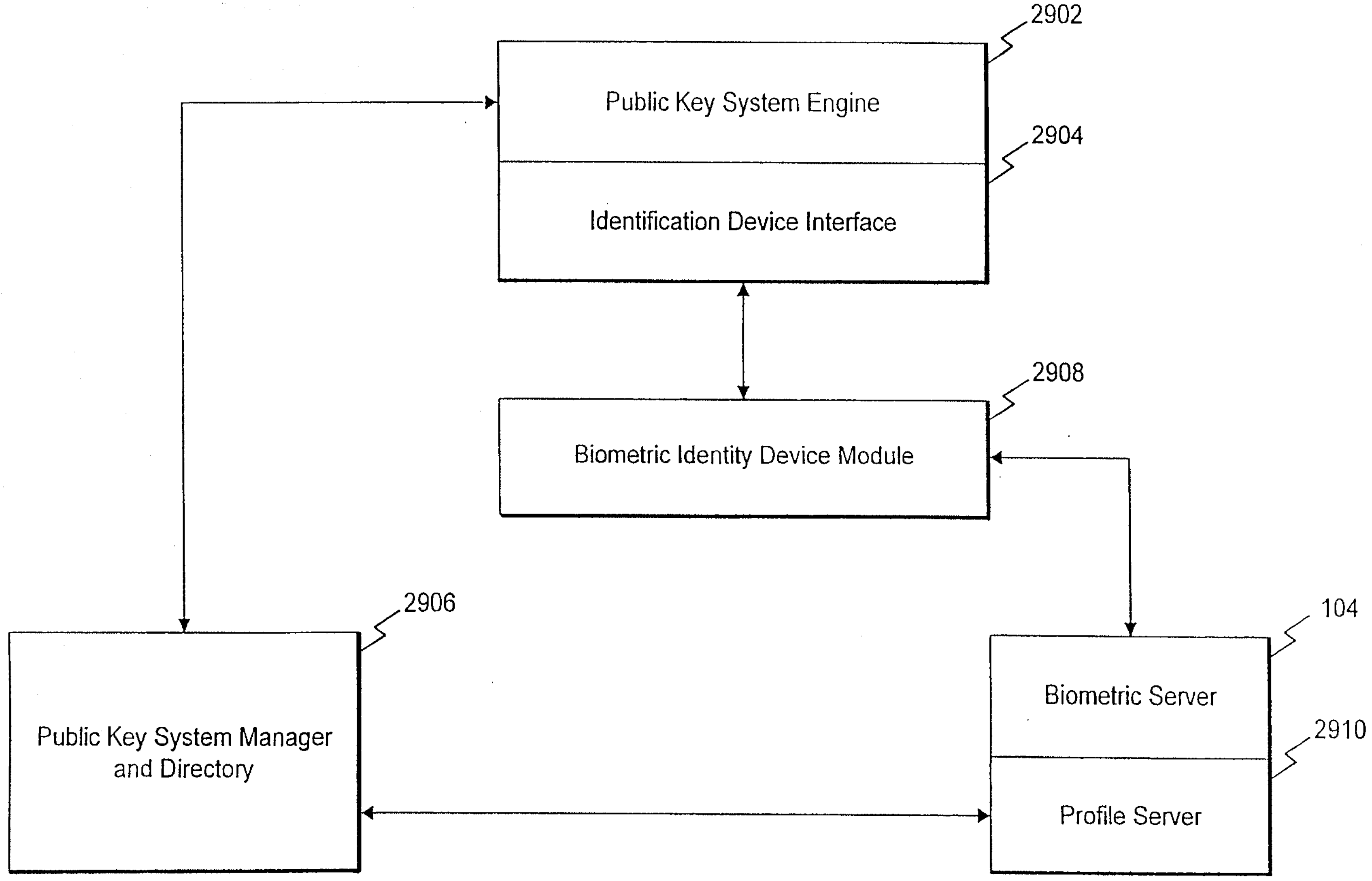

2902
Public Key System Engine
2904
Identification Device Interface
2908
Biometric Identity Device Module
2906
Public Key System Manager
and Directory
104
Biometric Server
2910
Profile Server

FIG. 29

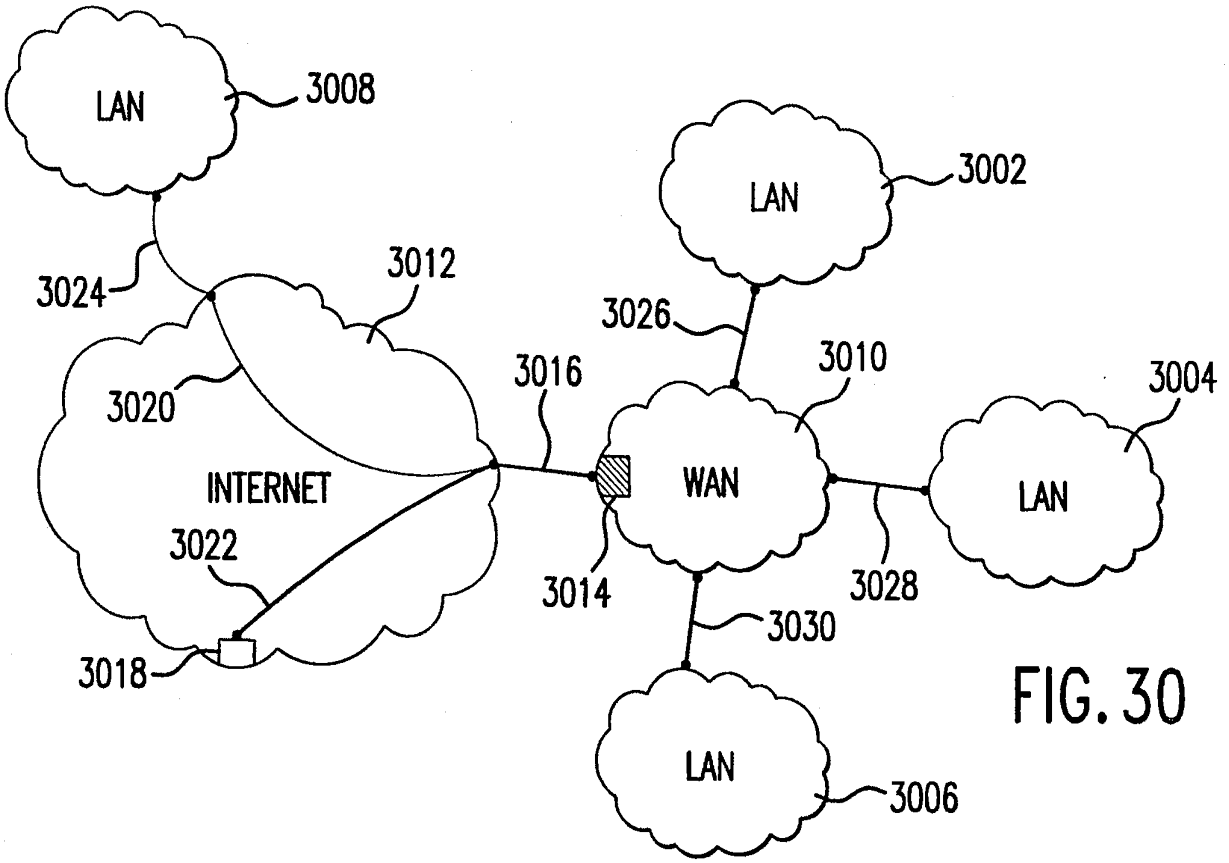

LAN
3008
LAN
3002
3024
3012
3026
3010
3004
3016
3020
INTERNET
WAN
LAN
3022
3014
3028
3030
3018
LAN
3006

FIG. 30

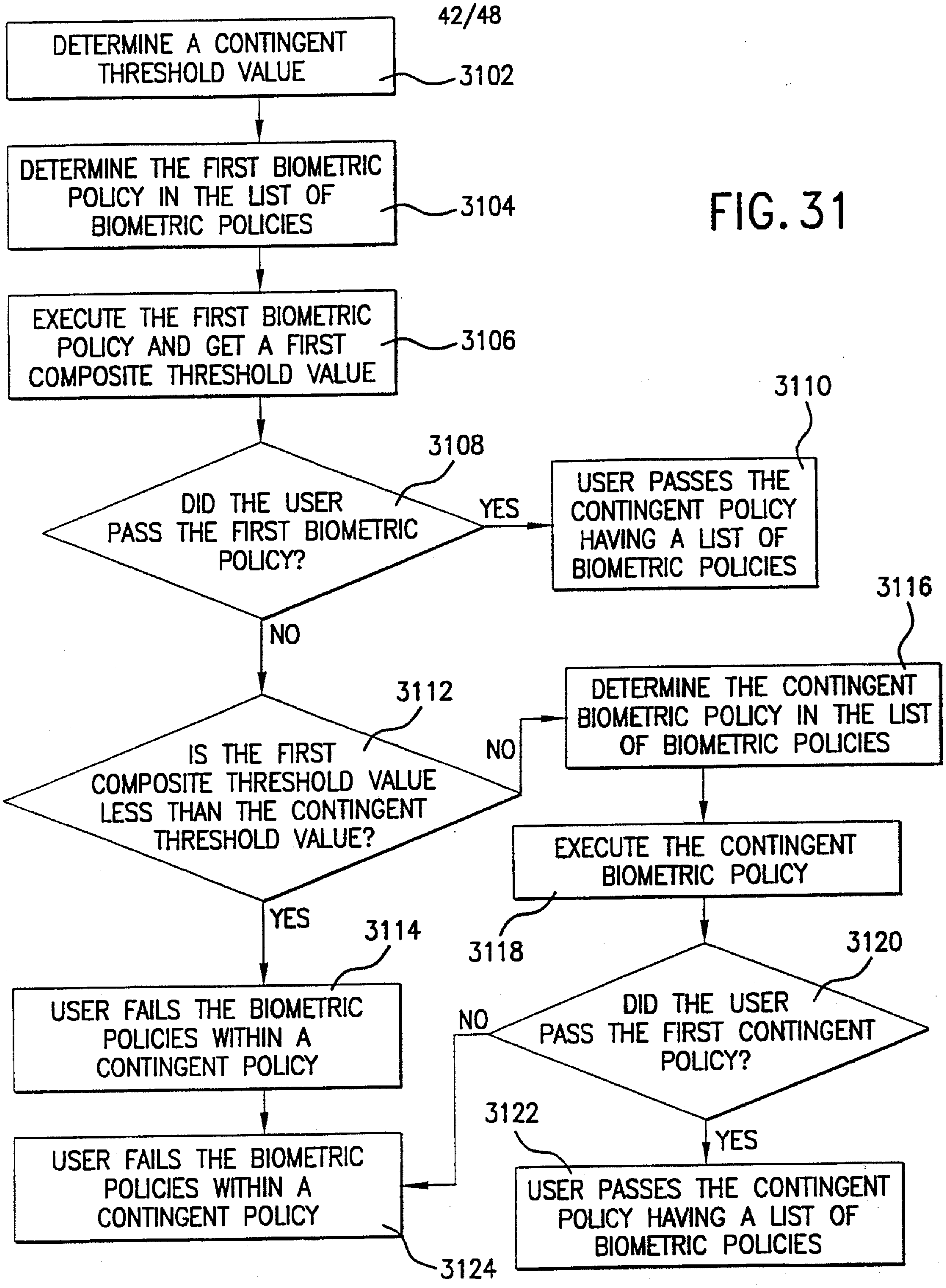

DETERMINE A CONTINGENT THRESHOLD VALUE
3102
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3104
EXECUTE THE FIRST BIOMETRIC POLICY AND GET A FIRST COMPOSITE THRESHOLD VALUE
3106
3108
DID THE USER PASS THE FIRST BIOMETRIC POLICY?
YES
3110
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF BIOMETRIC POLICIES
NO
3112
IS THE FIRST COMPOSITE THRESHOLD VALUE LESS THAN THE CONTINGENT THRESHOLD VALUE?
NO
3116
DETERMINE THE CONTINGENT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
EXECUTE THE CONTINGENT BIOMETRIC POLICY
3118
YES
3114
USER FAILS THE BIOMETRIC POLICIES WITHIN A CONTINGENT POLICY
3120
DID THE USER PASS THE FIRST CONTINGENT POLICY?
NO
YES
3122
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF BIOMETRIC POLICIES
USER FAILS THE BIOMETRIC POLICIES WITHIN A CONTINGENT POLICY
3124

FIG. 31

SUBSTITUTE SHEET (RULE 26)

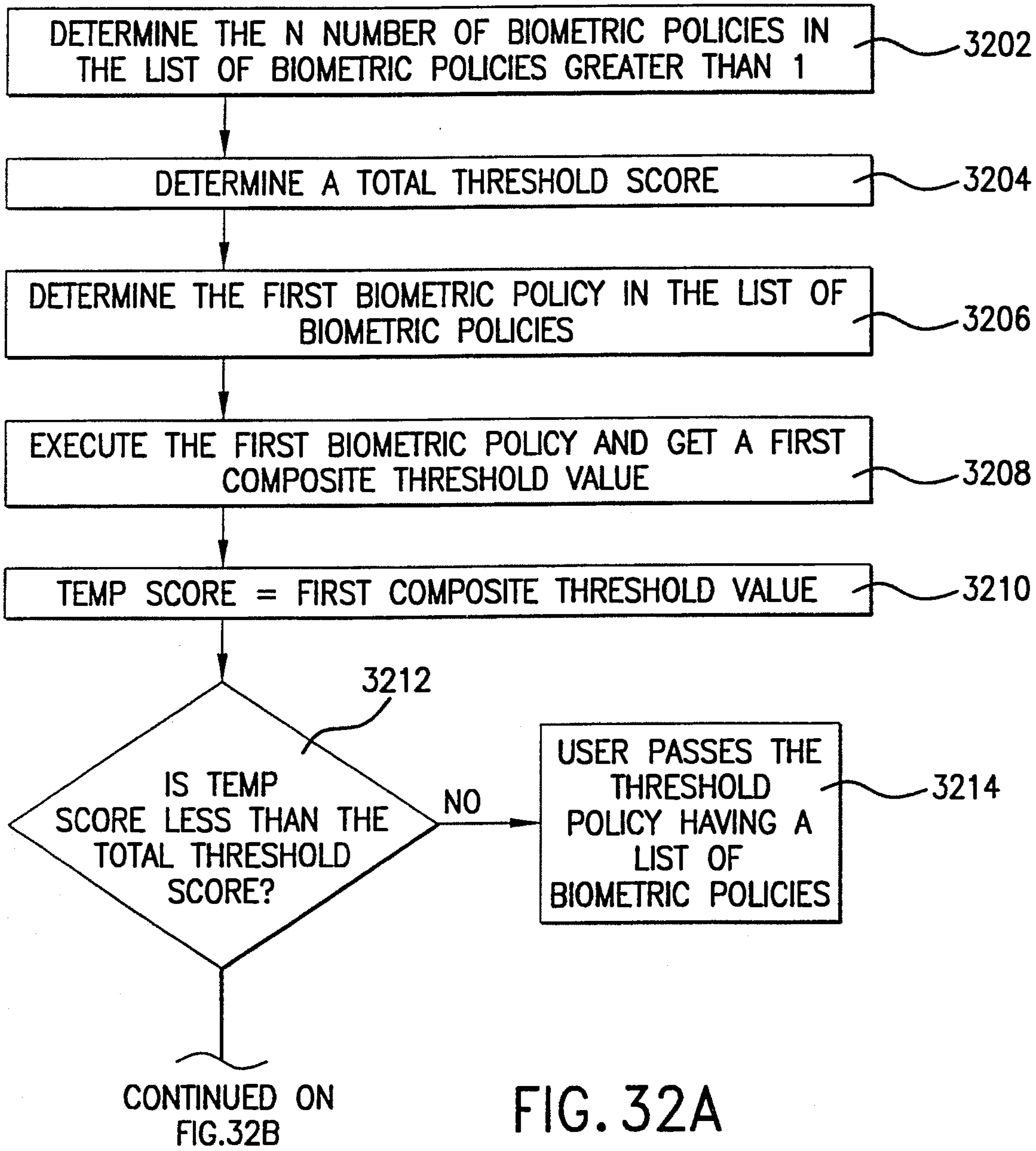

DETERMINE THE N NUMBER OF BIOMETRIC POLICIES IN THE LIST OF BIOMETRIC POLICIES GREATER THAN 1
3202
DETERMINE A TOTAL THRESHOLD SCORE
3204
DETERMINE THE FIRST BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3206
EXECUTE THE FIRST BIOMETRIC POLICY AND GET A FIRST COMPOSITE THRESHOLD VALUE
3208
TEMP SCORE = FIRST COMPOSITE THRESHOLD VALUE
3210
3212
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
3214
CONTINUED ON FIG.32B

FIG. 32A

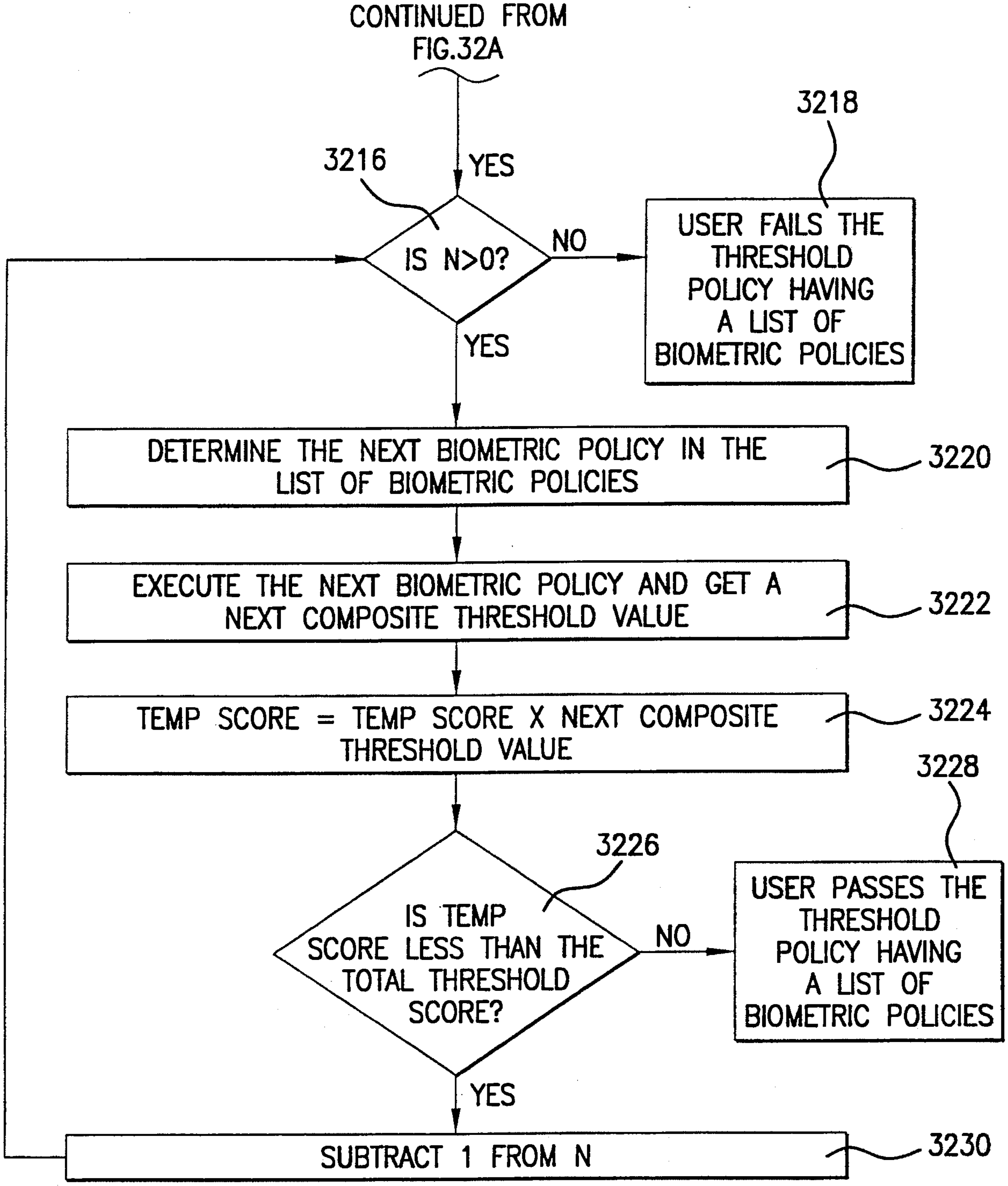

CONTINUED FROM FIG.32A
YES
3216
IS N>0?
NO
3218
USER FAILS THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
YES
DETERMINE THE NEXT BIOMETRIC POLICY IN THE LIST OF BIOMETRIC POLICIES
3220
EXECUTE THE NEXT BIOMETRIC POLICY AND GET A NEXT COMPOSITE THRESHOLD VALUE
3222
TEMP SCORE = TEMP SCORE X NEXT COMPOSITE THRESHOLD VALUE
3224
3228
3226
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF BIOMETRIC POLICIES
YES
SUBTRACT 1 FROM N
3230

FIG. 32B

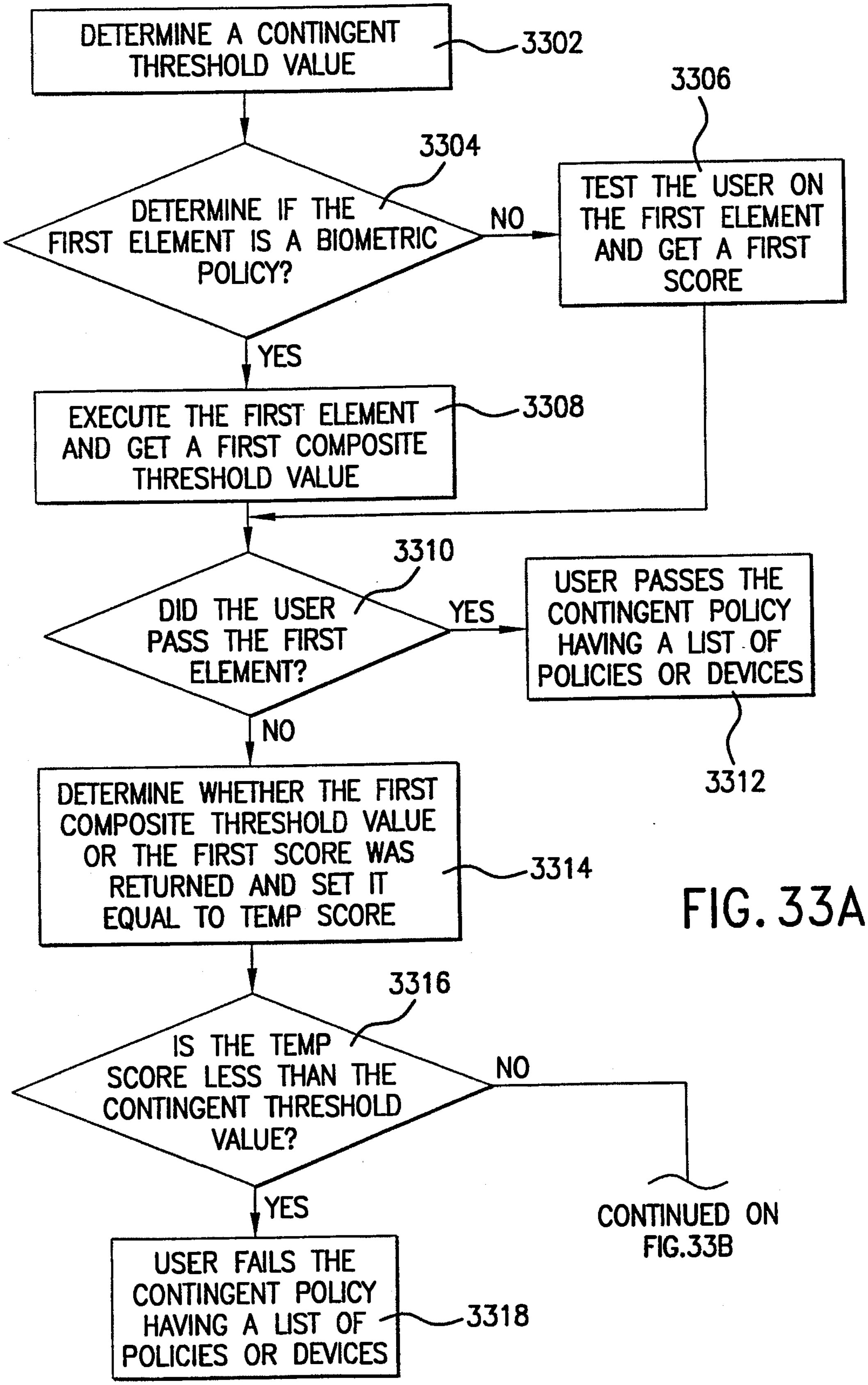

DETERMINE A CONTINGENT THRESHOLD VALUE
3302
3306
3304
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE FIRST ELEMENT AND GET A FIRST SCORE
YES
EXECUTE THE FIRST ELEMENT AND GET A FIRST COMPOSITE THRESHOLD VALUE
3308
3310
DID THE USER PASS THE FIRST ELEMENT?
YES
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
3312
DETERMINE WHETHER THE FIRST COMPOSITE THRESHOLD VALUE OR THE FIRST SCORE WAS RETURNED AND SET IT EQUAL TO TEMP SCORE
3314
3316
IS THE TEMP SCORE LESS THAN THE CONTINGENT THRESHOLD VALUE?
NO
YES
CONTINUED ON FIG.33B
USER FAILS THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
3318

FIG. 33A

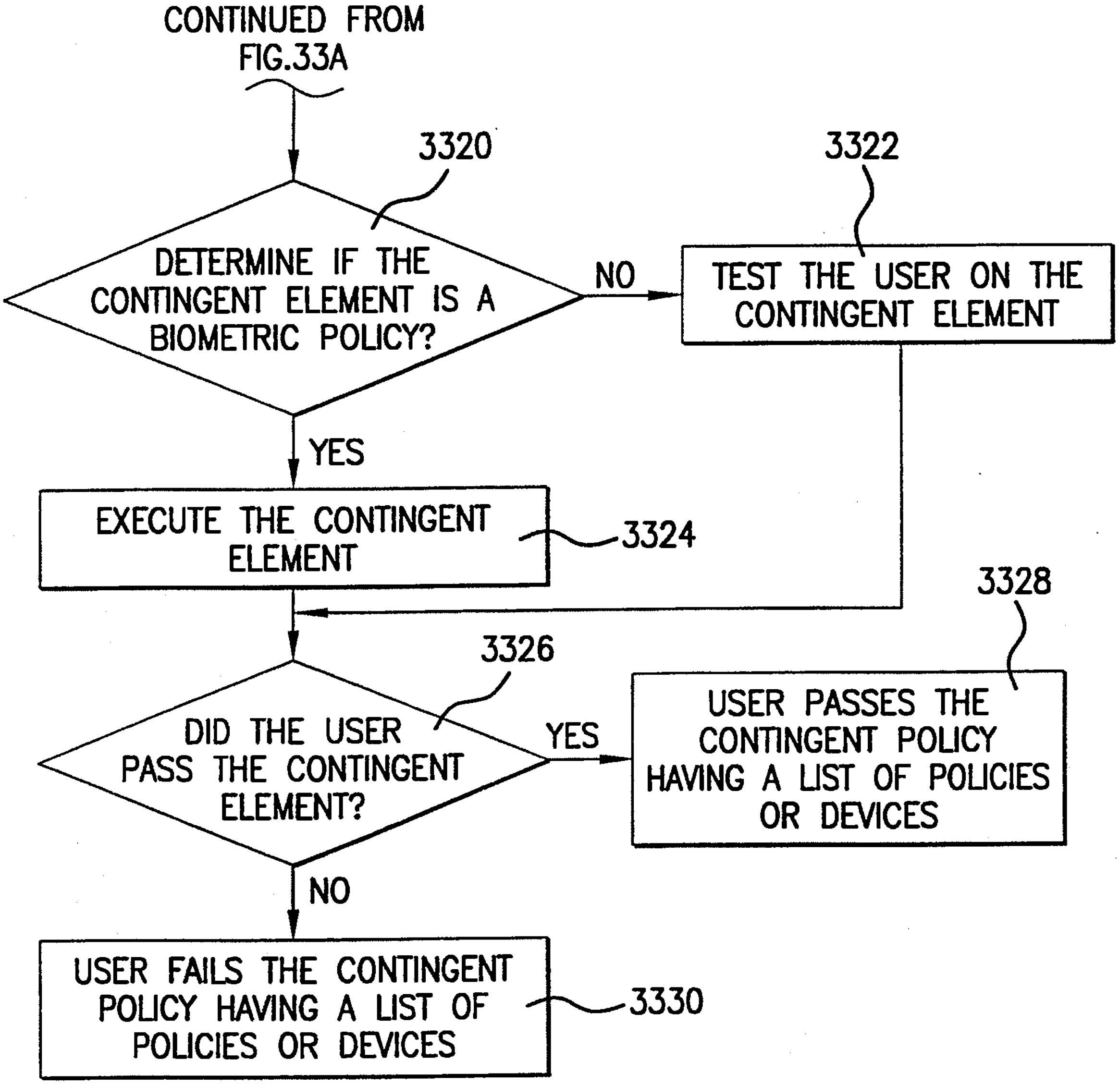

CONTINUED FROM FIG.33A
3320
DETERMINE IF THE CONTINGENT ELEMENT IS A BIOMETRIC POLICY?
NO
3322
TEST THE USER ON THE CONTINGENT ELEMENT
YES
EXECUTE THE CONTINGENT ELEMENT
3324
3328
3326
DID THE USER PASS THE CONTINGENT ELEMENT?
YES
USER PASSES THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
NO
USER FAILS THE CONTINGENT POLICY HAVING A LIST OF POLICIES OR DEVICES
3330

FIG. 33B

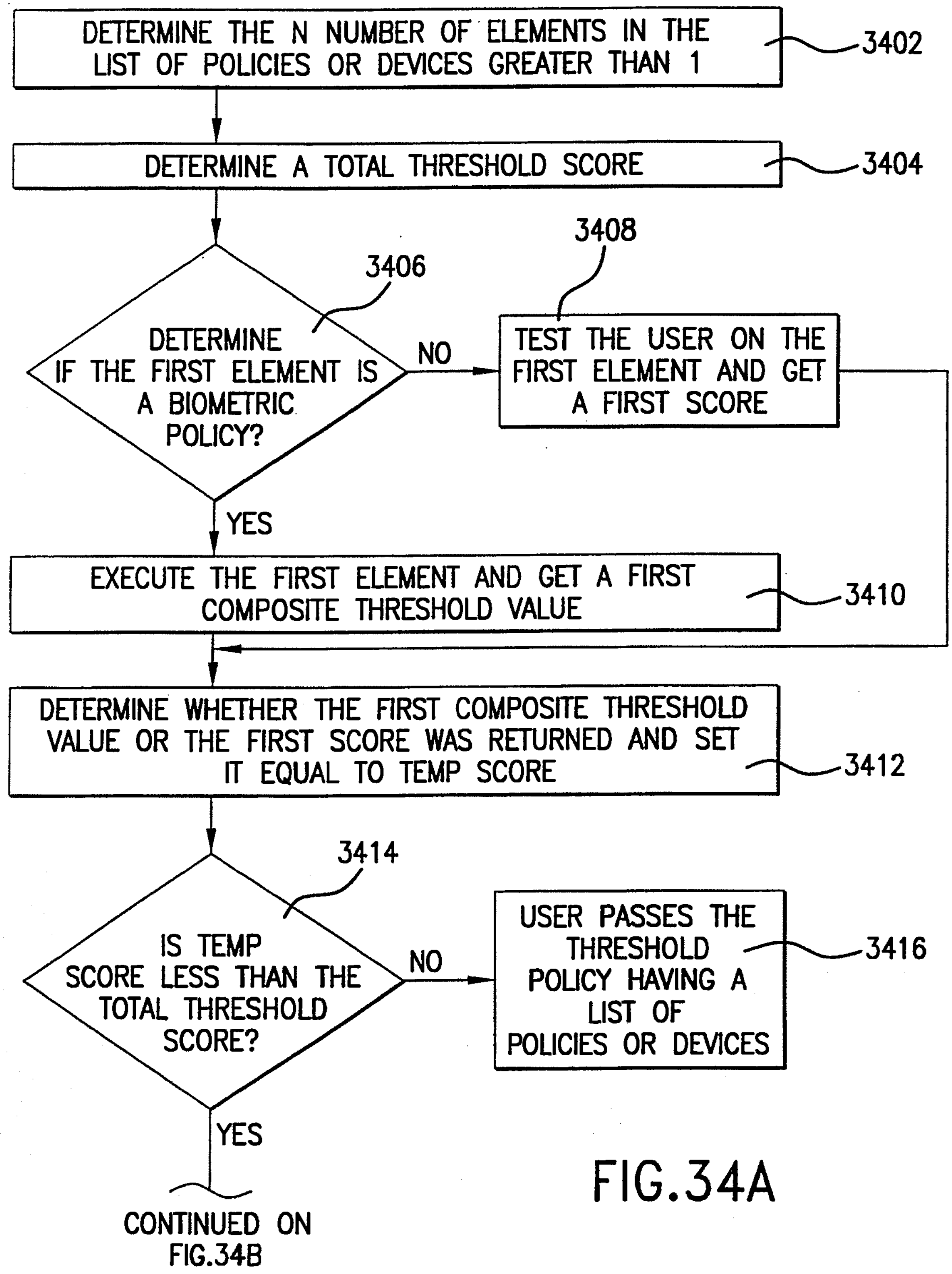

DETERMINE THE N NUMBER OF ELEMENTS IN THE LIST OF POLICIES OR DEVICES GREATER THAN 1
3402
DETERMINE A TOTAL THRESHOLD SCORE
3404
3406
DETERMINE IF THE FIRST ELEMENT IS A BIOMETRIC POLICY?
NO
3408
TEST THE USER ON THE FIRST ELEMENT AND GET A FIRST SCORE
YES
EXECUTE THE FIRST ELEMENT AND GET A FIRST COMPOSITE THRESHOLD VALUE
3410
DETERMINE WHETHER THE FIRST COMPOSITE THRESHOLD VALUE OR THE FIRST SCORE WAS RETURNED AND SET IT EQUAL TO TEMP SCORE
3412
3414
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3416
YES
CONTINUED ON FIG.34B

FIG.34A

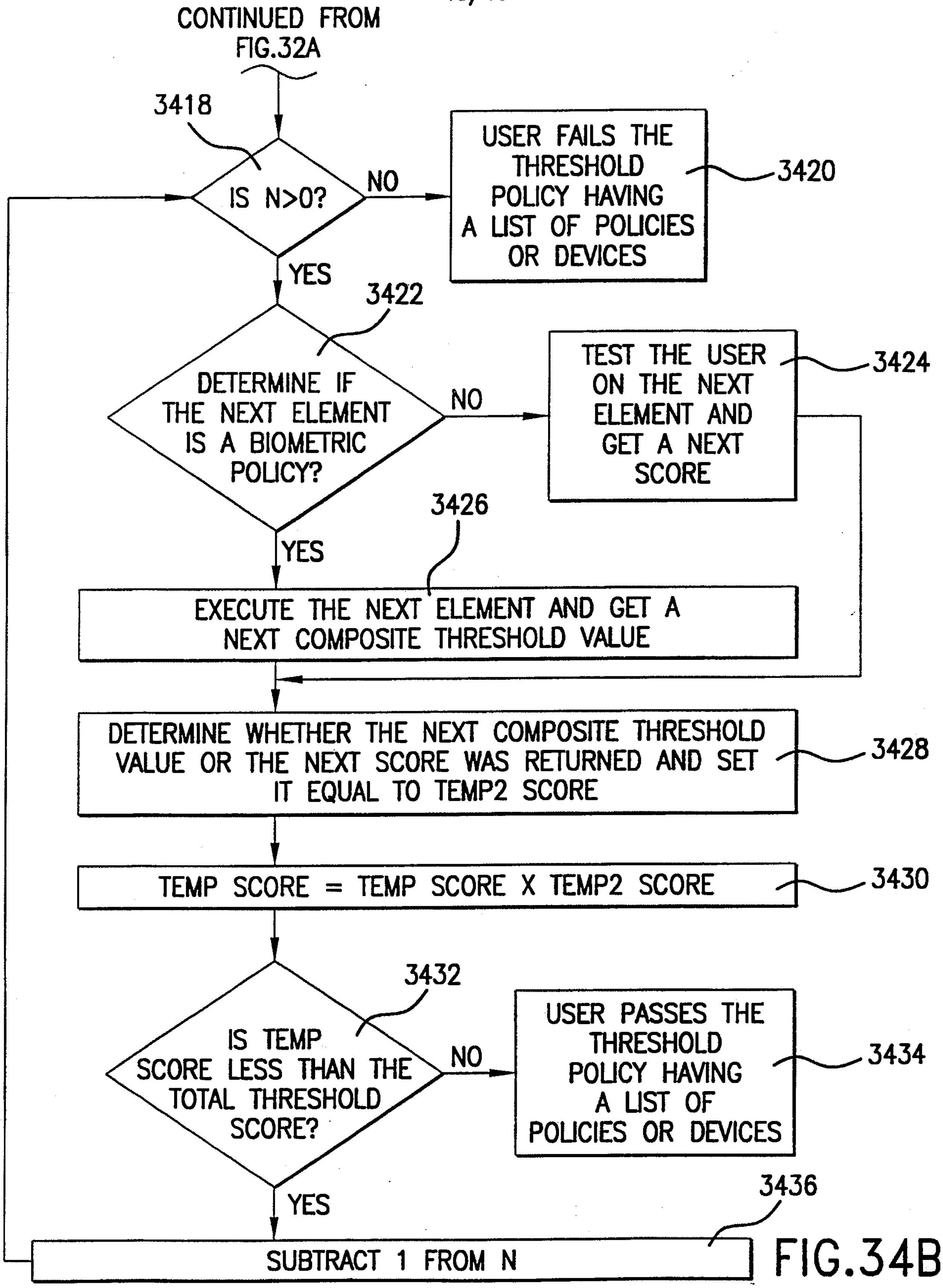

CONTINUED FROM FIG.32A
3418
IS N>0?
NO
USER FAILS THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3420
YES
3422
DETERMINE IF THE NEXT ELEMENT IS A BIOMETRIC POLICY?
NO
TEST THE USER ON THE NEXT ELEMENT AND GET A NEXT SCORE
3424
YES
3426
EXECUTE THE NEXT ELEMENT AND GET A NEXT COMPOSITE THRESHOLD VALUE
DETERMINE WHETHER THE NEXT COMPOSITE THRESHOLD VALUE OR THE NEXT SCORE WAS RETURNED AND SET IT EQUAL TO TEMP2 SCORE
3428
TEMP SCORE = TEMP SCORE X TEMP2 SCORE
3430
3432
IS TEMP SCORE LESS THAN THE TOTAL THRESHOLD SCORE?
NO
USER PASSES THE THRESHOLD POLICY HAVING A LIST OF POLICIES OR DEVICES
3434
YES
3436
SUBTRACT 1 FROM N

FIG.34B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05722

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 9/00
US CL : 713/200, 201, 202, 186; 709/229; 380/3, 4,
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202, 186; 709/229; 380/3, 4,

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

none

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

none

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim N
Y	US 5,615,277 A (HOFFMAN) 25 MARCH 1997, col 1, lines 13-64, col 2, lines 8-38, col 3, lines 1-47.	1-49
Y	US 5,594,806 A (COLBERT) 14 JANUARY 1997, col 1, lines 16-43, col 2, lines 10-54, col 3, lines 28-57, col 4, lines 6-48.	1-49

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 20 APRIL 2000	Date of mailing of the international search report 19 JUN 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BEAUSOLEIL ROBERT W. Jr. Joni Hi Telephone No. (703) 305-3987

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
A63F 9/22, G06F 19/00

A1

(11) International Publication Number: **WO 98/08581**

(43) International Publication Date: 5 March 1998 (05.03.98)

(21) International Application Number: PCT/US97/08072

(22) International Filing Date: 7 May 1997 (07.05.97)

(30) Priority Data:
08/643,827 7 May 1996 (07.05.96) US

(71)(72) Applicant and Inventor: BARCELOU, David, M . [US/US]; 720 New Galena Road, Chalfont, PA 18914 (US).

(74) Agents: SHAMOS, Michael, I. et al.; Webb Ziesenheim Bruening Logsdon Orkin & Hanson, P.C., 700 Koppers Building, 436 Seventh Avenue, Pittsburgh, PA 15219-1818 (US).

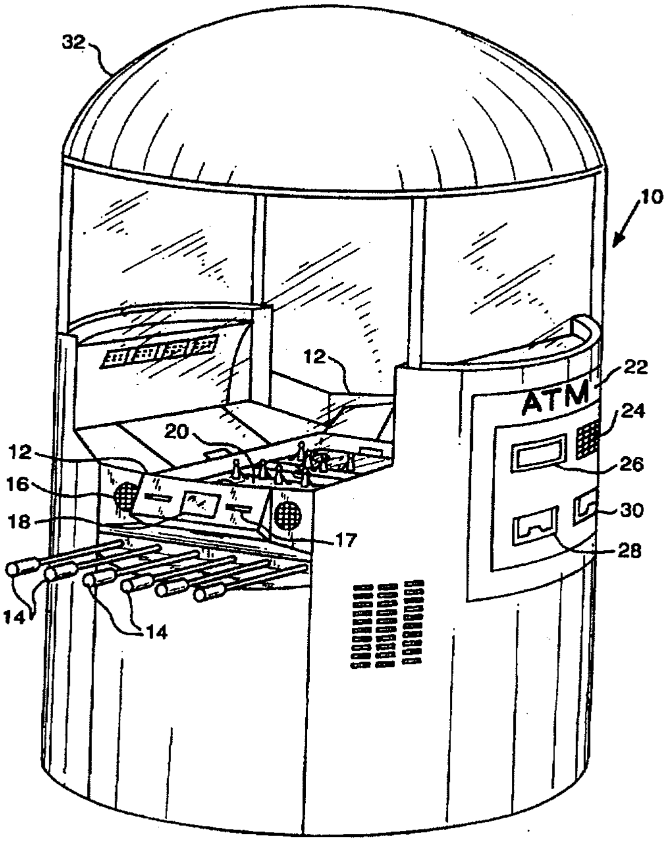
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AUTOMATED LEAGUE AND TOURNAMENT DEVICE

(57) Abstract

A sport or skill game device in which equipment (22) for accepting and dispensing currency, preferably of more than one type (both actual cash and encoded credit, for example), is provided in close proximity with and in electronic connection to one or more of any of a number of sport or skill game devices (14, 20) for play by two or more players. The device contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among two or more entrants whose entry fees and currency pay outs (to the winners) are tendered and distributed as part of the overall operation of the device.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece		Republic of Macedonia	**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's	**NZ**	New Zealand		
CM	Cameroon		Republic of Korea	**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AUTOMATED LEAGUE AND TOURNAMENT DEVICE

Field of the Invention

The invention adapts multiple aspects of entertainment technology and other technologies to sport and skill games and/or devices.

Background of the Invention

Entertainment technology has evolved beyond recognition in a mere ten or fifteen years. New motion pictures are released into complicated and ever more calculated schemes of sequential availability to commercial theaters, rental operations and home theaters--the latter of which can bear startling resemblance to the former. Audio recordings known as "enhanced CDS" offer not only audio but multimedia video replication, and personal computers and televisions and their networks are individually evolving so that soon they may well be virtually indistinguishable. A wide array of online information and interaction tempts us, moreover, from opportunities as unsophisticated as the online equivalent of a group of teenagers sharing a party telephone line to those inherent in ineffable data banks pertaining to satellite photography, medicine and genetic engineering, just to name a few.

Beneath the most enhanced entertainment technology lies a troubling and largely unrecognized assumption, however. With some but minor exceptions, cutting edge entertainment technology is predicated upon the belief that its consumers prefer a largely passive role while the technological dazzle occupies the stage. Multimedia CD jukeboxes are a good example of this phenomenon--a pub or restaurant in which such a machine is installed is overtaken by a genial Wizard of Oz in which social activities, other than the tendering of adequate currency to the welcome sorcerer, take on secondary importance.

This is not to say that the entertainment industry requires passive participation--quite the contrary--just that the concomitant technology generally does. For example, the Karaoke machine in which prerecorded (or sequenced) orchestrations may be augmented by live vocals is at this writing barely taken seriously as an embodiment of entertainment technology, and customarily it is subjected to lighthearted scorn. Even with the newest theme park amusements the "ride" is generally passive. "Hot buttons" on click screens or touchscreens in multimedia interactive applications never seem to deliver the promised autonomy and volition with which such systems entice new users. On the other hand, where true active entertainment participation is maximized the technology tends to be minimal at this writing, such as is evident from the undying popularity of traditional pool or pinball competitions, or in electronic darts and their leagues, or old fashioned amusement park autobahns where the driver can actually (heavens!) steer the car. Consumers of up-to-the-minute elaborate entertainment technology are not today supposed to impose themselves too visibly, or too actively, into the mechanations of their experience.

Quite apart from the entertainment technology industries, sport and skill game leagues of all kinds are gaining in popularity in various settings. The aforementioned electronic darts leagues are immensely popular across a wide socioeconomic spectrum, and other games of skill organized into fee-for-entry leagues include but are not limited to chess, bowling, pool, miniature soccer, miniature hockey, and pinball and video games of skill. These leagues are operated separately from legal and less-than-legal gambling channels, such as those having to do with video poker, because the leagues sponsor games of skill only and proceeds are thus not distributed on the basis of chance. These leagues tend to be surprisingly conventional in their organization, solicitation, seasonal entry, execution and end-of season payout, possibly because the same individuals who value active participation in their leisure pursuits likewise tend to take an active role in the hands-on administration of traditionally organized amusement game and sports leagues.

Accordingly, a need remains for an improvement in entertainment technology in which some or all aspects of that technology, as well as other technologies, are redesigned directly to embrace participatory activities such as those of a sport or skill game league rather than merely the passive participation typical of entertainment technology heretofore.

Summary of the Invention

In order to meet this need, the present invention is a sport or skill game device in which an amalgam of various technologies cooperate to facilitate an active sport or skill game between two players or among three or more players, usually organized into leagues. The device necessarily includes equipment for accepting and dispensing currency, preferably of more than one type (both actual cash and digital cash in the form of encodable credit, for example), in close proximity with and in electronic connection to one or more of any of a number of sport or skill game devices such as may be used for electronic darts, minature hockey, chess, miniature bowling, pinball, video games of skill or virtually any other game of skill in either full sized or miniaturized versions. Preferably, the device includes multimedia enhancements such as controllably cheering crowds and context specific video displays. Moreover, the device necessarily contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among 2 or more entrants whose entry fees and currency payouts (to the winners) are tendered and distributed as part of the overall operation of the device.

The device may occupy a single location, with equipment to allow play by two or more players, or may embody a network of individual game kiosks under centralized control. The device may offer additional optional services including, but not limited to, jukebox activation, full automated teller function, vending of various retail goods and services such as mail order catalogue purchases, sporting and cultural event tickets, cruise or airline tickets, dating services, stock trading or other investment services or even direct vending of foods, beverages, publications, esoterica, etc.

Brief Description of the Drawings

Figure 1 is a perspective view of a first embodiment of the invention;

Figures 2a and 2b are schematic diagrams showing the elements of the first embodiment and a second embodiment of the invention;

Figure 3 is a schematic diagram of a third embodiment of the invention;

Figure 4 is a side elevational view of a control panel according to a fourth embodiment of the invention;

Figure 5 is a side elevational view of the same mechanics as shown in Figure 4, but with the control panel removed;

Figure 6 is a plan view of the game playing field shown in Figure 1;

Figure 7 is a schematic diagram of a fifth embodiment of the invention; and

Figure 8 is a schematic diagram of a sixth embodiment of the invention.

Detailed Description of the Invention

The present invention is a sport or skill game device in which an amalgam of various technologies cooperate to solicit, to organize and to administer an active sport or skill game between two players or among three or more players, with larger numbers usually being organized into leagues. The device may occupy a single location, with equipment to allow play by two or more players, or may embody a network of individual games under centralized control.

The inventive sports league device necessarily includes equipment for accepting and dispensing currency, preferably of more than one type (both actual cash and at least one form of digital currency such as encodable credit, for example), in close proximity with and in electronic connection to any of a number of sport or skill game devices such as may be used for electronic darts, miniature hockey, chess, miniature bowling, pinball, video games of skill or virtually any other game of skill in either full sized or miniaturized versions. Preferably, the device includes multimedia enhancements such as controllably cheering crowds and pertinent video displays. Moreover, the device necessarily contains a computerized function (and appropriate hardware and software) so that the outcome of at least one game of skill may be decided among two or more entrants whose entry fees and currency payouts (to the winners) are tendered and distributed as part of the overall operation of the device.

The device may offer additional optional services including, but not limited to, jukebox activation, full automated teller function, direct vending of foods, beverages, publications and other retail items or remote vending of various retail goods and services such as mail order catalogue purchases or restaurant take-out orders, online service access, sporting and cultural event tickets, cruise or airline tickets, telephone or other smart card encoding, dating services, stock trading or other investment or banking services, health assessment and treatment services, pharmacy services including drug interaction databases, government benefits administration such as food stamps or Medicaid, or insurance brokerage. Other services are limited only by the imagination.

By convention throughout this specification, the "device" refers to the sport or skill game system as a whole, notwithstanding the varying nature of the device as an individual kiosk, such as is shown in Figure 1, or local area networks or wide area networks for multiple station league play with or without the additional functions of retail kiosks for direct or remote vending. The invention and the device, for the purposes of this specification, are thus synonymous.

The present device is used to solicit, to enroll, to govern play and to pay the winner of any one or more of a number of games of skill. A description of the details of how to govern games between two people or league tournament competitions is largely omitted here, because the underlying administrative procedures are both well known and variable regarding aspects such as entry fees, playoff progression and other aspects of tournament administration. However, the present device preferably includes equipment to allow for one or more of the following entertainment technology enhancements to tournament play, including but not limited to:

a) sound and/or motion sensors to initiate attract mode displays on device video display(s) and from audio speakers;

b) audio as well as video instructions and menus;

c) game command interactive touchscreen which also commands selective cheers or taunts from built in speakers, or the national anthem at the start of play, or other light or sound enhancements of game play;

d) juke box provision with operation both independent of and/or interrelated to game play;

e) portrait camera(s) for encoding digital portraits inserted either on players' individual smart cards or as a means of access to a pictorial database;

f) real time video telephone and/or video broadcasting connections between and among local or wide area players or other video networks; printouts of discount coupons, award certificates, player statistics and/or game or tournament results and/or coming tournaments and attractions and schedules.

Enhancements beyond entertainment technology per se have already been listed and include ticket services, dating services, etc. as options. However, the following list helps to illustrate the wide variety of services which can be included: E-M Games of Skill Services; Smart Card Services; Insurance Services; Restaurant Services; Travel Services; Sports Services; Gaming Device Services; Delivery Services; Coupon Services; Introduction Services; Audio Services; News Services; Transportation Services; Utility Services; Physician Services; School Services; Security Services; Building Services; Credit Services; Directory Services; Home Services; Military Services; Personal Services; Automotive Services; Employment Services; Recreational Services; Travelers Check Services; Kids Services; Videogames of Skill Services; Internet Services; Brokerage Services; Government Services; Entertainment Services; Library Services; Catalog Services; Print Services; Diagnostic Services; Chat Services; Video Services; Database Services; Barter Services; Engineering Services; Pharmacy Services; Identification Services; Detective Services; Church Services; Loan Services; Training Services; Buying Services; Recruitment Services; Accounting Services; Photographic Services; Food Services; Radio Services; Credit Services; Theme Park Services; Music Services; Financial Services; Full-line Vending Services; Health Care Services; Remote Access Services; Payment Services; Computer Services; Search Services; Network Services; Subscription Services; Virtual Reality Services; Advertising Services; Rental Services; Programming Services; Beverage Services; Credit/Debit Card Services; Freight Services; Stored Value Card Services; Beauty

Services; Tax Services; Leasing Services; Medical Services; Emergency Services; Publishing Services; Counseling Services; Satellite Services; Screening Services; Real Estate Services; Telephone Services; Ticket Services; Television Services; Dating Services; Information Services; Lottery Services; Software Services; Reservation Services; Communication Services; Intranet Services; Adult Services; Referral Services; Repair Services; Legal Services; Consulting Services; Maintenance Services; Moving Services; Trade Show Services; Design Services; Lodging Services; Mail Services; Fast Food Services; Automated Services; Recording Services; Clothing Services; Wireless Services; Human Services; and Encryption Services.

In a manner similar to the known nature of the league administrative organization, software systems capable of coordinating the combined functions of the present invention are within the skill of the art and do not form a central part of the invention, nor actually do specific video displays and interactive protocols associated therewith (apart from independent proprietary design). For example, the Remote Procedure Call (RPC) model is an industry wide, well tested technology enabling the design and implementation of distributed applications such as the multi-vendor interoperability intrinsic to the present device. The RPC service enables the local game or sport player to invoke a remote procedure as if it were local to the calling process (a remote procedure is a procedure located in an address space separate from the calling code). Ordinarily, the present device will be coordinated according to the RPC model, generally using TCP/IP support protocol computerized systems and known smart card encoding/decoding, database, directory, currency transfer, alternative error recovery and security systems in Local Area Network (LAN), frequently in conjunction with Wide Area Network (WAN), configurations. The invention inheres in the novel interactive combination of several separate technologies as described above, and not in the specifics of the man-machine interface protocols which govern either individual transactions or the overall device.

The above generalized disclosure of the invention is illustrated further by means of the six embodiments specifically illustrated in Figures 1-8, which embodiments are not exhaustive of the various ways the present invention may be implemented.

Referring now to Figure 1, a kiosk 10 is shown in perspective in which two play stations 12 are fitted with play controls 14, a smart card reader/encoder 16, a credit card reader 17, and a video command touchscreen 18. Play controls 14 govern play on a playing field 20 (the playing field itself is shown in greater detail in Figure 6, below), and scoring is automatically calculated and communicated to a computerized control (not shown) interior to and/or exterior to the kiosk 10. The computerized control connects directly to the smart card reader/encoder 16, the credit card reader 17 and the video command screen 18. On a side of the kiosk 10 generally normal to the two play stations 12, an automated teller machine (ATM) 22 includes typical ATM hardware including a card reader (not shown), keyboard 24, instruction screen 26, bill dispenser 28 and receipt dispenser 30. The playing field 20 is covered by and protected by a penetration resistant dome 32 and a standard ATM/bank security camera 31.

In operation, the kiosk of Figure 1 contains all the hardware necessary to enable a player to stand in front of the play station 12, to place a credit card in the credit card reader 17, and to vend or to add value to a smart card (not shown) via the video command touchscreen and the smart card reader/encoder 16. By continuing to use the video command touchscreen, the player may initiate play of a game of skill embodied in the kiosk with another player (either real or virtual), usually after paying an entry fee. Electronic sensors within the kiosk connected with the accompanying computerized control determine the winner of the game of skill and winner identity can be confirmed via the video command touchscreen. Payout of any cash prize owing to the winner can be directed by the computerized control by encoding a credit on the smart card with which game entry was effected, and at the same time the computerized control may also encode player game statistics on the smart card as well. The winner of the game may then insert his smart card through the card reader of the ATM for the purpose of transacting immediate cash disbursement or, alternatively, may deposit his winnings to an existing bank account or make any other electronic credit transaction he or she wishes--including leaving the winnings on the smart card for payment of further entry fees or other retail transactions.

The above exemplary configuration is subject to wide variation, particularly with respect to the smart card reader/encoder 16 and the credit card reader 17. In modified embodiments these structures may be combined as multifunctional smart card/credit card readers and/or a bill acceptor may be added or substituted.

An important aspect of the present invention is the provision of a game of skill to two or more players. For the purposes of the invention, a "player" may be a computer program capable of operating in lieu of a live player, so that for example a single player using the kiosk of Figure 1 could be given the option, via his touchscreen, of playing a computerized opponent. The opponent may even be mechanical, such as in the cyclical rotation of moving targets in a shooting match game of skill. The provision of the option of a computerized or mechanized opponent does not, however, convert a game of skill to a game of chance (viz. computerized chess opponents who invoke very real chess skills). This is an important distinction to arguable games of skill which are really games of chance, such as video solitaire or other games in which the skill required is primarily that of marshaling the chance or random element. Ordinarily, the skill games and sports contemplated for incorporation in the present device are those which require skills of either eye-hand or eye-motor coordination and/or the intellectual skills necessary to answer or to solve problems of science, trivia or war strategy. Skill games well suited to inclusion within the present device are mechanical hockey, chess, video football and others, whereas games substantially governed by die-rolling or card dealing (and their virtual equivalents) are not what is generally meant by "game of skill."

The separate use of a smart card, first at a play station and later (in the event of winning) at an ATM is not strictly speaking a necessary feature of the present invention--although it can be an extremely practical one. Kiosks such as are shown in Figure 1 will be welcomed in places where heretofore neither fully automated league devices nor ATMs have traditionally been available, such as pubs and bars, restaurants, public waiting areas, game arcades and amusement parks. Anticipated high usage of the kiosks suggests that some individuals will form a queue to use the ATM even while other individuals are using the play stations, so that direct credit of winnings to the player's smart card can be more secure than would an automatic payout to the adjacent ATM--which someone else other than the winner might be using at the time.

In the most preferred embodiment of the invention, the smart card has a greater processing and/or memory capacity than can be encoded in mere bar codes or magnetic stripes, as a result of inclusion of processors and/or computer chips therein. Such "smartest" cards can keep track of the owner's usage--game handicap, statistics and scores, for example. Music preferences and other menus can be stored in such cards.

That said, however, the smart card is not strictly essential to the present invention. The first embodiment of the invention as described in reference to Figure 1 is shown in the schematic diagram of Figure 2a, but Figure 2b illustrates that the smart card itself, as well as the smart card reader/encoder, may be eliminated from the present invention. If smart cards are not used at all, the control function of the present device merely directs payout, to the winner, via the adjacent currency acceptor/disburser. As shown in Figure 2b, players may pay their entry fees to the cash acceptor/disburser and proceed to play at stations 1 and 2, which are in two-way communication with a control (usually computerized), whereupon the control determines the winner and directs payment to the currency acceptor/disburser. Figure 2b shows an optional two-way communication between the play station and the currency acceptor/disburser, to permit the player to control the timing of actual disbursement of the winnings ("Are you ready to receive cash payout now? Y/N," for example).

Figure 2a shows in schematic diagram the invention substantially as described with reference to Figure 1. A device containing two play stations also contains a currency acceptor/disburser, all of which are in two-way communication with a control (usually computerized). Each play station is in two-way communication with a smart card reader/encoder, which may include credit card reading capability. After the players pay their entry fees (either by credit card via the smart card reader/encoder or at the currency acceptor/disburser) and play the game of skill or sport, the control may judge the contest and direct payout to the winner directly to the winner's smart card, via the smart card reader/encoder, after which the player may then use his smart card in a separate transaction at the currency acceptor/disburser. The arrangement of Figure 2a does allow for the possibility that the control means may direct immediate payout via the currency acceptor/disburser, but Figure 2a does not illustrate the player's option of mediating that payout directly, without going through the control.

Notwithstanding the above, it is entirely possible to combine individual smart card usage and multi-station ATM ports and still fall within the scope of the present invention. For example, a player using a smart card could still direct cash disbursement to be made immediately adjacent his play station, if the device is configured to offer cash disbursement in this way. This possibility is discussed further below, in the section which describes Figures 4 and 5. Smart cards may also be encoded with digital portraits of individual players as well as one or more currency accounts and player statistics and/or handicap, as well as current tournament standing if applicable.

A more elaborate, third embodiment of the invention is shown in Figure 3, in which the control function mediates among four play stations each having four adjacent smart card reader/encoder devices. The system also includes two currency acceptor/disburser mechanisms. A device according to the third embodiment of the invention is designed for use in high traffic areas where league competition and/or ATM usage are expected to be high. Although Figures 1-3 refer to two or four play stations, any number of play stations and adjacent smart card and currency handling equipment can be combined along the same organizational schemes--the number of play stations is not critical as long as the present device includes two or more of them.

Despite the practical and commercial appeal of separate provision of play stations and ATM(s), the present invention also embraces the direct combination of one or more play stations with direct cash acceptance and disbursement functions, as shown in Figures 4 and 5. Referring now to Figure 4, a partial side elevational view of a fourth embodiment of the present device is shown, in which a kiosk 40 includes a control panel 42 having a video command touchscreen 44, at least one smart card dispenser 46, a credit card reader 48, stereo speakers 50, a bill (cash) acceptor 52, a bill dispenser 54 and a receipt (printer) dispenser 56. Optionally, one of the smart card dispensers 46 may be recording means for encoding information on media other than smart cards, including but not limited to magnetic recording tape; floppy or removable hard disks or drives; recordable CDS, PC cards or PCMCIA cards and etc. A motion/sound/position sensor 58 is also provided adjacent the video command touchscreen. A player using the control panel 42 thus has all device functions available to him or her in a single location. Entry fees may be paid with credit card, smart card value or cash (or even coin, coin acceptor not shown). Games of skill may be played entirely using the video command touchscreen 44 (although there is no reason why manual controls such as appear in Figure 1 may not be incorporated in the control panel 42). Winnings, if any, may be collected as smart card credits or cash or may even be directed to remote credit locations via the video command touchscreen, if the control feature of the device provides such an option. Video touchscreen commands may activate a juke box internal to the kiosk 40 to play music through the stereo speakers 50 either separate from or in conjunction with game play.

Figure 5 illustrates the control panel 42 of Figure 4 with its cover removed, exposing the underlying mechanical features. A bill dispenser security safe 55 and associated vending hardware is thus positioned adjacent the bill dispenser 54. A bill acceptor mechanism 53 known in the art supports the bill acceptor 52 shown in Figure 4. A smart card safe 47 contains smart card inventory to supply to the smart card dispenser(s) 46. A motion/sound/position device 59 supports the sensor 58. A printer 57 provides receipts or other printed material to the receipt (printer) dispenser 56. Each individual mechanism illustrated in Figures 4 and 5 is known in the art, and the invention combines a number of them in a novel way to achieve a heretofore un-dreamed-of sport league device of almost inestimable ingenuity and consumer appeal.

It is not necessary for a kiosk, such as that shown in Figure 1, actually to include a mechanical skill game therein. A kiosk may simply include a video game of skill via one or more control panels 42 according to Figure 4, or variations thereof as described above. Alternatively, the control panels 42 may be provided as wall mounted stations without a free standing kiosk at all.

Other mechanisms included in the present device but not necessarily novel thereto are the games of skill themselves. Figure 6 provides a plan view of an exemplary playing field for miniature hockey, for inclusion in for example the invention shown in Figure 1, in which the playing field 60 contains a plurality of player gearbox mechanisms 62 for controlling a plurality of electromechanical teamsmen (not shown). Play is conducted by causing the teamsmen mechanically to strike a puck dropped from a puck ejector 64 competitively to score one or more goals into the nets 66, from which the pucks are automatically retrieved by puck tracks 68 back into the puck ejector 64. Computerized control of such a playing field thus requires only addition of counting sensors to the nets 66, to keep track of and to communicate the number of goals scored by each player.

A fifth embodiment of the invention is shown in the schematic diagram of Figure 7. The fifth embodiment differs from the third embodiment in two primary ways: a complete retail kiosk is incorporated into the device instead of simply one or more currency acceptor/disburser means, and sonic detector/loud speaker means provide a number of functions including an "attract" mode to advertise the retail kiosk as well as the game stations. The retail kiosk may be designed for literally any direct or remote vending as discussed earlier in this specification, and may provide endless combinations of point-of-sale purchases including passport application with on-site photography, international phone card dispensing with simultaneous ticket and travel services, accommodations, confirmations and execution of immediate e-mail and facsimile communications with simultaneous customized vending of postcards or personalized aerograms (with or without prepaid postage) for later travel use.

In the device as illustrated in Figures 1-7, the control equipment is generally provided from within a single game site or kiosk, but this is not necessary to the present invention and is not really even preferable. In fact, the most preferred embodiments of the present device are those which accommodate full scale league competitions, and so have at least LAN if not WAN configurations. Referring now to Figure 8, a WAN configuration of the present device is shown in schematic diagram wherein the WAN includes central control of a system of LANs controlled by local servers (according to the computer client/server model). A plurality of game kiosks, such as those shown in other Figures herewith, are controlled by each server, and all servers can be coordinated to administer league play. Network connection with banks, financial institutions and general retail goods and services providers is represented by the box labeled "BANKS." With the system illustrated in Figure 8, skill game or sport league devices according to the invention can administer tournaments throughout a single city, throughout several separate geographic locations or--quite easily--throughout the world.

For the purpose of Figure 8, "game kiosk" should be understood to mean any terminal or play station capable of network interconnection with the disclosed system, some of which may not resemble the subject matter of Figure 1 at all. For example, home participants using a PC or a machine manufactured by companies such as SEGA or NINTENDO may be added to the network with or without a smart card peripheral device therewith.

It is apparent from the above that the inventive concept is susceptible of wide variation without departure from the essential invention as described herewith. For this reason, the invention is only to be considered limited insofar as is set forth in the accompanying claims.

We claim:

1. A league device comprising: game means wherein means are provided for play by at least two players of a game of skill; control means in communication with said game means; and means for accepting and disbursing currency in communication with said control means; whereby administration of league play of two or more players of a game of skill is conducted automatically including acceptance of entry fees and disbursement of any winnings.

2. The league device according to claim 1 wherein said means for accepting and disbursing currency further comprises, in combination, a bill acceptor, a bill dispenser, a credit card reader and a smart card reader.

3. The league device according to claim 1 wherein said game means further includes a video screen for control of said game means.

4. The league device according to claim 1 wherein said game means further includes a video touchscreen for control of said game means and further for control of at least one additional retail transaction means present in association with same game means.

5. The league device according to claim 1 wherein said game means is substantially housed by a kiosk, wherein said control means engages a local area network and further wherein said kiosk houses an automated teller machine.

6. The league device according to claim 1 wherein the device includes at least two kiosks each of which substantially houses at least one of said game means, wherein said control means engages a wide area network, and further houses an automated teller machine.

7. The league device according to claim 1 wherein said game means includes means for playing at least one of the games in the group of skill games consisting of mechanical and electromechanical skill games and video games of skill.

8. The league device according to claim 7 wherein said game means includes at least one video control screen, at least one card reader/encoder and at least one audio speaker.

9. The league device according to claim 8 wherein said game means further includes control means for said at least one audio speaker.

10. The league device according to claim 9 wherein said game means is housed substantially within a kiosk which also contains juke box means and at least one control therefor.

11. The league device according to claim 10 wherein said kiosk further houses means for E-M Games of Skill Services; Smart Card Services; Insurance Services; Restaurant Services; Travel Services; Sports Services; Gaming Device Services; Delivery Services; Coupon Services; Introduction Services; Audio Services; News Services; Transportation Services; Utility Services; Physician Services; School Services; Security Services; Building Services; Credit Services; Directory Services; Home Services; Military Services; Personal Services; Automotive Services; Employment Services; Recreational Services; Travelers Check Services; Kids Services; Videogames of Skill Services; Internet Services; Brokerage Services; Government Services; Entertainment Services; Library Services; Catalog Services; Print Services; Diagnostic Services; Chat Services; Video Services; Database Services;

Barter Services; Engineering Services; Pharmacy Services; Identification Services; Detective Services; Church Services Loan Services; Training Services; Buying Services; Recruitment Services; Accounting Services; Photographic Services; Food Services; Radio Services; Credit Services; Theme Park Services; Music Services; Financial Services; Full-line Vending Services; Health Care Services; Remote Access Services; Payment Services; Computer Services; Search Services; Network Services; Subscription Services; Virtual Reality Services; Advertising Services; Rental Services; Programming Services; Beverage Services; Credit/Debit Card Services; Freight Services; Stored Value Card Services; Beauty Services; Tax Services; Leasing Services; Medical Services; Emergency Services; Publishing Services; Counseling Services; Satellite Services; Screening Services; Real Estate Services; Telephone Services; Ticket Services; Television Services; Dating Services; Information Services; Lottery Services; Software Services; Reservation Services; Communication Services; Intranet Services; Adult Services; Referral Services; Repair Services; Legal Services; Consulting Services; Maintenance Services; Moving Services; Trade Show Services; Design Services; Lodging Services; Mail Services; Fast Food Services; Automated Services; Recording Services; Clothing Services; Wireless Services; Human Services; and Encryption Services.

12. A league device, comprising: game means wherein means are provided for play by at least one player, and at least one opponent, of a game of skill, said game means being positioned adjacent a means for accepting and disbursing currency wherein said game means and said means for accepting and disbursing currency further contain means to enable independent or simultaneous operation of said game means and said means for accepting and disbursing currency.

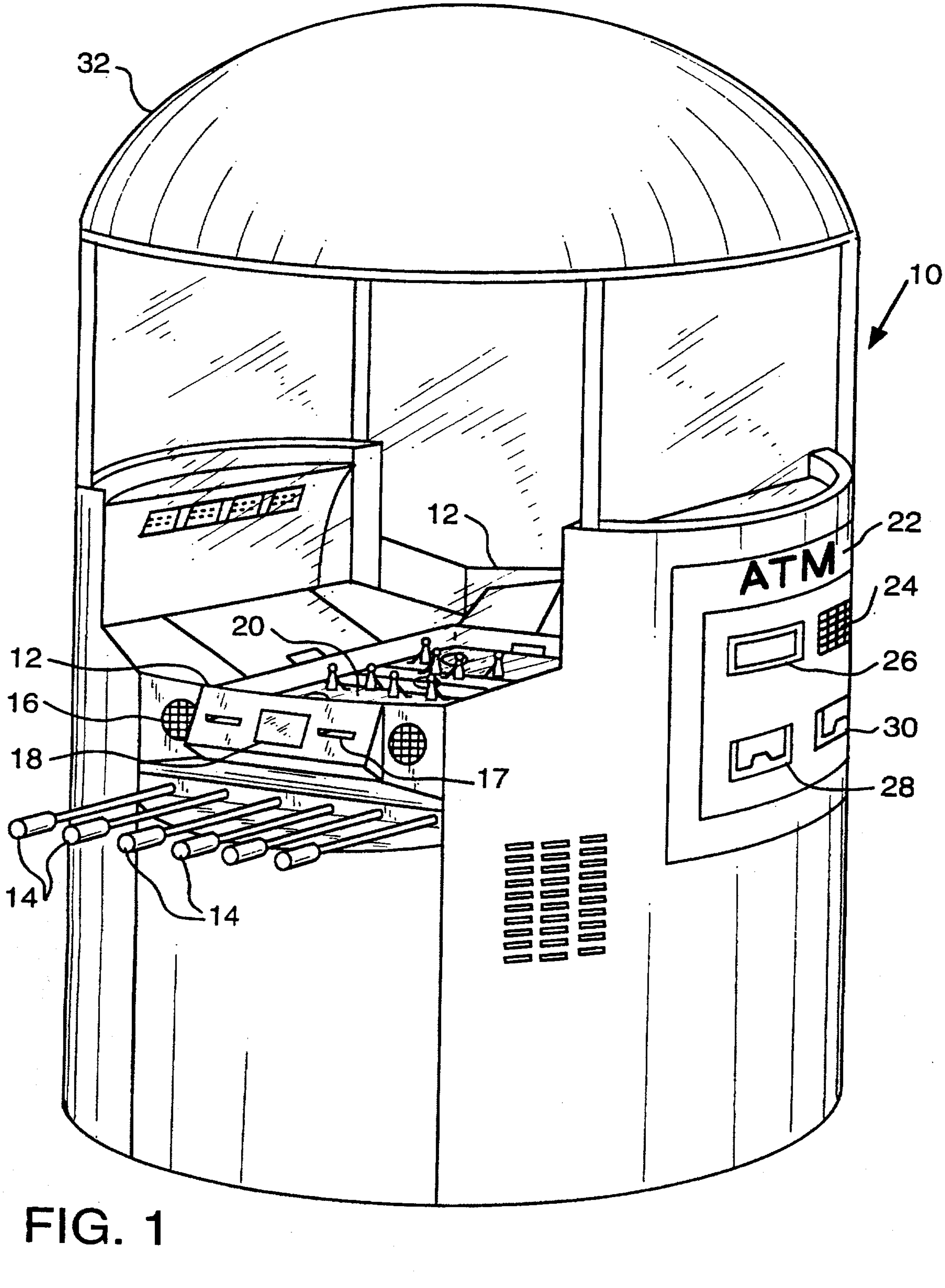


FIG. 1

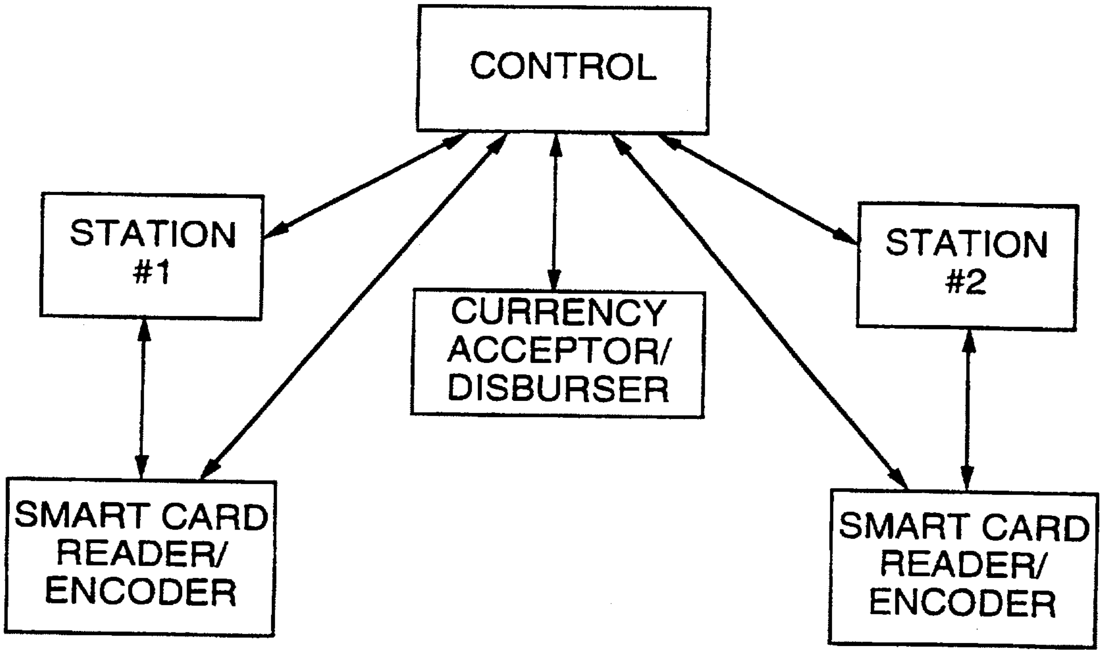

CONTROL
STATION #1
CURRENCY ACCEPTOR/ DISBURSER
STATION #2
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 2a

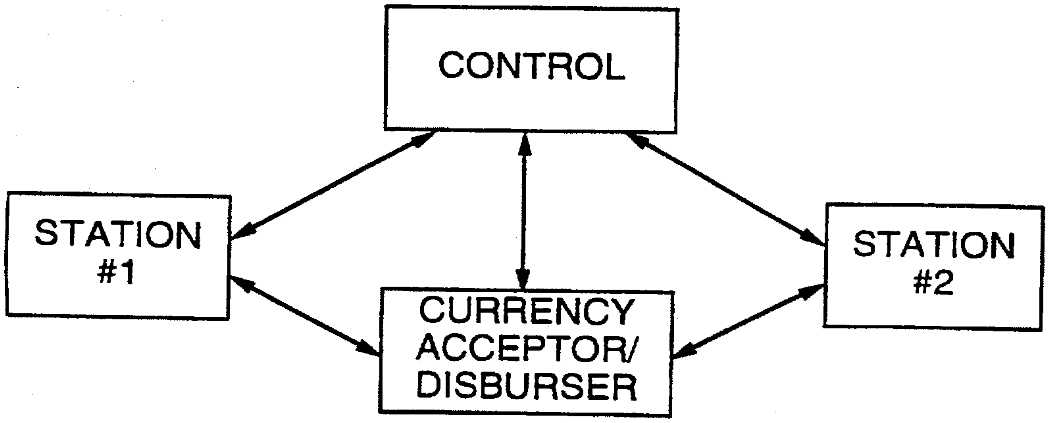

CONTROL
STATION #1
STATION #2
CURRENCY ACCEPTOR/ DISBURSER

FIG. 2b

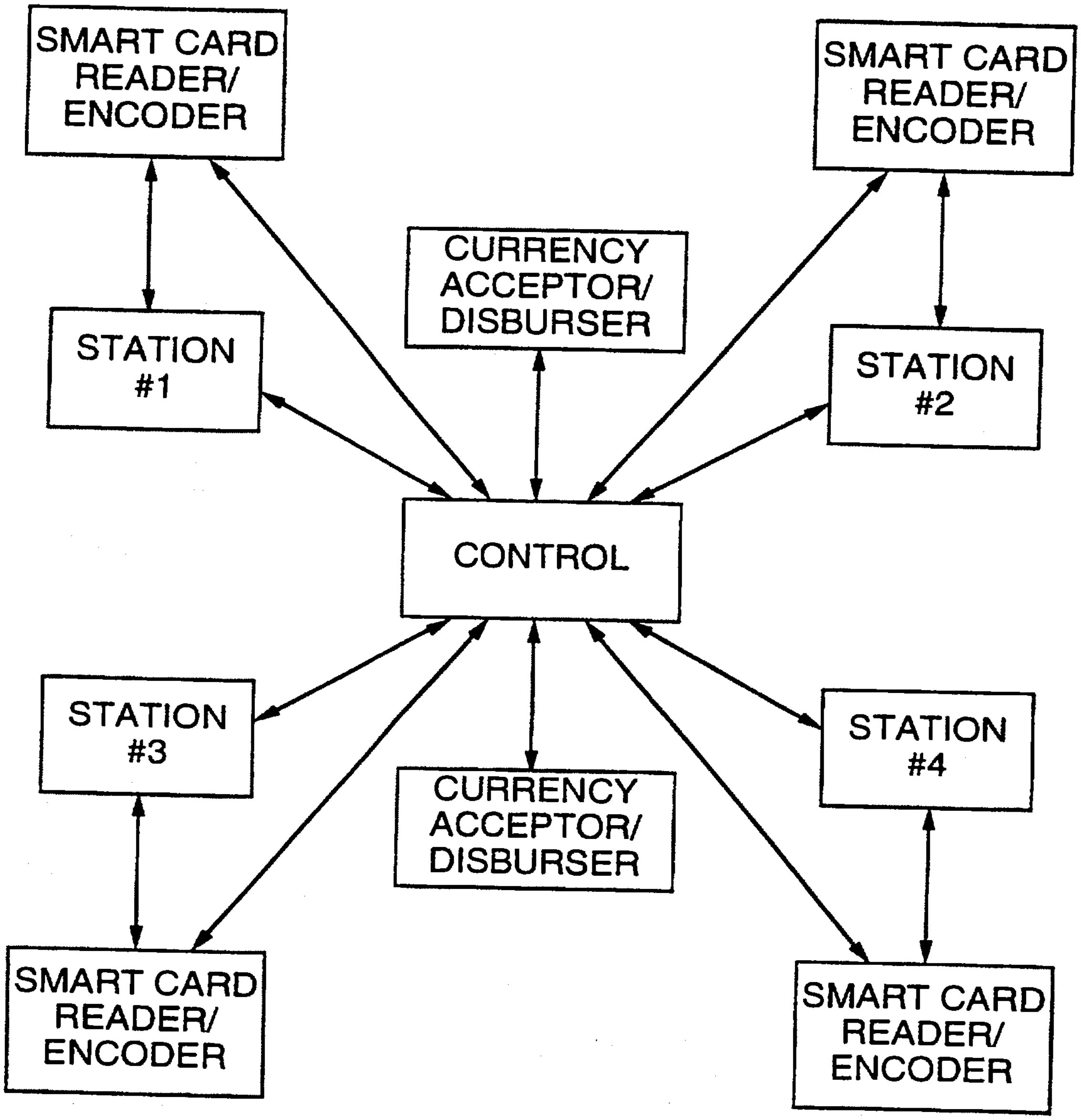

SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER
CURRENCY ACCEPTOR/ DISBURSER
STATION #1
STATION #2
CONTROL
STATION #3
STATION #4
CURRENCY ACCEPTOR/ DISBURSER
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 3

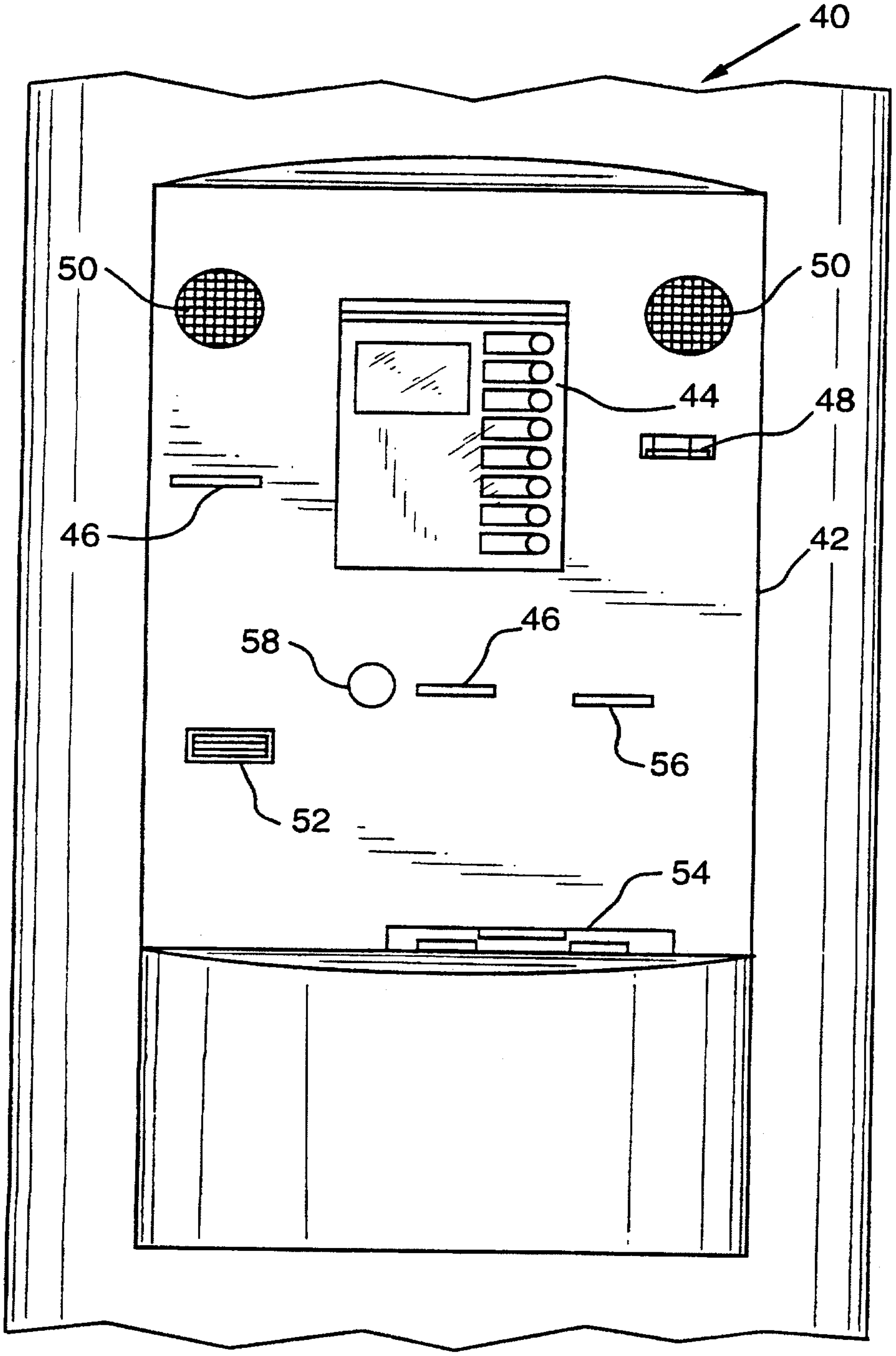


FIG. 4

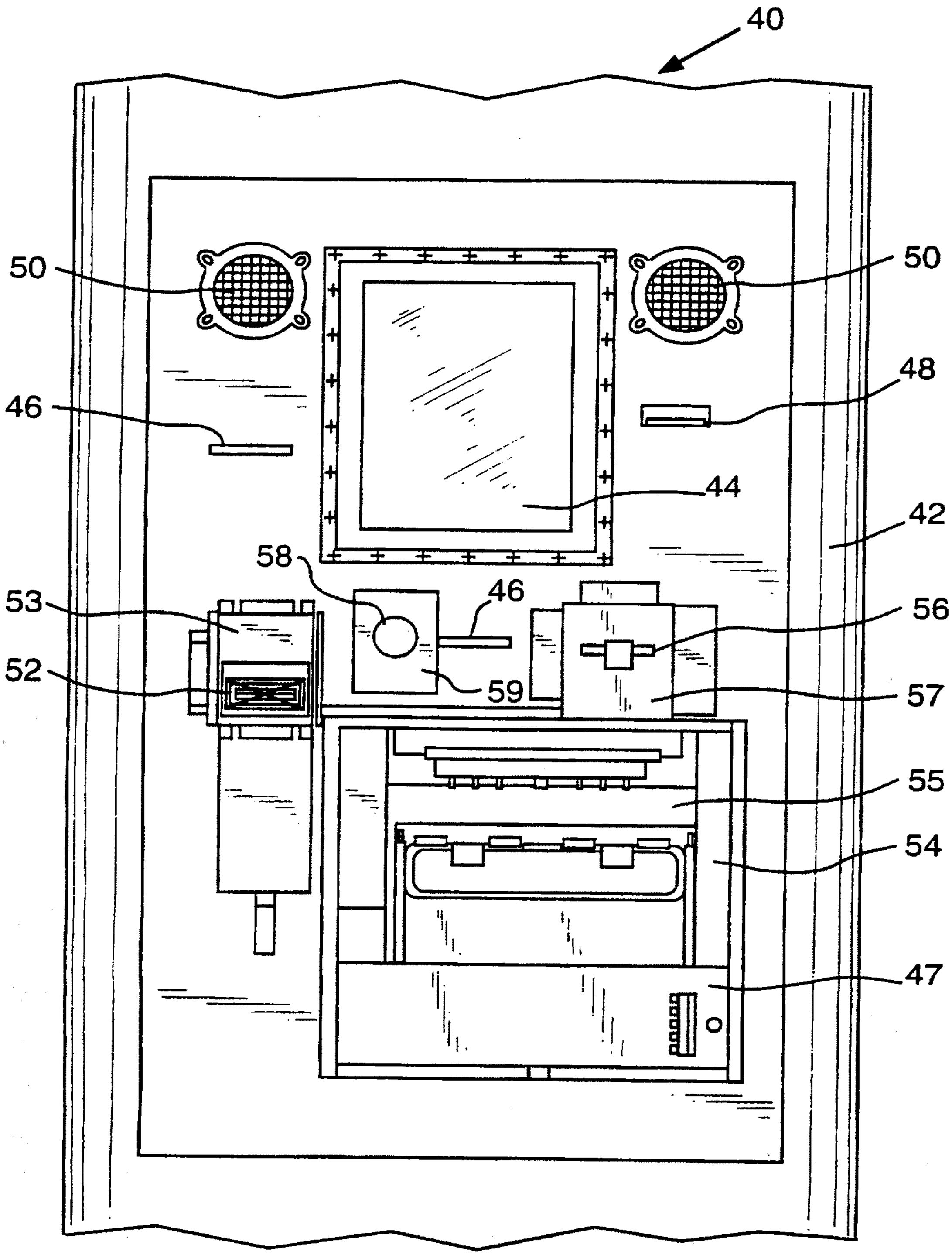


FIG. 5

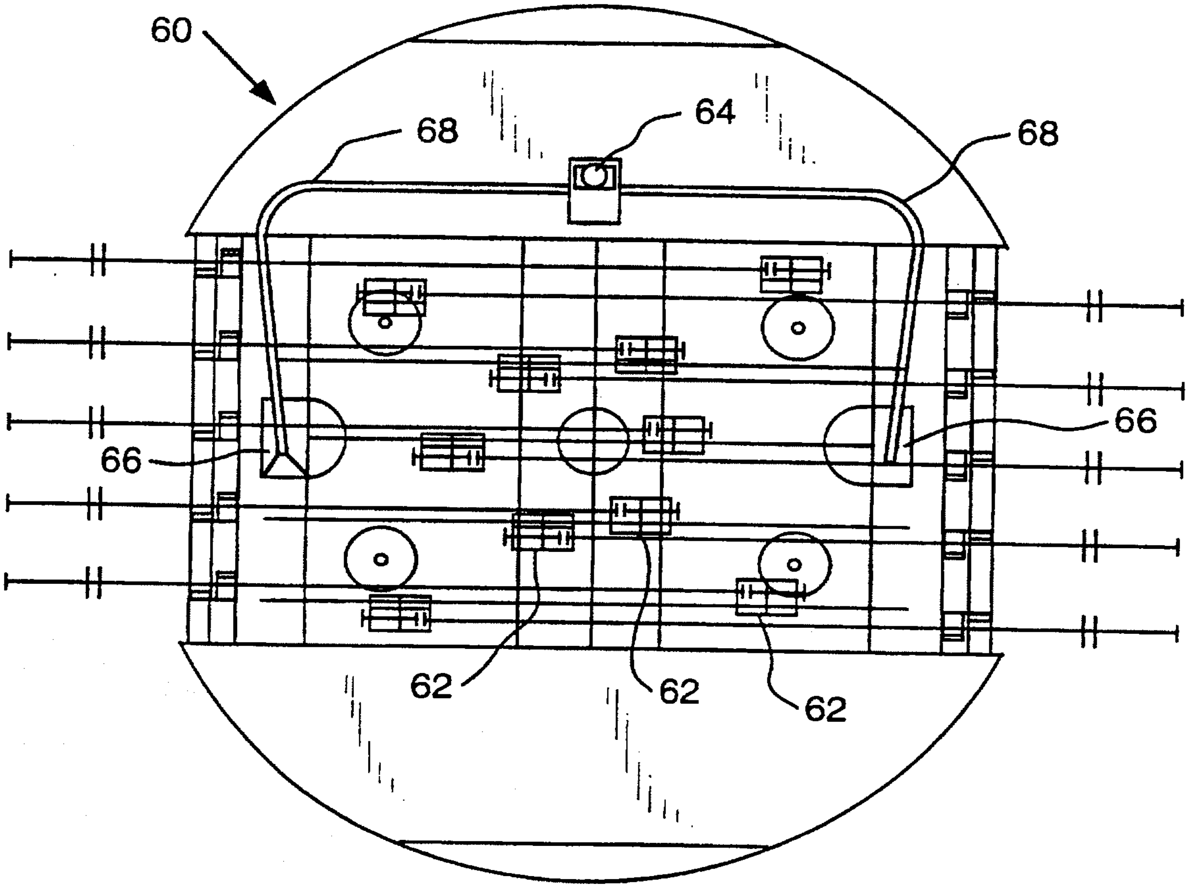


FIG. 6

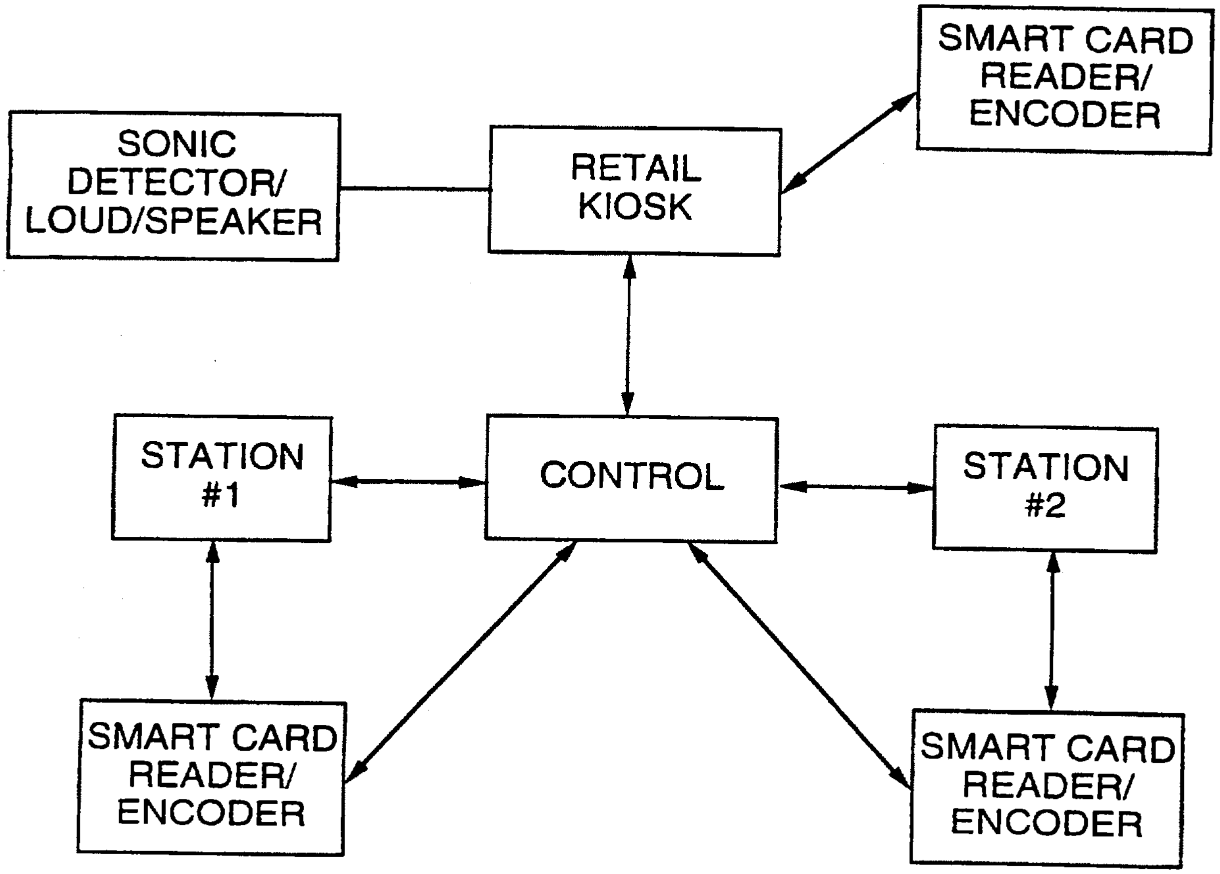

SMART CARD READER/ ENCODER
SONIC DETECTOR/ LOUD/SPEAKER
RETAIL KIOSK
STATION #1
CONTROL
STATION #2
SMART CARD READER/ ENCODER
SMART CARD READER/ ENCODER

FIG. 7

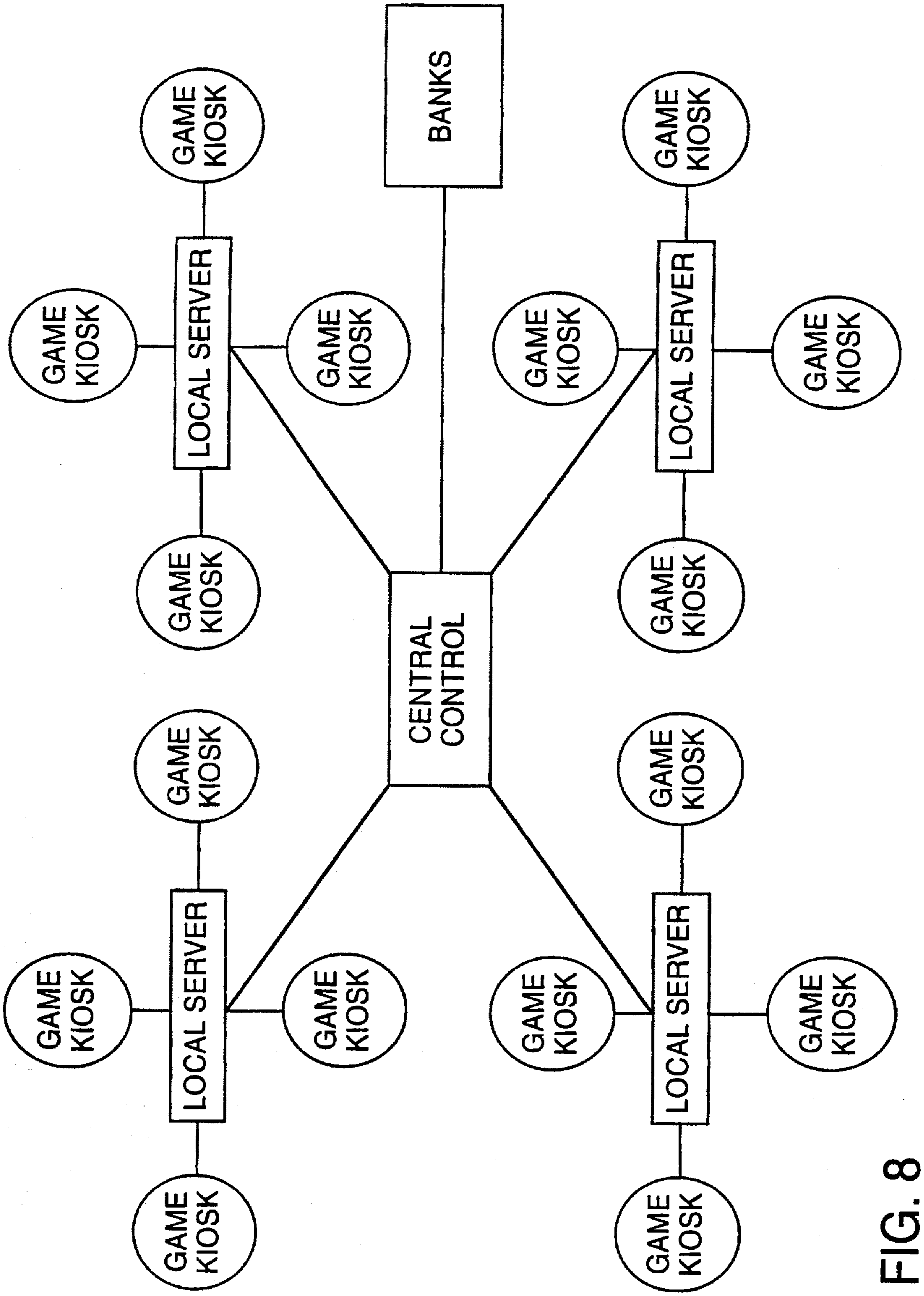

BANKS
CENTRAL CONTROL
LOCAL SERVER
LOCAL SERVER
LOCAL SERVER
LOCAL SERVER
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK
GAME KIOSK

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08072

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :A63F 9/22; G06F 19/00
US CL :235/279; 463/25, 42, 46
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 463/1, 4, 7, 25, 29, 40, 42, 46; 235/279

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- A	US 5,083,271 A (THACHER et al) 21 January 1992, entire document.	1-4, 7-9, 12 --- 5, 6, 10, 11
A	US 4,669,730 A (SMALL) 02 June 1987, entire document.	5, 6, 10, 11

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 17 AUGUST 1997	Date of mailing of the international search report 10 SEP 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES SCHAAF Telephone No. (703) 308-3397

Electronic Acknowledgement Receipt

EFS ID:	7961162
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	06-JUL-2010
Filing Date:	21-AUG-2007
Time Stamp:	17:58:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDSofJuly06-2010.pdf	10422374 f431a0fdfffa0fa1a2b87d193cb93138e8be9b1c	yes	204

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	Foreign Reference	4	166
	Foreign Reference	167	198
	NPL Documents	199	204

Warnings:

Information:

Total Files Size (in bytes):	10422374

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	3711
Examiner Name	
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6219836	B2	2001-04-17	B. Wells et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number³	Country Code² i	Kind Code⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

	1	Communication pursuant to Article 94(3) EPC of April 6, 2010 in related EP application 02780726.2	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-07-06
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	7962506
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	06-JUL-2010
Filing Date:	21-AUG-2007
Time Stamp:	19:54:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDS2ndofJuly62010.pdf	803609 b00b4d4cf477a6cd1fe4f62f757d974bc22557c9	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	NPL Documents	4	8
Warnings:			
Information:			
	Total Files Size (in bytes):	803609	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

	1	Communication pursuant to Article 94(3) EPC of April 6, 2010 in related EP application 02784552.8	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-07-06
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 096 438 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.05.2001 Bulletin 2001/18

(51) Int. Cl.^{7}: **G07F 7/10**, G07C 9/00

(21) Application number: **00123164.6**

(22) Date of filing: **25.10.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.10.1999 US 430242**

(71) Applicant:
International Game Technology
Reno, Nevada 89511-8986 (US)

(72) Inventors:
- **Uihlein, Mark**
  Henderson, Nevada 89014 (US)
- **Carson, Robert H., Jr.**
  Sparks, Nevada 89431 (US)
- **Powell, Tracy**
  Reno, Nevada 89511 (US)

(74) Representative:
Manitz, Finsterwald & Partner
Postfach 22 16 11
80506 München (DE)

(54) A lighted keypad assembly, method and system for tracking players

(57) A keypad assembly and method for use with a card reader adapted to receive and read a player identification card therein. The keypad assembly includes a keypad mechanism having a plurality of keys to input data, and a feedback mechanism coupled to the keypad. A validation device is provided which is adapted to determine the validation of information relating to the identification card upon reading thereof in the card reader. The validation device is further operably coupled to the feedback mechanism to visually inform the Player that the information relating to identification card has been validated.

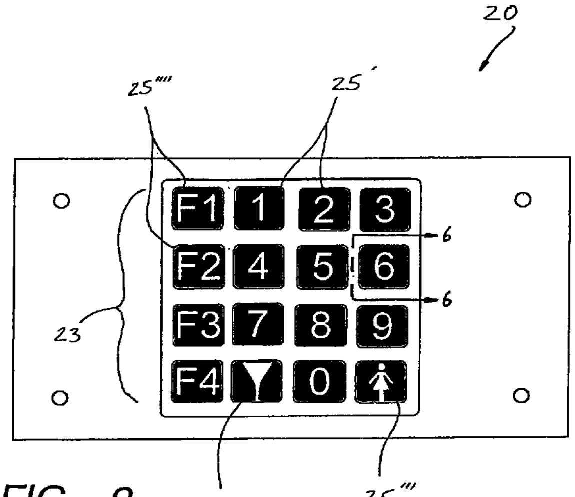


FIG._2

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

TECHNICAL FIELD

[0001] This present invention relates, generally, to player tracking systems for gaming devices and, more particularly, relates to keypad and card reader devices for player tracking systems.

BACKGROUND ART

[0002] As technology in the gaming industry progresses, the once traditional mechanically-driven reel slot machines have been replaced with electronic counterparts having CRT video displays or the like. These video/electronic gaming advancements enable the operation of more complex gambling games which would not otherwise be possible on mechanical-driven gambling machines. For example, in addition to reel slot machines, it is now common to observe stand alone or multiple platform video electronic games including Keno, Blackjack, Poker, Pai Gow, and all the variations thereof, in even the smallest gaming establishments.

[0003] These electronic game devices are also commonly interconnected to a host computer through a network system. Such intercommunication has several advantages which include competitive gaming machine play, and additional and more complex bonusing schemes to entice Players to participate. Another benefit derived from these networked systems is the collection of accounting data such as the usage and payout of each gaming machine which allows the gaining establishment to immediately assess their profitability. Typical of such patented systems may be found in U.S. Patent Nos.: 5,470,079 to LeStrange et al.; and 4,283,709 to Lucero et al.

[0004] Another primary advantage of these networked gaming devices is the ability to collectively track the individual Player use of the gaming devices, player tracking, for instance, allows the gaming establishment to monitor individual Player use for accounting and advertising purposes. As an incentive to return, the gaming establishment often awards complimentary meals, rooms and event tickets to the Player An example of such systems include U.S. Patent Nos.: 5,655,961; 5,702,304; 5,741,183; and 5,752,882 to Acres et al.; and 5,761,647 to Boushy.

[0005] Generally, each participating Player is issued an individual player tracking card which incorporates a unique player identification code corresponding to the customer's account. Upon insertion of the player tracking card into a card reader at a respective gaming machine, the unique identification code is extracted from the card and transmitted to the host computer to commence tracking of the Player's gaining activity. Subsequently, the host computer updates the customer's account to reflect the new activity.

[0006] Occasionally, the Player inserts the player tracking card into the card reader slot incorrectly. Should the customer begin play of the game while the identification card is incorrectly inserted, the player tracking data will not be properly recorded. Consequently, the Player's activity will not be credited to their account and will thus be lost, while the gaming establishment's records will be incomplete.

[0007] In an attempt to notify the Player of the status of their card insertion, a light emitting diode (LED) or the like is often mounted to the card reader or on the gaming device in close proximity to the display screen. Typically, once the proper card insertion is verified, the diode is illuminated to inform the Player that the identification card has been properly inserted. One problem associated with this approach, however, is that the bright lighting in the gaming establishments often overpower the visualization of the relatively dim LEDs.

[0008] Accordingly, even if the status of the card insertion is indicated to be incorrect, the Player may not even notice.

[0009] U.S. Patent No. 5,702,304 to Acres et al. attempts to overcome this deficiency by back lighting the large bezel surrounding the card reader opening of the card reader. Upon a proper identification of the code embedded in the Player's card, the large bezel will be back lit in one color, while an improper identification will cause the bezel to be back lit in another color.

[0010] While this solution is satisfactory in many instances, the patron is required to visually observe the card reader for verification. This momentary delay may be annoying for anxious Players, especially for those who switch gaming machines frequently. Moreover, the newer player tracking systems may require the input of additional information from a keypad mechanism which may be spaced away from the card reader. In these instances, the anxious Player may quickly insert their player tracking card and begin keying in this additional information before ever observing the status indication at the card reader.

[0011] Accordingly, in view of the above observations, it would be desirable to provide a player tracking system which simplifies the visual observation of the player tracking card insertion status to the Player.

DISCLOSURE OF INVENTION

[0012] The present invention provides a keypad assembly for use with a card reader adapted to receive and read a player identification card therein. The keypad assembly includes a keypad mechanism having a plurality of keys to input data, and a feedback mechanism coupled to the keypad. A validation device is provided which is adapted to determine the validation of information relating to the identification card upon reading thereof in the card reader. The validation device is further operably coupled to the feedback mechanism to visually inform the Player that the information relating to identification card has been validated.

[0013] The present invention, therefore, allows the Player to visually determine the validation of the information directly at the keypad mechanism. This facilitates system efficiency since the customer no longer has to observe the card reader for verification before turning their attention to the keypad mechanism. Such information, for example, may relate to the identification cards such as the verification of proper card insertion or of the validation of the input of the Personal Identification Number (PIN).

[0014] In one embodiment, the validation device provides a first lighting mode to visually inform the Player that the information relating to the identification card has been validated, and a second lighting mode to visually inform the Player that the information relating to the identification card has not been validated. Preferably, the illumination device is provided by a multicolor light emitting diode so that in the first lighting mode, the light emitting diode illuminates in one color, and in the second lighting mode, the light emitting diode illuminates in another color.

[0015] Preferably, each key of the keypad is translucent for back lighting thereof, wherein the multicolor light emitting diodes provide back lighting to each key. Thus, upon validation or invalidation, the keys will be illuminated to inform the Player of the status of the information relating to the identification card before they begin keying in additional input data.

[0016] In another configuration, the validation device includes a microcontroller to control the animation of each light emitting diode in the first lighting mode and the second lighting mode. The microcontroller further includes an attract mode which operates each light emitting diode in an attract sequence when no identification card is positioned in the card reader opening. For example, when there is no identification card inserted in the card reader, the translucent keys may flash randomly or in patterns, as well as in different colors, to attract new Players.

[0017] In another aspect of the present invention, a player tracking system is provided for tracking Players of a plurality of gaming machines interconnected to a host computer which includes a player tracking device adapted to monitor the game play of a Player, and a card reader for reading a player identification card inserted in a card reader opening of the card reader. The system further includes a keypad mechanism having a plurality of keys to input data for use in the player tracking device, and an illumination device coupled thereto. In accordance with the present invention, a validation device is provided to determine the validation of information relating to the identification card inserted in the card reader opening. When the information is validated, the illumination device is illuminated at the keypad mechanism to visually inform the Player of such validation.

[0018] In still another aspect of the present invention, a method of validating information relating to a player identification card inserted into a card reader is provided including receiving the identification card in a card reader opening of the card reader; and providing a keypad mechanism having a plurality of keys for the input of data. The method further includes validating information relating to the identification card upon insertion of the card into the card reader opening for reading thereof; and illuminating an illumination device on the keypad mechanism to visually inform the Player that the information relating to identification card has been validated.

[0019] The validating information preferably includes illuminating the illumination device in a first lighting mode, to visually inform the Player that the information relating to the identification card has been validated, and illuminating the illumination device in a second lighting mode, to visually inform the Player that the information relating to the identification card has not been validated. The validating information may further include sensing the proper insertion of the identification card in the card reader opening for reading thereof.

[0020] In another embodiment, the validating information includes reading an identification code encoded on the identification card, and comparing the identification code to a predetermined code to determine the validation.

[0021] Yet another aspect of the present invention includes a method of validating information relating to a player identification card inserted into a card reader of one of a plurality of gaming device interconnected to a host computer. The method includes receiving the identification card in a card reader opening of a card reader of one of the gaming devices, and validating information relating to the identification card upon insertion of the card into the card reader opening for reading thereof. The method further includes illuminating an illumination device on a keypad mechanism, having a plurality of keys for the input of player tracking data, to visually inform the Player that the information relating to identification card has been validated.

[0022] In one embodiment, the method further includes, after validating the information, enabling the Player to input player tracking data through the keys of the keypad mechanism. The method may further include, after the validating the information, tracking the Player's game play on the gaming device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The method and assembly of the present invention has other objects and features of advantage which will be more readily apparent from the following description of the Best Mode of Carrying Out the Invention and the appended claims, when taken in conjunction with the accompanying drawing, in which:

FIGURE 1 is a top perspective view of a conventional gaming machine incorporating a keypad assembly constructed in accordance with the present invention.

FIGURE 2 is an enlarged top plan view of a keypad mechanism of the keypad assembly of FIGURE 1.

FIGURE 3 is a schematic representation of a player tracking system for a gaming machine which incorporates the keypad assembly of the present invention.

FIGURE 4 is a schematic representation of the keypad assembly of the present invention.

FIGURE 5 is a schematic diagram of the keypad assembly of the present invention.

FIGURE 6 is a fragmentary, enlarged side elevation view, in cross-section, of a key component of the keypad mechanism taken substantially along the plane of the line 6-6 in FIGURE 2.

FIGURE 7 is a top plan view of the keypad mechanism of FIGURE 2 illustrating an illumination pattern in the form of a "√" symbol representing a validation of information.

FIGURE 8 is a top plan view of the keypad mechanism of FIGURE 2 illustrating an illumination pattern in the form of a "X" symbol representing an invalidation of information.

FIGURE 9 is an enlarged top perspective view of a conventional card reader device employed with the keypad assembly of the present invention.

BEST MODE OF CARRYING OUT THE INVENTION

[0024] While the present invention will be described with reference to a few specific embodiments, the description is illustrative of the invention and is not to be construed as limiting the invention. Various modifications to the present invention can be made to the preferred embodiments by those skilled in the art without departing from the true spirit and scope of the invention as defined by the appended claims. It will be noted here that for a better understanding, like components are designated by like reference numerals throughout the various figures.

[0025] Attention is now directed to FIGURES 1-4, 6 and 9 where a keypad assembly, generally designated 20, in accordance with the present invention is illustrated for use with a card reader 21 configured to read a player identification card 22 (FIGURE 9) therein. The keypad assembly 20 includes a keypad mechanism 23 having a plurality of key components 25 to input data, and a feedback mechanism 26 (FIGURE 6) coupled to the keypad mechanism 23. A validation device, generally designated 27, is provided which is adapted to determine the validation of information relating to the identification card 22 upon cooperation thereof with the card reader 21. The validation device 27 is operably coupled to the feedback mechanism 26 to visually inform the Player that the information relating to the Player's identification has been validated or invalidated.

[0026] Accordingly, the keypad mechanism itself is employed as a means to visually inform the Player about particular information relating to the Player's identification. The identification indicia, for example, include the input of a Personal Identification Number (PIN), a key, a SMARTCARD, an electronic button, a finger print imaging device, a retinal scan, combinations of any of these, combinations of a credit or debit card and any of the foregoing, etc. Moreover, the information relating to the Player's identification may include information relating to the Player's identification card such as the manual input of the PIN or a proper identification card insertion and read of the card in the card reader.

[0027] Once the player inserts their personal identification card into the card reader, or the Player inputs their PIN into the keypad mechanism, for example, the Player is visually informed of the validation or invalidation of such particular information through the illumination or non-illumination of the keypad assembly. This enables the Player to direct their attention immediately to the keypad mechanism to visually determine the validation of the particular information relating to the identification card. Unlike the current information validation systems, this is advantageous in that the key-in or acquisition of additional data may commence more quickly once verification occurs since the Player's attention is already directed toward the keypad.

[0028] The present invention is particularly suitable for use with a player tracking system 28 which, in the gaining industry, is typically employed for tracking Players of a plurality of gaining machines 30. Briefly, as shown in the schematic diagram of FIGURE 3, each gaining machine 30 is electrically interfaced to a central player tracking or host system computer 32 through a respective a player tracking module 31. The player tracking system 28 further includes card reader 21, keypad assembly 20 and a display device 33 which collectively allow the Player to interface with the system computer 32. Once the Player's identification is verified, preferably via an issued player identification card 22 which itself incorporates a unique personal identification code, the keypad assembly 20 of the present invention will allow the player tracking module 31 to obtain information from the Player through key component presses and to assess the validation of the particular information through the visualization of the backlit key components 25.

[0029] Briefly, it will be understood that the details of the circuitry and electronics of the present invention, such as the microcontrollers, the application software, and the like, may be resident in any one of the keypad mechanism 23, the host system computer 32, the gaming machine itself, or a combination thereof. However, for clarity and the easy of description, the present invention is primarily described in reference to the embodiment having the majority of the componentry resident in the keypad assembly. Most of this componentry, however, may adaptable for application with the system computer or the gaming machine with minimal design change.

[0030] FIGURE 3 illustrates that the player tracking module 31 further includes a player tracking controller unit 35 which generally performs the functions of communicating with the gaming machine, communicating with the system, verifying the card was read correctly, writing data to display. Operably coupled to this unit 35 is the keypad assembly 20 of the present invention which enables the Player to interface with the other components of the player tracking system 28 such as the card reader 21 and the host system computer 32. The keypad assembly 20 includes an onboard microcontroller 36 which provides all scanning and decoding functions of the keypad component matrix, as well as control of the visual feedback of the individual keys. This microcontroller 36 further operates to interface the player tracking controller unit 35 with the keypad mechanism 23 through a clocked serial interface (FIGURES 3 and 4). Thus, the keypad assembly 20 of the present invention is adaptable to interface with existing player tracking controller units through clocked serial connections, or with new versions of the player tracking controller units through ASYNC serial communications and I^{2}C serial communications.

[0031] Referring back to FIGURE 2, the keypad mechanism 23 preferably includes sixteen (16) key components aligned in a 4x4 matrix. It will be appreciated, of course, that a larger or smaller matrix may be employed. Preferably, keypad includes ten (10) conventional number key components 25', a "cocktail" key component 25" and an "attendant" key component 25'". Four (4) programmable "function" key components 25"" may be included for optional functions and features such as the inquiry of information relating jackpot bonus games, player tracking information or the like.

[0032] During conventional data input use, the key components 25 may be configured to illuminate and/or flash when pressed and/or not pressed, such as when the Player's Personal Identification Number (PIN) is being keyed-in through the keypad mechanism 23. Briefly, and as shown in an exemplary schematic diagram of the keypad mechanism 23 in FIGURE 5, the columns of the keypad matrix are scanned by embedded software and the row inputs are read in and decoded. Column selection is performed by the use of two bits from port RA (RA0 and RA1). These output ports are connected to one half of a 74HC139 2-to-4 decoder. As a binary pattern is presented to the input of the 74HC139, one of the 4 outputs is driven low. This is the select for a column. As viewed in the schematic diagram, port RB0 — RB3 are all tied to V_{CC} with a 10K resistor to assert a logic true condition until a key component 25 is pressed. When a particular key component 25 is pressed, the corresponding row is sinked to ground which causes a zero (0) to be read on the corresponding pin of port RB(RB0-RB3). Each of the column sinks is isolated with a diode, allowing any two key components 25 to be depressed simultaneously with full identification by the microcontroller 36. Should any more than two key components be depressed simultaneously, an invalid input will be yielded and should be rejected as invalid input.

[0033] The illumination devices 26, preferably Light Emitting Diodes (LED), are driven through a similar column select as that of the keypad components. As viewed in FIGURE 5, two bits of RA are used to control the other half of the 74HC139 decoder (RA2 and RA3). The output of the decoder is connected to a current sink. During reset conditions, the 74HC139 decoder is disabled to guarantee that a column of LEDs is not selected when the processor is not active. Port D (RD0-RD7) is used to drive the column source drivers for the LEDs, which therefore requires the LEDs to be multiplexed. The outputs of RD are connected to the red and green LED drive signals as follows:

RD0 =	Row 0 red
RD1 =	Row 0 green
RD2 =	Row 1 red
RD3 =	Row 1 green
RD4 =	Row 2 red
RD5 =	Row 2 green
RD6 =	Row 3 red
RD7 =	Row 3 green

[0034] To provide the desired visual feedback function, each key component 25 is backlit by a respective illumination device 26 which is operably connected to the microcontroller 36 of the validation device 27 for on/off operation thereof. As best viewed in the cross-section of FIGURE 6, each key component 25 preferably includes a flexible translucent or transparent cover 37, such as silicone rubber or the like, which is formed to house the illumination device 26 therein. Upon illumination, the light generated by the illumination device 26 radiates out of the top of the cylindrical column 38 and through the translucent cover 37 to provide the backlit visual illumination.

[0035] In the preferred embodiment, each illumination device 26 is provided by a conventional Light Emitting Diode (LED). Advantageously, these LEDs reduce power consumption and generate substantially less heat than incandescent lights. More preferably, these LEDs are tri-color-type LEDs capable of illumination in red, green or yellow. Other colors may be employed, however. In this manner, at least one or a plurality of key components 25 can be illuminated in a first lighting mode to visually inform the Player that the information relating to the identification card has been validated, while in the event of an invalidation of the information, the validation device includes a second lighting mode to visually inform the Player that the information relating to the identification card has not been validated. For instance, upon validation of the particular information, one or a plurality of the backlit key components 25 may be illuminated in the color "green" to indicate a "valid" key-in of the Personal Identification Number (PIN) in the keypad mechanism 23. In contrast, in the second lighting mode, the backlit keys may be illuminated in the color "red" to indicate an invalid input of the required information thereof.

[0036] Moreover, since each multi-color LED is individually addressable, the 4x4 matrix may be illuminated in predetermined patterns, as well as multiple color schemes. For example, upon validation of the particular information such as proper identification card insertion, the validation device may illuminate the keypad matrix in a first illumination pattern (i.e., the first lighting mode). Such a pattern, as shown in FIGURE 7, may be in the form of an "√" symbol in the color green by illuminating the "F2", "3", "5" and "7" key components 25, while in the event of invalidation of the information, a second illumination pattern (i.e., the second lighting mode) in the form of an "X" symbol in the color red may be illustrated (FIGURE 8) by illuminating the "1", "3", "5", "7" and "9" key components 25 . It will be understood, of course, that other symbols as well as other color schemes may be employed without departing from the true spirit and nature of the present invention.

[0037] In accordance with another aspect of the present invention, the keypad assembly 20 may include an attract sequence which animates the keypad components 25 when the keypad assembly 20 is not in use. For example, using a set of animation tables residing in code ROM, the individually addressable LEDs can be flashed in a patterned or colored sequence to attract Players to the gaming machine 30. Such an attract sequence may be automatically activated during non-use of the keypad or when the card reader is in non-use. Upon detection of use of a key component closure or insertion of an identification card, the microcontroller 36 can abort the attract sequence. Additionally, more than one animation mode may be included depending upon the circumstance, such as during bonus play.

[0038] Referring now to FIGURE 9, the card reader 21 is illustrated with the identification card 22 inserted in a card reader opening 40 thereof. In accordance with the present invention, any conventional card reader device may be utilized which is adapted to read/write cards having magnetic strips, bar codes, etc. Moreover, other state of the art identification devices may be used, such as SMARTCARD technology, which generally describe cards having a computer processor for use in a secure payment system and are employed for player tracking and/or cashless gaining use. Typically, these cards include a stored or embedded card identification number which identifies the origin of the particular card read by the card reader. As an example, and for security purposes, especially with smart and debit card applications, the input of a PIN code may be necessary, similar to an ATM card, before use or commencement of the player tracking system. In this configuration, thus, the Player may be required to input or key-in a four to six digit identification code through the keypad mechanism for validation. Once the keyed-in PIN code is input, the microcontroller 36 or the tracking system host computer 32 compares this input code with the Player's PIN code stored in the host computer for validation thereof. Upon validation, the keypad assembly 20 of the present invention would immediately visually inform the Player of such validation by illuminating one or more of the key components 25.

[0039] In another example, these tracking systems often incorporate an identification code specific to the institution of issuance. Thus, in the same manner, should the identification code read from the identification card 22 fail to correspond to the institution identification code, then the keypad would indicate an invalid illumination.

[0040] In still another example, the validation device 27 of the present invention may further include a sensor device or the like which cooperates with the card reader to determine whether the identification card 22 has been properly inserted into the card opening 40 of the card reader. Should the sensor indicate that the identification card 22 has been properly seated in the card reader 21 for a proper card "read", the keypad mechanism will be illuminated in a "valid" mode of operation.

[0041] Incorporated in the keypad assembly 20 is software which performs the following functions for the keypad mechanism 23. These functions include receive commands from and send key press information to the player tracking controller unit 35. Moreover, the keypad software further functions to acknowledge receipt of commands from the player tracking controller, decode and debounce key switch activation, and process commands received from the player tracking controller unit 35.

[0042] The control of all back lighting of keypad mechanism 23, as executed by the microcontroller 36, is further operated by the keypad software. Briefly, each key component 25 can be lit when released and/or lit when pressed, and/or each key can be flashing when released and/or flashing when pressed. The keypad software further includes a set of built-in attract sequences which animate the key colors when the keypad is not in use. Attract sequences can be selected using the command language.

[0043] More specifically, in accordance with the attributes and subroutines, an attribute table resides in on-chip RAM which comprises 16 attribute bytes, each of which includes a 16-byte array residing in on-chip RAM which comprises 16 attribute bytes, each of which corresponds to one key component 25. The respective attribute byte for a key component determines whether the LED is illuminated when pressed, not illuminated when not pressed, the color of illumination if lit, and whether the respective LED is flashed when pressed and/or not pressed.

[0044] At a command interface, the commands are received from the host computer 32 via a clocked serial interface. Preferably, this is at rate of 9600 baud, but may vary in accordance with the state of the field. These commands include a define keypad attributes command, an attract mode command and a stop attract mode command. Each command is composed of an address (wakeup bit set) byte; a command code byte; a length of command byte, including address, command code, length byte, all data and both CRC bytes; an optional data byte; a CRC low byte; and a CRC high byte. Furthermore, each byte of a command consists of a start bit, 8 data bits, a 9th bit called the wakeup bit, and a stop bit.

[0045] In a Keypad Status Reporting routine, whenever a key component 25 is pressed, an ASCII code corresponding to the key component is sent to the host system computer 32. If a command is being received from the host computer system when the key component is pressed, the ASCII code is not sent until command reception is completed. The keypad status reporting is handled by a main loop code, to be discussed below. A single-byte buffer will contain a key code if the interrupt service routine has detected a key closure. Another subroutine NEWK determines if the key closure is that of a new key component. In the event that the key closure is a new key, a subroutine ASCTRANS is called to send the ASCII code to the host system computer 32. The single-byte buffer is then set to zero to indicate that it is ready to handle another key component.

[0046] During an initialization routine after a power-up, a subroutine INIT_PIC commences to perform three initialization functions. These functions include the programming and initialization of the I/O ports, and the programming of a timer 0 to overflow every 10 milliseconds. Finally, the attribute table is initialized with default keypad attributes such as: off when the key component is not pressed, and a solid yellow illumination of the LEDs when a corresponding key component is pressed.

[0047] After initialization is complete, the main loop code accesses two subroutines. A CK_BUFFER subroutine checks if a new key component has been pressed. A SENDKEY subroutine is then accessed to send the ASCII code to the host system computer. Secondly, a CK_COMMAND subroutine checks for a start bit from the host computer system. Should the start bit be detected, this subroutine subsequently receives a byte from the host computer system. If the byte received is the last byte of a command, the CK_COMMAND subroutine interprets and executes the command.

[0048] Timer 0 is configured to continuously interrupt the microcontroller 36 at 10 ms intervals. During each interrupt, the keypad mechanism 23 is scanned, and any backlighting is commenced or refreshed. Further tasks are preferably performed at this time include flash timing, and an attract mode animation, which are discussed henceforth.

[0049] During keypad scanning, each column of the keypad mechanism 23 is scanned at 10 millisecond intervals by the Timer 0 interrupt service routine. A variable contains the column number currently being scanned, and is incremented at each timer 0 interrupt. The column number is used to enable a key column via the microcontroller output Port A. Key closures are then detected by reading the microcontroller input port B. When a key component 25 closure is detected, its code is stored in the single-byte key buffer, but only if the single-byte key buffer is 0. In the event the single-byte key buffer already contains a key code, this code will not overwritten. The main loop code will translate the key code into an ASCII code and send it to the host system computer 32. As previously described, single-byte key buffer is then set to zero which indicates to the interrupt service routine that another key code can be sent.

[0050] Immediately after the keypad scan, backlighting of the corresponding keypad LEDs commences in the key column being scanned. The keypad attributes are fetched from the attribute array and the LEDs are programmed with the appropriate color depending on whether a key component is pressed or not. If the key attribute indicates flashing, and the flasher bit is "OFF", the corresponding LED is turned off.

[0051] As above-indicated, flash timing of the keypad assembly commences during each interrupt interval. A subroutine BLINK is accessed which complements all the flasher bits in the keypad attribute table. This is preferably performed about every 116th interval, which yields a flash interval of about 1.2 seconds. Another predetermined number of intervals may be employed of course.

[0052] In an attract mode, the key component LEDs are animated using a set of animation tables which reside in code ROM. Each frame of the animation sequence consists of four (4) bytes. Each byte contains the 2-bit color code for four (4) key lights. The frames are preferably advanced every thirty-two (32) Timer 0 interrupt periods for an animation speed of 320 ms per frame.

[0053] As indicated, preferably three (3) animation modes are supported, which includes "snake", "swipe", and "fire" effects. For example, a "snake" effect would emulate a snake moving around the keypad, while a "swipe" effect would appear as a color change sweeping across the entire keypad. Finally, the "fire" effects would employ the colors of the LED to emulate fire.

[0054] The animation mode determines which of three animation tables are used. A subroutine ANIMATE is preferably called every twenty-one (21) timer 0 interrupt periods to advance the frame. The ANIMATE subroutine retrieves the next frame from the animation table and employs this data to override the keypad attributes. Upon detection of a key component closure, the attract mode is aborted.

[0055] In accordance with another aspect of the present invention, a method of validating information relating to a Player's identification for a gaming device is provided including the steps of receiving an identification card 22 in a card reader opening 40 of the card reader 21, and providing a keypad assembly having a plurality of key components for the input of data. The next step includes validating information relating to the identification card 22 upon insertion of the card into the card reader opening for reading thereof; and illuminating an illumination device 26 on the keypad mechanism 23 to visually inform the Player that the information relating to identification card has been validated.

[0056] Upon validation of the information, the method of the present invention includes illuminating the illumination device 26 in a first lighting mode to visually inform the Player that the information relating to the identification card has been validated. In the event the information relating to the identification card has not been validated, the method includes illuminating the illumination device 26 in a second lighting mode to visually inform the Player of the invalidation. The first lighting mode, for example, may include illuminating the multi-color LEDs in one color in the first lighting mode, and illuminating the multi-color LEDs in another color in the second first lighting mode.

[0057] The method of the present invention may further includes the step of illuminating the illumination device 26 in a third lighting or attract mode when no identification card 22 is positioned in the card reader opening 40. Further, the validating information includes the step of reading a unique identification code encoded on the identification card, and comparing the identification code to a predetermined code to determine the validation.

[0058] Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, although the specification has described a keypad assembly and card reader on gaming machines, such interface may be used on other casino stations as well. For example, a pad assembly of the type described above may also be used with blackjack or craps tables. Further, the systems of this invention are not limited to conventional casino gaming machines and stations, but may include other machines such as amusement machines, televisions, vending machines, etc. In addition, the reader will understand that the terminals as describe herein can be with gaming machines that are not necessarily located in a casino or connected to a LAN. Thus, in some embodiments, the gaming machines incorporating the keypad assembly of this invention may be stand-alone machines located in bars, drug stores, or other establishments.

Claims

1. A keypad assembly for use with a card reader configured to read a player identification card therein, said keypad assembly comprising:

a keypad mechanism having a plurality of keys to input data;
a feedback mechanism coupled to the keypad mechanism;
a validation device adapted to determine the validation of information relating to the identification card upon cooperation thereof with the card reader, said validation device further being operably coupled to the feedback mechanism to visually inform the Player that the information relating to the identification card has been validated or not validated.

2. The keypad assembly as defined in claim 1, wherein

said feedback mechanism includes an illumination device mounted to the keypad mechanism.

3. The keypad assembly as defined in claim 2, wherein

said validation device includes a first lighting mode to visually inform the Player that the information relating to the identification card has been validated, and a second lighting mode to visually inform the Player that the information relating to the identification card has not been validated.

4. The keypad assembly as defined in claim 2, wherein

said keys are translucent for back lighting thereof, and said illumination device includes a plurality of illumination devices each corresponding to a respective key.

5. The keypad assembly as defined in claim 4, wherein

each said illumination devices is provided by a Light Emitting Diode (LED).

6. The keypad assembly as defined in claim 5, wherein

each said LED is a multi-color LED illuminating one color in a first lighting mode to visually inform the Player that the information relating to the identification card has been properly validated, and illuminating another color in a second lighting mode to visually inform the Player that the information relating to the identification card has not been properly validated.

7. The keypad assembly as defined in claim 4, wherein

said information relating to the identification card includes the validation of an identification code input through the key components by the Player.

8. The keypad assembly as defined in claim 7, wherein

said key components of the keypad mechanisms are arranged in a matrix,
said validation device includes a first illumination pattern of illuminated keys components of said matrix upon validation of the identification code, and includes a second illumination pattern of illuminated keys components of said matrix upon the invalidation of the identification code.

9. The keypad assembly as defined in claim 8, wherein

said first illumination pattern is in the form of an "√" symbol, and said second illumination pattern is in the form of a "X" symbol.

10. The keypad assembly as defined in claim 1, wherein

said information relating to the identification card includes the proper insertion into a card reader opening of the card reader for reading thereof.

11. The keypad assembly as defined in claim 10, wherein,

said validation device includes a sensing device cooperating with the card reader to detect the proper insertion of the identification card in said card reader opening.

12. The keypad assembly as defined in claim 2, wherein

said information relating to the identification card includes gaming establishment code information to verify use at selected establishments.

13. The keypad assembly as defined in claim 6, wherein,

said validation device includes a microcontroller to control the animation of each light emitting diode in the first lighting mode and the second lighting mode.

14. The keypad assembly as defined in claim 13, wherein,

said microcontroller further includes an attract mode which operates each light emitting diode in an attract sequence when no identification card is positioned in the card reader opening.

15. A player tracking system for tracking Players of a plurality of gaming machines interconnected to a host computer comprising:

a player tracking device adapted to monitor the game play of a Player;
a card reader for reading a player identification card inserted in a card reader opening of the card reader;
a keypad mechanism having a plurality of keys to input data for use in the player tracking device;
an illumination device coupled to the keypad;
a validation device adapted to determine the validation of information wherein said illumination device is illuminated at the keypad mechanism to visually inform the Player that the information relating to identification card has been validated.

16. The player tracking system as defined in claim 15, wherein

said validation device includes a first lighting mode to visually inform the Player that the information has been validated, and a second lighting mode to visually inform the Player that the information has not been validated.

17. The player tracking system as defined in claim 15, wherein

said keys are translucent for back lighting thereof, and said illumination device includes a plurality of illumination devices each corresponding to a respective key.

18. The player tracking system as defined in claim 17, wherein

each said illumination device is provided by a multi-color Light Emitting Diode (LED) illuminating one color in a first lighting mode to visually inform the Player that the information has been properly validated, and illuminating another color in a second lighting mode to visually inform the Player that the information has not been properly validated.

19. The player tracking system as defined in claim 18, wherein

said validation device includes a sensing device cooperating with the card reader to detect the proper insertion of the identification card in said card reader opening.

20. The player tracking system as defined in claim 18, wherein,

said validation device includes a microcontroller to control the animation of each LED in the first lighting mode and the second lighting mode.

21. The player tracking system as defined in claim 20, wherein,

said microcontroller further includes an attract mode which operates each LED in an attract sequence during non-use of the card reader.

22. The player tracking system as defined in claim 17, wherein

said information includes the validation of an identification code input through the key components by the Player.

23. The player tracking system as defined in claim 22, wherein

said key components of the keypad mechanisms are arranged in a matrix,
said validation device includes a first illumination pattern of illuminated keys components of said matrix upon validation of the identification code, and includes a second illumination pattern of illuminated keys components of said matrix upon the invalidation of the identification code.

24. The player tracking system as defined in claim 23, wherein

said first illumination pattern is in the form of an "√" symbol, and said second illumination pattern is in the form of a "X" symbol.

25. A method of validating information relating to a player identification card inserted into a card reader of a gaming device comprising:

receiving the identification card in a card reader opening of the card reader;
providing a keypad mechanism having a plurality of keys for the input of data;
validating information relating to the identification card upon insertion of the card into the card reader opening for reading thereof; and
illuminating an illumination device on the keypad mechanism to visually inform the Player that the information relating to identification card has been validated.

26. The method as defined in claim 25, wherein

the validating information includes illuminating the illumination device in a first lighting mode to visually inform the Player that the information relating to the identification card has been validated, and illuminating the illumination device in a second lighting mode to visually inform the Player that the information relating to the identification card has not been validated.

27. The method as defined in claim 26, wherein

the illuminating the illumination device includes back lighting at least one of said keys.

28. The method as defined in claim 27, wherein

the illumination device is provided by a multicolor Light Emitting Diode (LED), and
the back lighting of the at least one key includes illuminating the multi-color LED in one color in the first lighting mode, and illuminating the multi-color LED in another color in the second first lighting mode.

29. The method as defined in claim 26, wherein

said information relating to the identification card includes the proper insertion into a card reader opening of the card reader for reading thereof.

30. The method as defined in claim 29, wherein,

the validating information includes sensing the proper insertion of the identification card in said card reader opening for reading thereof.

31. The method as defined in claim 25, further including:

tracking the Player's game play on the gaming device upon validation of the information.

32. The method as defined in claim 26, further including:

illuminating the illumination device in a third lighting mode when no identification card is positioned in the card reader opening.

33. The method as defined in claim 26, wherein

the illuminating the illumination device includes back lighting each key in the first lighting mode, when the information relating to the identification card has been validated, and back lighting each key in the second lighting mode when the information relating to the identification card has not been validated.

34. The method as defined in claim 33, further including:

back lighting each key in a third lighting mode when no identification card is positioned in the card reader opening.

35. The method as defined in claim 25, wherein,

said validating information includes reading an identification code encoded on said identification card, and further including:
comparing said identification code to a predetermined code to determine the validation.

36. A method of validating information relating to a player identification card inserted into a card reader of one of a plurality of gaming device interconnected to a host computer, the method comprising:

receiving the identification card in a card reader opening of a card reader of one of the gaming devices;
validating information relating to the identification card upon insertion of the card into the card reader opening for reading thereof; and
illuminating an illumination device on a keypad mechanism, having a plurality of keys for the input of player tracking data, to visually inform the Player that the information relating to the identification card has been validated.

37. The method as defined in claim 36, further including:

after validating the information, enabling the Player to input player tracking data through the keys of said keypad mechanism.

38. The method as defined in claim 36, further including:

after the validating the information, tracking the Player's game play on the gaming device.

39. The method as defined in claim 36, wherein

the validating information includes illuminating the illumination device in a first lighting mode to visually inform the Player that the information relating to the identification card has been validated, and illuminating the illumination device in a second lighting mode to visually inform the Player that the information relating to the identification card has not been validated.

40. The method as defined in claim 39, wherein

the illuminating the illumination device includes back lighting each key in the first lighting mode, when the information relating to the identification card has been validated, and back lighting each key in the second lighting mode when the information relating to the identification card has not been validated.

41. The method as defined in claim 40, wherein

each illumination device is provided by a multi-Light Emitting Diode (LED), and
the back lighting of the keys include illuminating the multi-color LED in one color in the first lighting mode, and illuminating the multi-color LED in another color in the second first lighting mode.

42. The method as defined in claim 41, further including:

after validating the information, enabling the Player to input player tracking data through the keys of said keypad mechanism.

43. The method as defined in claim 42, further including:

after the validating the information, tracking the Player's game play on the gaming device.

44. The method as defined in claim 36, wherein,

the validating information includes sensing the proper insertion of the identification card in said card reader opening for reading thereof.

45. The method as defined in claim 44, wherein, said validating information further includes reading an identification code encoded on said identification card, and further including:

comparing said identification code to a predetermined code to determine the validation.

46. The method as defined in claim 45, further including:

illuminating the illumination device in a third lighting mode when no identification card is positioned in the card reader opening.

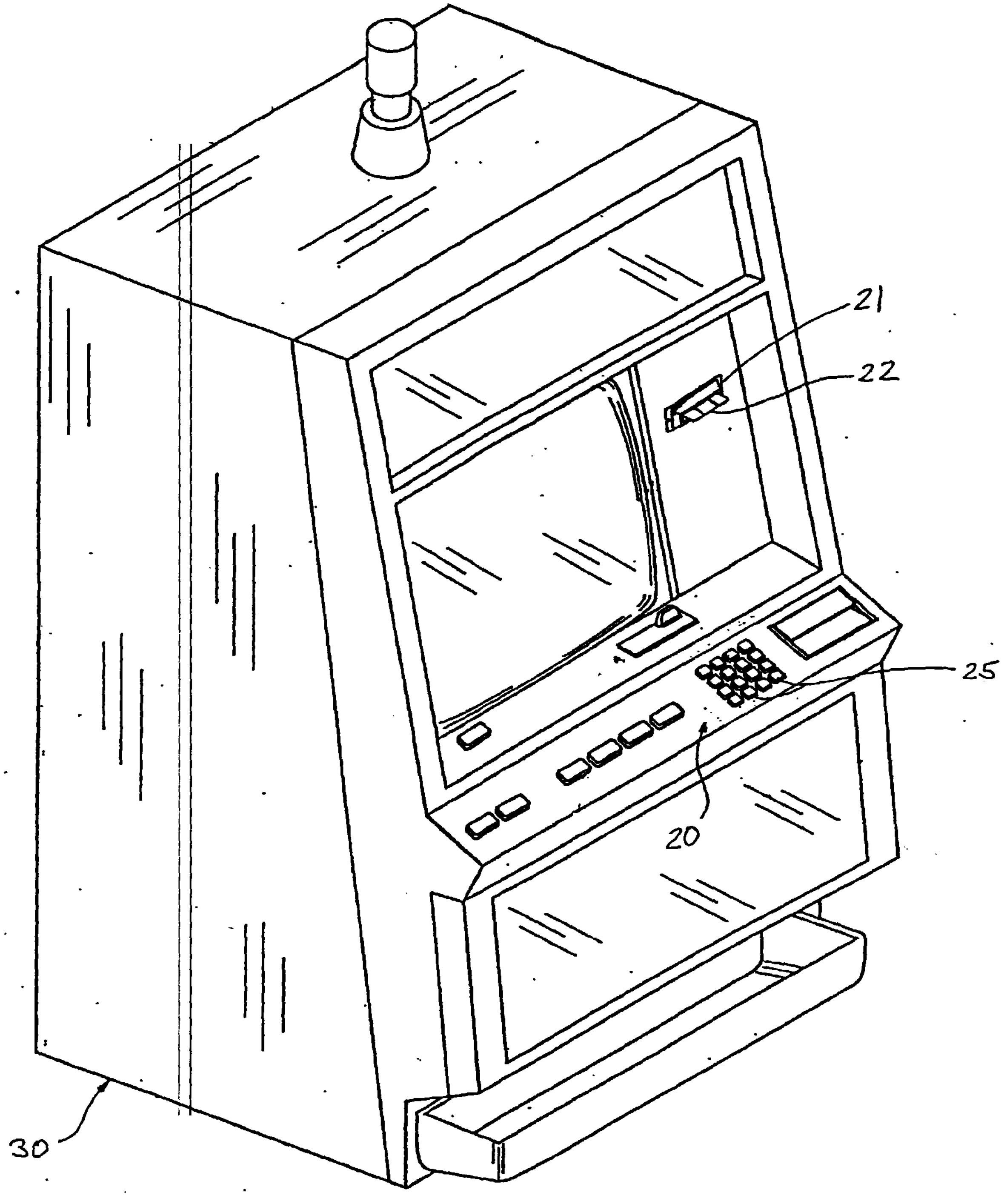


FIG._1

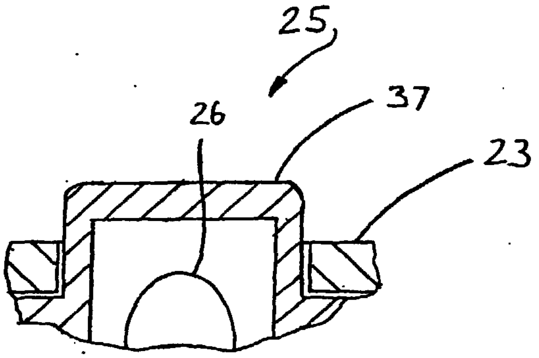


FIG._6

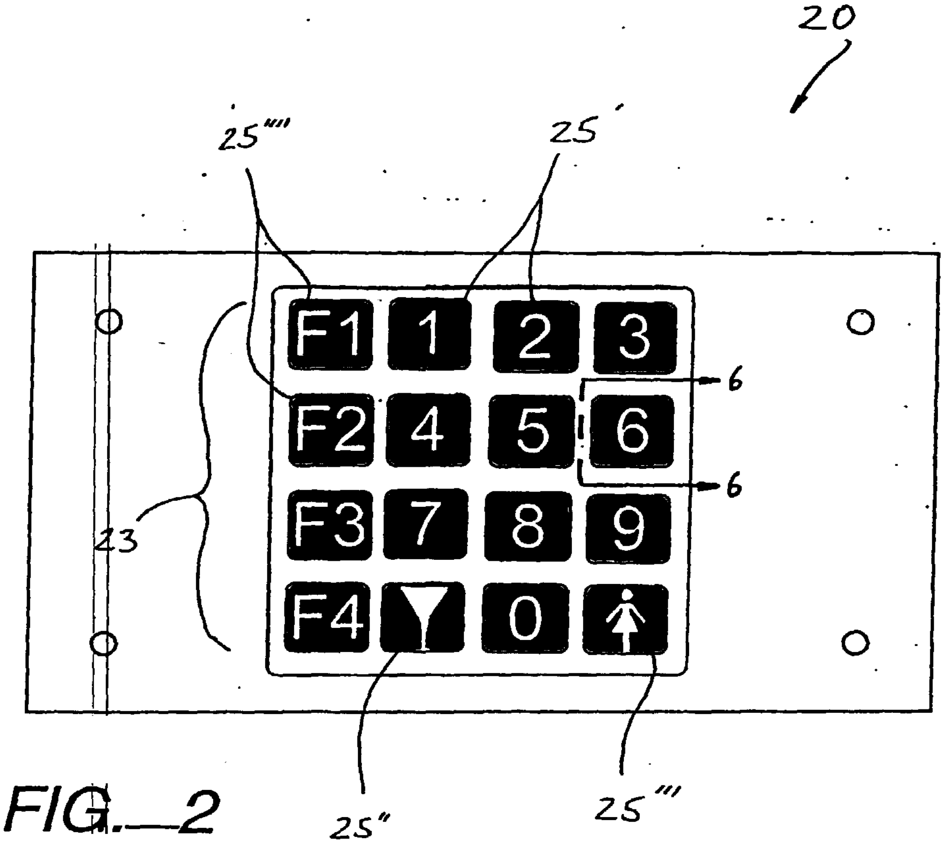


FIG._2

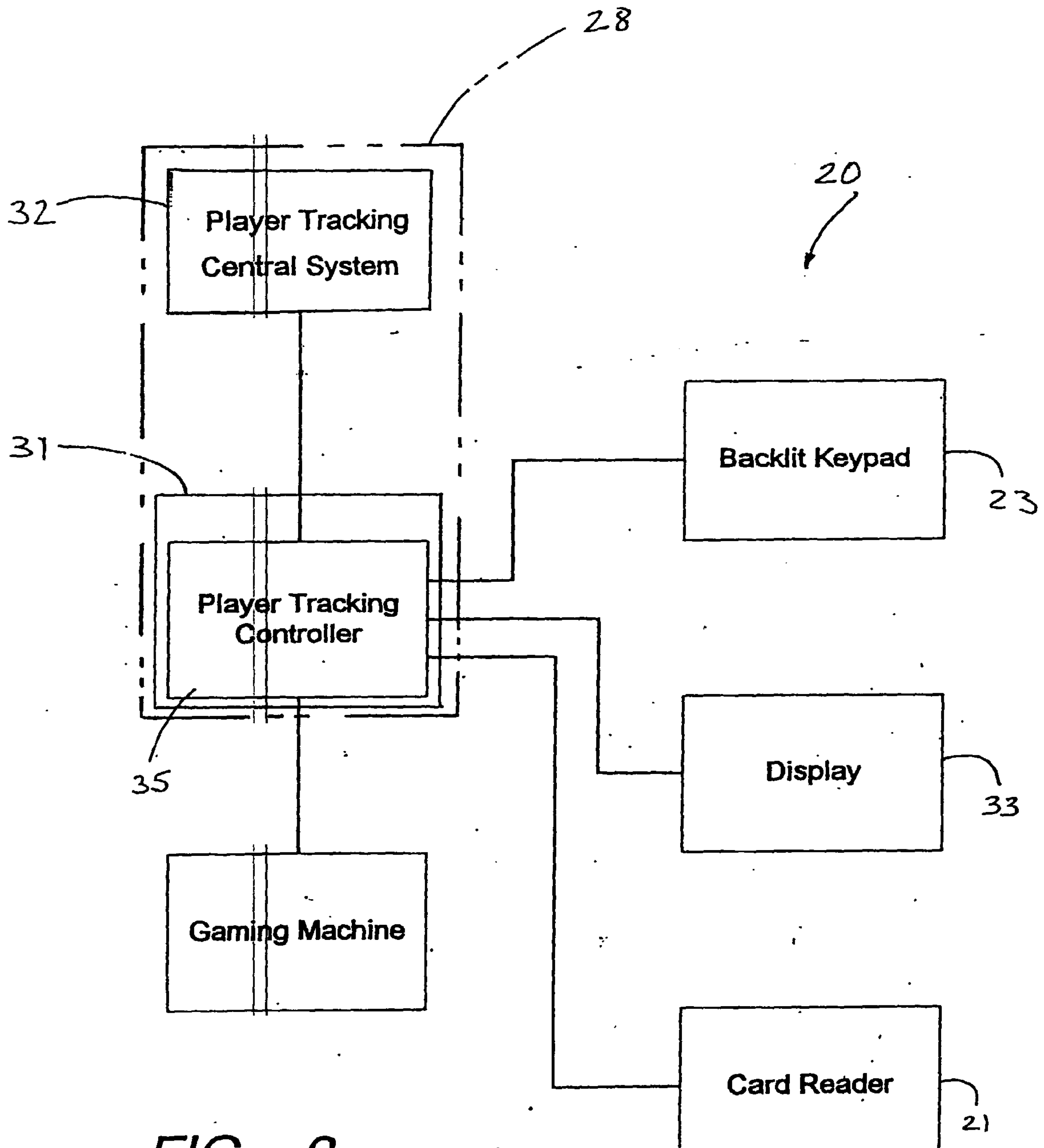

28
20
32
Player Tracking Central System
31
Player Tracking Controller
35
Backlit Keypad
23
Display
33
Gaming Machine
Card Reader
21

FIG._3

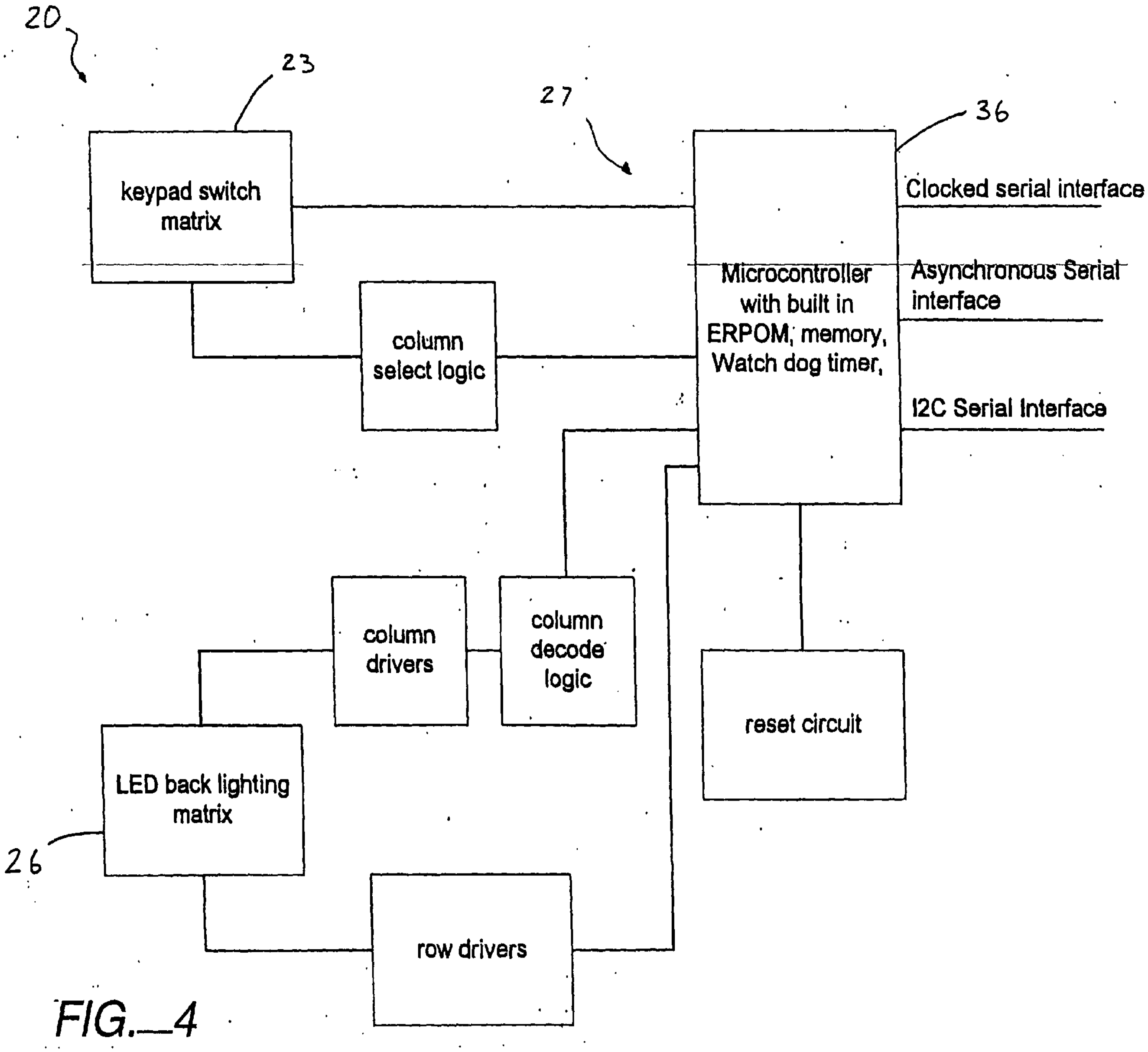

20
23
keypad switch matrix
27
36
Microcontroller with built in ERPOM, memory, Watch dog timer,
Clocked serial interface
Asynchronous Serial interface
I2C Serial Interface
column select logic
column drivers
column decode logic
reset circuit
LED back lighting matrix
26
row drivers

FIG.__4

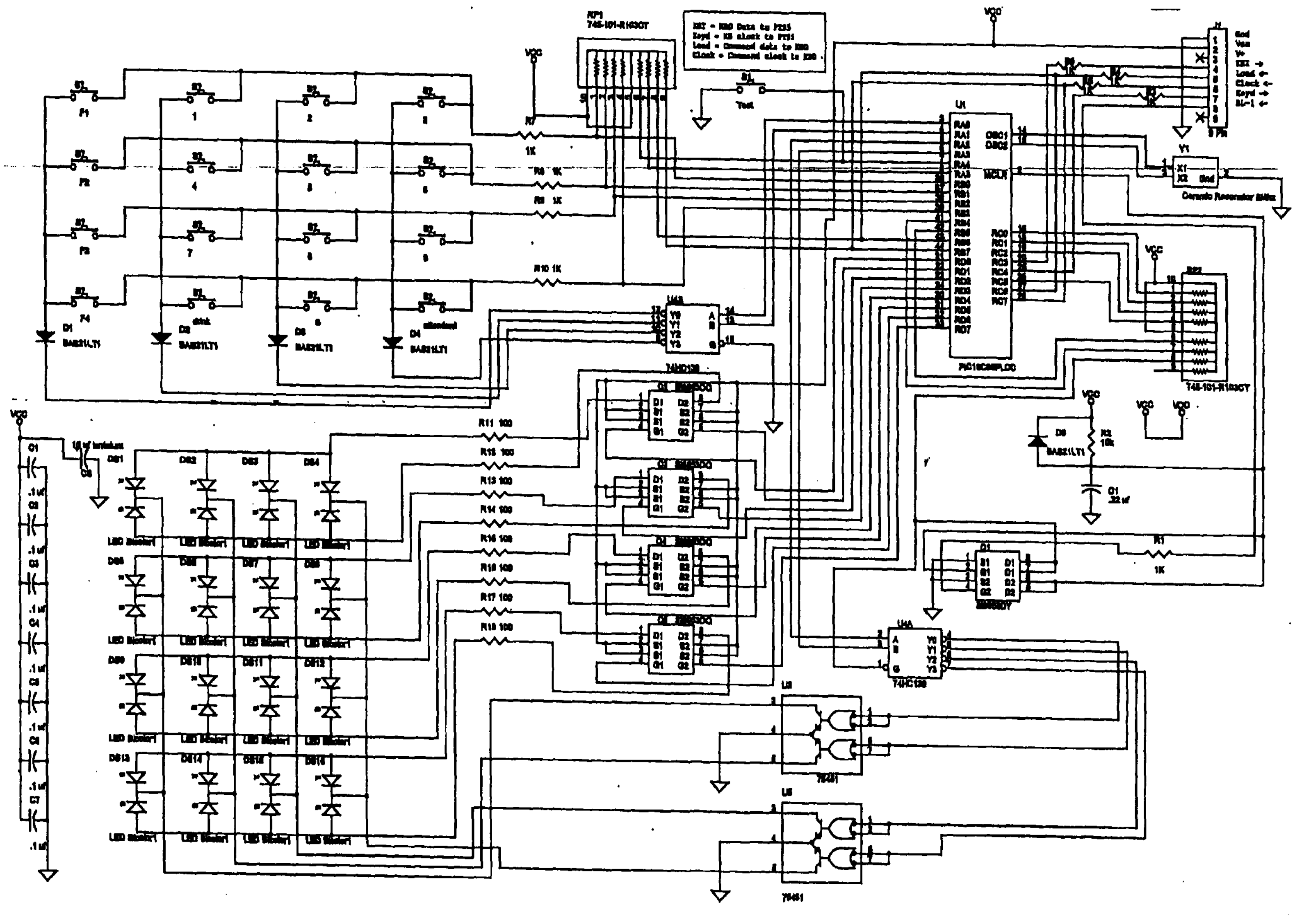

RP1
74S-101-R103GT
RKI = KBD Data to PT35
Keyd = KB clock to PT35
Load = Command data to KBD
Clock = Command clock to KBD
VCC
J1
Gnd
Vss
V+
RKI →
Load ←
Clock ←
Keyd →
BL-1 ←
9 Pin
S1
Test
U1
RA0
RA1
RA2
RA3
RA4
RA5
RB0
RB1
RB2
RB3
RB4
RB5
RB6
RB7
RD0
RD1
RD2
RD3
RD4
RD5
RD6
RD7
OSC1
OSC2
MCLR
RC0
RC1
RC2
RC3
RC4
RC5
RC6
RC7
PIC16C65PLCC
Y1
X1
X2
Gnd
Ceramic Resonator 8Mhz
RP2
74S-101-R103GT
S2
F1
F2
F3
F4
1
2
3
4
5
6
7
8
9
deal
attendant
D1
D2
D3
D4
BAS21LT1
R7
1K
R8 1K
R9 1K
R10 1K
U4B
Y0
Y1
Y2
Y3
A
B
G
74HC139
Q1
Q2
Q3
Q4
D1
S1
G1
D2
S2
G2
R11 100
R12 100
R13 100
R14 100
R15 100
R16 100
R17 100
R18 100
D5
BAS21LT1
R2
10k
C1
.22 uf
R1
1K
U4A
74HC139
DS1
DS2
DS3
DS4
DS5
DS6
DS7
DS8
DS9
DS10
DS11
DS12
DS13
DS14
DS15
DS16
LED Bicolor1
10 uf tantalum
C8
C1
C2
C3
C4
C5
C6
C7
.1 uf
U2
U3
75451

FIG._5

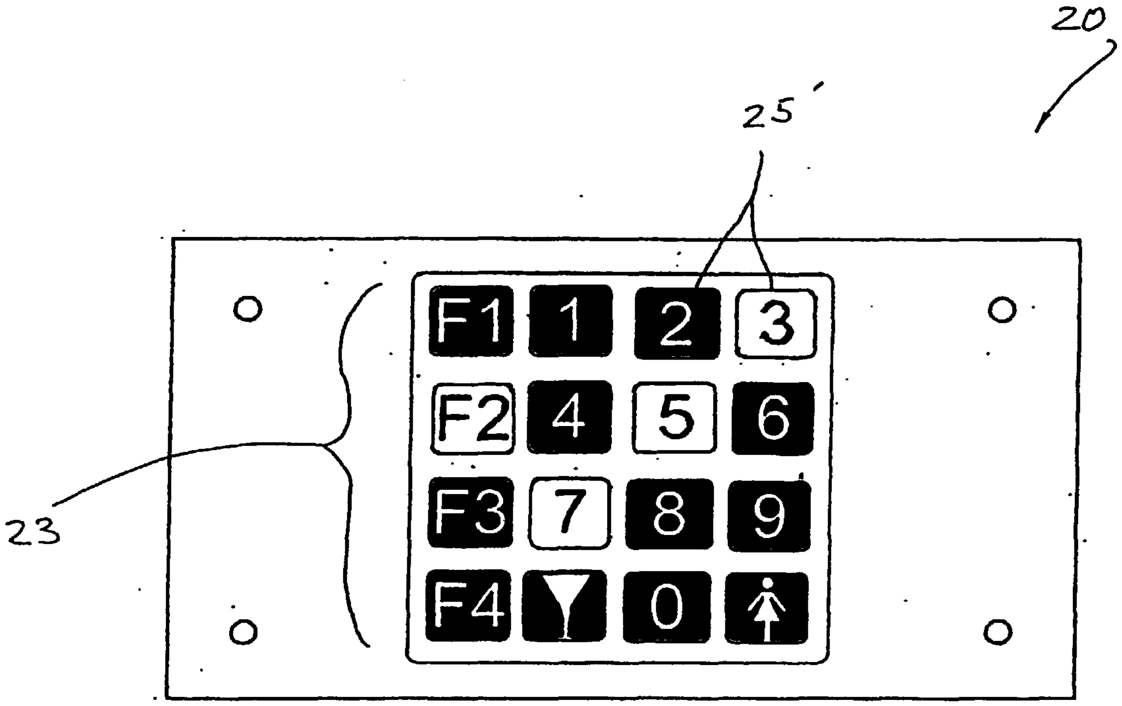


FIG._8

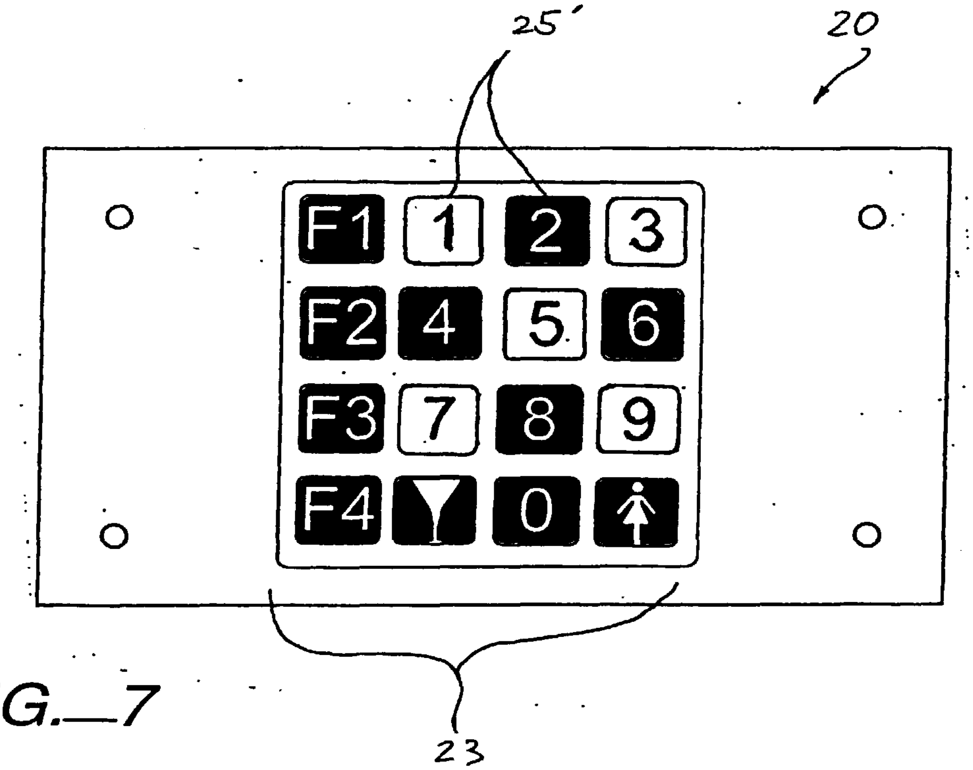


FIG._7

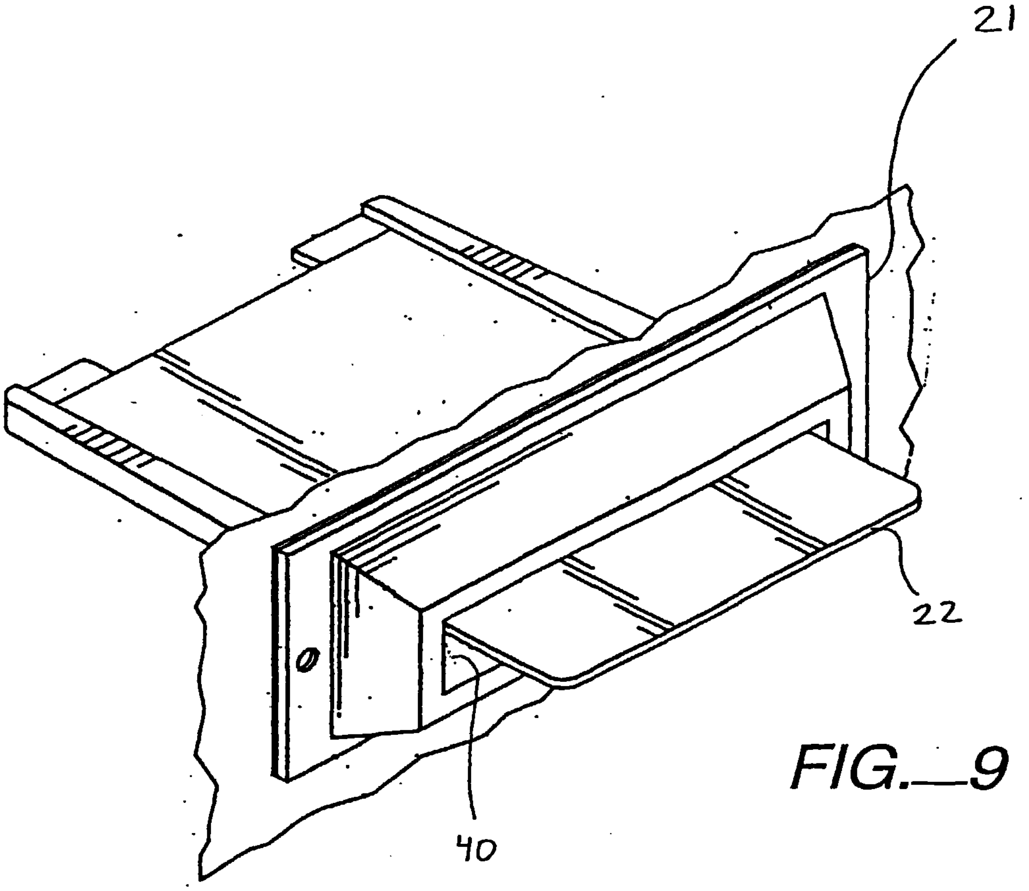


FIG._9

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 096 438 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
21.01.2004 Bulletin 2004/04

(43) Date of publication A2:
02.05.2001 Bulletin 2001/18

(21) Application number: **00123164.6**

(22) Date of filing: **25.10.2000**

(51) Int Cl.7: **G07F 7/10**, G07C 9/00

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.10.1999 US 430242**

(71) Applicant: **International Game Technology**
Reno, Nevada 89511-8986 (US)

(72) Inventors:
- **Uihlein, Mark**
  Henderson, Nevada 89014 (US)
- **Carson, Robert H., Jr.**
  Sparks, Nevada 89431 (US)
- **Powell, Tracy**
  Reno, Nevada 89511 (US)

(74) Representative:
Manitz, Finsterwald & Partner GbR
Postfach 31 02 20
80102 München (DE)

(54) A lighted keypad assembly, method and system for tracking players

(57) A keypad assembly and method for use with a card reader adapted to receive and read a player identification card therein. The keypad assembly includes a keypad mechanism having a plurality of keys to input data, and a feedback mechanism coupled to the keypad. A validation device is provided which is adapted to determine the validation of information relating to the identification card upon reading thereof in the card reader. The validation device is further operably coupled to the feedback mechanism to visually inform the Player that the information relating to identification card has been validated.

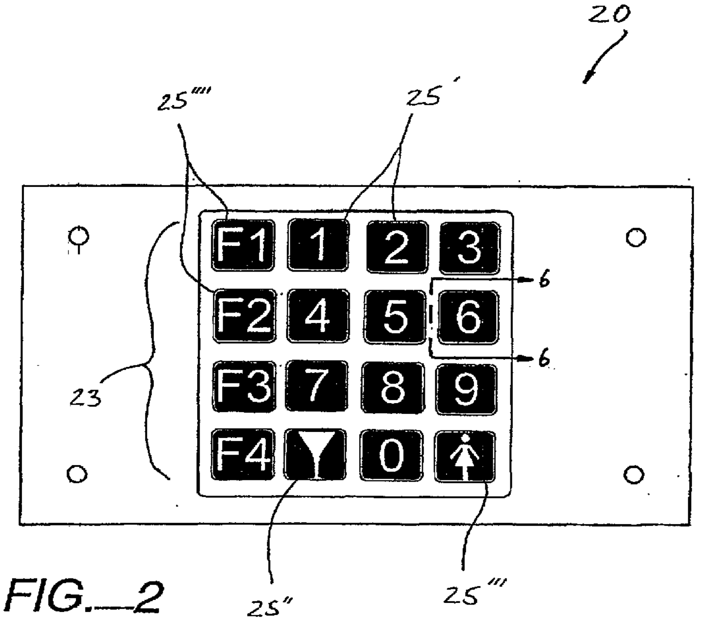


FIG._2

Printed by Jouve, 75001 PARIS (FR)

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 3164

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	EP 0 854 412 A (NCR INT INC) 22 July 1998 (1998-07-22) * the whole document * ---	1-46	G07F7/10 G07C9/00
Y	US 5 702 304 A (GINSBURG ALEC ET AL) 30 December 1997 (1997-12-30) * abstract * * column 1, line 50 - column 3, line 43 * * column 6, line 27 - column 8, line 63 * * column 11, line 21 - column 13, line 6 * * column 13, line 60 - column 15, line 38 * * column 19, line 2 - column 20, line 43 * * column 26, line 37 - column 30, line 57 * * figures 1-34 * ---	1-46	
A	US 5 326 104 A (PEASE LOGAN L ET AL) 5 July 1994 (1994-07-05) * abstract * * figures 1-6 * * column 3, line 49-64 * * column 5, line 34 - column 6, line 5 * * column 7, line 19 - column 14, line 38 * * column 15, line 34 - column 16, line 61 * * column 18, line 50 - column 19, line 40 * ---	1-46	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07C G07F G06F
A	EP 0 534 718 A (BALLY MFG CORP) 31 March 1993 (1993-03-31) * the whole document * ---	1-46	
A	EP 0 805 424 A (INT GAME TECH) 5 November 1997 (1997-11-05) * abstract * * column 10, line 36-56; claim 10 * * figures 1-5 * --- -/--	1-46	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 November 2003	Pañeda Fernández, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 3164

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 919 965 A (INT GAME TECH) 2 June 1999 (1999-06-02) * abstract * * paragraph ‘0030! * * paragraph ‘0042! - paragraph ‘0044! * * paragraph ‘0085! * * paragraph ‘0094! * * paragraph ‘0104! * * figures 1-6 * -----	1-46	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 November 2003	Pañeda Fernández, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 00 12 3164

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-11-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854412 A	22-07-1998	DE 69720674 D1	15-05-2003
		EP 0854412 A1	22-07-1998
		JP 11154046 A	08-06-1999
		US 5962830 A	05-10-1999
		ZA 9711123 A	15-06-1998
US 5702304 A	30-12-1997	US 5655961 A	12-08-1997
		US 6162122 A	19-12-2000
		AU 686824 B2	12-02-1998
		AU 2719295 A	02-05-1996
		AU 3587895 A	06-05-1996
		AU 697582 B2	08-10-1998
		AU 4847897 A	26-02-1998
		AU 7416198 A	03-09-1998
		US 6254483 B1	03-07-2001
		WO 9612262 A1	25-04-1996
		US 6565434 B1	20-05-2003
		US 5836817 A	17-11-1998
		US 5752882 A	19-05-1998
		US 5741183 A	21-04-1998
		US 5820459 A	13-10-1998
		US RE37885 E1	15-10-2002
		US 6319125 B1	20-11-2001
		US 2001055990 A1	27-12-2001
		US 6257981 B1	10-07-2001
US 5326104 A	05-07-1994	NONE	
EP 0534718 A	31-03-1993	US 5429361 A	04-07-1995
		AT 146617 T	15-01-1997
		AU 693736 B2	02-07-1998
		AU 1785997 A	19-06-1997
		AU 664384 B2	16-11-1995
		AU 2529192 A	25-03-1993
		CA 2078936 A1	24-03-1993
		DE 69216029 D1	30-01-1997
		DE 69216029 T2	24-07-1997
		EP 0534718 A2	31-03-1993
		ES 2099801 T3	01-06-1997
		GR 3022859 T3	30-06-1997
		JP 2901821 B2	07-06-1999
		JP 7024144 A	27-01-1995
		NZ 244274 A	21-12-1995
		ZA 9207244 A	08-07-1993
EP 0805424 A	05-11-1997	US 5902983 A	11-05-1999

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 12 3164

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-11-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0805424 A		AU 721733 B2	13-07-2000
		AU 1913497 A	06-11-1997
		CA 2202689 A1	29-10-1997
		EP 0805424 A2	05-11-1997
		US 6347738 B1	19-02-2002
		US 6547131 B1	15-04-2003
		ZA 9703623 A	25-11-1997
EP 0919965 A	02-06-1999	AU 755826 B2	19-12-2002
		AU 7885398 A	18-02-1999
		BR 9806530 A	13-03-2001
		CA 2238678 A1	08-02-1999
		EP 0919965 A2	02-06-1999
		JP 11114137 A	27-04-1999
		ZA 9807115 A	17-03-1999

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Electronic Acknowledgement Receipt

EFS ID:	7962702
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	06-JUL-2010
Filing Date:	21-AUG-2007
Time Stamp:	20:22:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDS3rdofJuly62010.pdf	1196022 8e4eaf3a32a14d469a91b63729cdf3d8647 1054f	yes	33

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	NPL Documents	4	9
	Foreign Reference	10	33

Warnings:

Information:

Total Files Size (in bytes):	1196022

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] j	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

	1	Office Action of 12-06-2010 in related application 11/115,888	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

□ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

□ See attached certification statement.

□ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

□ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	
Name/Print		Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Electronic Acknowledgement Receipt

EFS ID:	9193170
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	08-JAN-2011
Filing Date:	21-AUG-2007
Time Stamp:	13:38:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5805CIPIDSof01-08-2011asperOAof12062010of5806CON.pdf	878403 730673991dbc673b64c356ee81d890a44f9ad252	yes	23

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	NPL Documents	4	23
Warnings:			
Information:			
	Total Files Size (in bytes):	878403	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

NFORMATION DISCLOSURE STATEMENT BY APPLICANT

Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	3711
Examiner Name	
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

xaminer nitial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE37885	E	2002-10-15	Acres	

f you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

xaminer nitial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

f you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

xaminer nitial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

f you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

xaminer nitials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11842147
	Filing Date		2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit		3711
	Examiner Name		
	Attorney Docket Number		CYBV5805CIP

	1	Office Action of 01/04/2011 in related application 11/844,201	

f you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

xaminer Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a itation if not in conformance and not considered. Include copy of this form with next communication to applicant.

See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO tandard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent documer Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here nglish language translation is attached.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

86915 7590 06/08/2011

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

EXAMINER	
TIV, BACKHEAN	

ART UNIT	PAPER NUMBER
2451	

MAIL DATE	DELIVERY MODE
06/08/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 11/842,147	**Applicant(s)** BRUNET DE COURSSOU, THIERRY	
	Examiner BACKHEAN TIV	**Art Unit** 2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2007* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *8/21/07, 4/7/08, 11/7/08, 12/9/08, 3/20/09, 6/2/10, 7/6/10, 1/8/11, 4/1/11.*

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Detailed Action

Claims 1-41 are pending in this application.

Drawings

The Drawings filed on 8/21/07 are acceptable.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 8/21/07, 4/7/08, 11/7/08, 12/9/08, 3/20/09, 6/2/10, 7/6/10, 1/8/11, 4/1/11 has been considered.

Specification

The disclosure is objected to because of the following informalities:

The applicant is reminded to include all applications that are related to the instant application under the heading, "<u>Cross-References to Related Applications</u>" See 37 CFR 1.78 and MPEP § 201.11.

The use of the trademark IBM, Microsoft, Xbox, Sony PlayStation, Windows CE or XP, Firewire, . has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Appropriate correction is required.

Claim Objections

Claim 38 objected to because of the following informalities:

Claim 38 recites dependency on claim 354, for examination purposes, the Office will assume claim 38 depends on claim 35.

Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-41 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-41 of U.S. Patent No. 6,916,247 issued to Gatto et al(Gatto). Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant claims are anticipated by Gatto, obvious variants or are well known in the art and obvious to combine with Gatto.

Claims 1-41 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,945,870 issued to Gatto et al(Gatto). Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant claims are anticipated by Gatto, obvious variants or are well known in the art and obvious to combine with Gatto.

Claims 1-41 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-105 of U.S. Patent No. 7,297,062 issued to Gatto et al(Gatto). Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant claims are anticipated by Gatto, obvious variants or are well known in the art and obvious to combine with Gatto.

Claims 1-41 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1-75 of copending Application No. 11/844,201. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant claims are anticipated by copending application 11/844,201, obvious variants or are well known in the art and obvious to combine with co-pending application 11/844,201.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 10,14,15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 10,14,15, contains the trademark/trade name IEEE 1394 Firewire, Microsoft, IBM. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe particular bus standard, software, service oriented architecture and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 8-13, 17-22, 24-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,674,128 issued to Holch et al.(Holch) in view of US Patent 5,762,552 issued to Vuong et al.(Vuong).

As per claim 1, Holch teaches a distributed gaming system, comprising:

a communication bus(Fig.2); at least one first node, each including a first computer coupled to the communication bus(col.6, lines 21-52); at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol(col.6, lines 21-52), the first service oriented protocol being configured to negotiate service messages over the communication bus(col.6, lines 21-52), the first service oriented software being configured to selectively: publish the at least one high-level function; provide the at least one high-level function upon receiving a request to consume the at least one high-level function; enable execution of the at least one high-level function upon receiving a request for execution; perform a call back upon receiving a request to consume or execute the at least one high-level function, and return a reply subsequent to receiving a request for execution of the at least one high-level function(col.6, lines 21-52).

Holch however does not explicitly teach at least one second node, each including a second computer coupled to the communication bus, and at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively: subscribe to or consume the published or provided at least one high-level function; request that the at least one first node execute the at least one high-level function; accept the reply subsequent to receiving a reply from the at least one first node, and accept the call-back upon receiving a call-back from the at least one first node.

Vuong teaches at least one second node, each including a second computer coupled to the communication bus(Fig.1), and at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured(Fig.1, col.2, line 40-col.3, line 29), upon execution of the at least one function call, to selectively: subscribe to or consume the published or provided at least one high-level function; request that the at least one first node execute the at least one high-level function; accept the reply subsequent to receiving a reply from the at least one first node, and accept the call-back upon receiving a call-back from the at least one first node(col.4, line 63-col.5, line 35).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention to modify the teachings of Holch to include the teachings of Vuong in order to have a remote gaming system that allows remote players to place wagers in a real-time game(Vuong, col.1, lines 5-10).

One ordinary skill in the art would have been motivated to combine the teachings of Holch and Vuong in order to have a remote gaming system that allows remote players to place wagers in a real-time game(Vuong, col.1, lines 5-10).

As per claim 2, the distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call(Holch, col.6, lines 21-52, Vuong, col.4, lines 63-col.5, line 35). Motivation to combine set forth in claim 1.

As per claim 5, the distributed gaming system of claim 1, wherein the first service oriented software is configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call(Holch, col.6, lines 21-52, Vuong, col.4, lines 63-col.5, line 35). Motivation to combine set forth in claim 1.

As per claim 8, the distributed gaming system of claim 1, wherein the communication bus includes loosely coupled and/or tightly coupled nodes(Holch, col.6, lines 21-52, Vuong, Fig.1). Motivation to combine set forth in claim 1.

As per claim 9, the distributed gaming system of claim 8, wherein the loosely coupled nodes include nodes coupled via at least one of Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and satellite link(Vuong, col.5, lines 25-30). Motivation to combine set forth in claim 1.

As per claim 10, the distributed gaming system of claim 8, wherein the tightly coupled nodes include nodes coupled via at least one of inter-process communication, USB, Bluetooth, RS-232, RS-422 and IEEE1394 Firewire(Holch, col.5, lines 23).

As per claim 11, the distributed gaming system of claim 1, wherein the at least one high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and an outcome determination function(Holch, col.6, lines 31-52).

As per claim 12, the distributed gaming system of claim 1, wherein the at least one first node includes one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine(Holch, col.3, lines 25-27).

As per claim 13, the distributed gaming system of claim 1, wherein the at least one second node includes at least one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine(Vuong, Abstract). Motivation to combine set forth in claim 1.

As per claim 17, the distributed gaming system of claim 1, wherein the at least one second node includes a gaming machine(Vuong, Abstract). Motivation to combine set forth in claim 1.

As per claim 18, the distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine(Vuong, Abstract). Motivation to combine set forth in claim 1.

As per claim 19, the distributed gaming system of claim 1, wherein the at least one first node includes a gaming machine(Holch, col.3, lines 25-27).

As per claim 20, the distributed gaming system of claim 1, wherein the at least one first node is included inside a gaming machine(Holch, col.3, lines 25-27).

As per claim 21, the distributed gaming system of claim 1, wherein the at least one second node is a gaming machine played by a player and is configured to execute at least one function call during a game session(Vuong, Abstract, col.6, lines 9-29). Motivation to combine set forth in claim 1.

As per claim 22, the distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine played by a player and is configured to execute at least one function call during a game session(Vuong, Abstract, col.6, lines 9-29). Motivation to combine set forth in claim 1.

As per claim 24, the distributed gaming system of claim 1, wherein the negotiating of service messages on the communication bus include at least one of naming, discovery, message routing, publishing eventing, subscribing eventing, message transformations, workflows, and communication recovery from nodes powering-off then on again(Holch, col.6, lines 21-52, Vuong, Fig.1). Motivation to combine set forth in claim 1.

As per claims 25-41, rejected for the same reasons as set forth in claims 1, 2, 5, 8-13, 17-22, 24.

Claims 3, 4, 6, 7, 14-16, 23 rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,674,128 issued to Holch et al.(Holch) in view of US Patent 5,762,552 issued to Vuong et al.(Vuong) in view of Office Notice.

As per claims 3, Holch in view of Vuong teaches the distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function, as per claim 4, the distributed gaming system of claim 1, wherein the first service oriented software is configured to enable execution of the at least one high-level function upon receiving a request for execution, as per claim 6, the distributed gaming system of claim 1, wherein the first service oriented software is configured to return a reply subsequent to receiving a request for execution of the at least one high-level function(Holch, col.6, lines 21-52, Vuong, col.4, lines 63-col.5, line 35).

Holch in view of Vuong does not explicitly teach the use of HTTP request/replies.

Office Notice is taken; The use of HTTP request/replies is well known in the arts for use in distributed, collaborative, hypermedia information systems.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the use of HTTP request/replies with Holch to create a system for use in the World Wide Web.

As per claim 7, Holch in view of Vuong does not explicitly the distributed gaming system of claim 1, wherein the service oriented protocol is the Service Oriented Architecture Protocol (SOAP).

Office Notice is taken; SOAP is well known protocol used in the arts for exchanging structured information in the implementation of Web Services in computer networks.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the use of SOAP with Holch to create a system for easy communication over existing firewalls and proxies.

As per claim 14,15, Holch in view of Vuong does not explicitly the distributed gaming system of claim 1, wherein the first service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI.

Office Notice is taken; the software function of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Corba, SOAP, and UDDI are well known in the art for the purpose of better software efficiency.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine such software with Holch to create a system that runs smoother and is more efficient.

As per claim 16, Holch in view of Vuong does not explicitly the distributed gaming system of claim 1, wherein security over the communication bus is provided by implementation of at least one of the IPSec protocol, the VPN tunneling protocol and the SSL protocol.

Office Notice is taken; the use of IPSec protocol, VPN tunneling protocol, and SSL protocol are well known security protocol.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine security protocol with Holch to create a secure system for data communication.

As per claim 23, Holch in view of Vuong does not explicilty the distributed gaming system of claim 1, wherein the at least one first node is configured for load balancing with another one of the at least one first node.

Office Notice is taken; the art of load balancing is well known in the arts for distributing loads among devices.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the use of load balancing with Holch to create a secure system to balance loads so that one device is not overburden with request which can slow or crash the device.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in its entirety as potentially teaching of all or part of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BACKHEAN TIV whose telephone number is (571)272-5654. The examiner can normally be reached on M-T 7-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Backhean Tiv/
Examiner, Art Unit 2451

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER	
	Examiner BACKHEAN TIV	Art Unit 2451	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2001/0014881 A1	08-2001	Drummond et al.	705/43
*	B	US-RE37,885 E	10-2002	Acres et al.	463/42
*	C	US-6,595,859 B2	07-2003	Lynn, Scott W.	463/42
*	D	US-2003/0177187 A1	09-2003	Levine et al.	709/205
*	E	US-2005/0027382 A1	02-2005	Kirmse et al.	700/091
*	F	US-6,945,870 B2	09-2005	Gatto et al.	463/29
*	G	US-7,297,062 B2	11-2007	Gatto et al.	463/42
*	H	US-2008/0171601 A1	07-2008	Kirmse et al.	463/42
*	I	US-7,546,602 B2	06-2009	Hejlsberg et al.	719/313
*	J	US-5,762,552	06-1998	Vuong et al.	463/25
*	K	US-5,674,128	10-1997	Holch et al.	463/42
*	L	US-6,916,247	07-2005	Gatto et al.	463/42
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Virtual Private Network, Wikipedia, pages 1-7
	V	SOAP, Wikipedia, pages 1-4
	W	Transport Layer Security, Wikipedia, pages 1-17
	X	Load Balancing (Computing), Wikipedia, pages 1-6

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER
	Examiner BACKHEAN TIV	Art Unit 2451	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	IPsec, Wikipedia, pages 1-8
	V	Hypertext Transfer Protocol, Wikipedia, pages 1-8
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2880

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/842,147	08/21/2007 **RULE**	709	2451	CYBS5805CIP

APPLICANTS
Thierry Brunet de Courssou, Henderson, NV;

** **CONTINUING DATA** *************************
This application is a CIP of 10/120,635 04/10/2002 PAT 7,297,062
which claims benefit of 60/332,593 11/23/2001

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
08/31/2007

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed □ Yes ☑ No 35 USC 119(a-d) conditions met □ Yes ☑ No Verified and Acknowledged /BACKHEAN TIV/ Examiner's Signature	□ Met after Allowance Initials	NV	23	41	4

ADDRESS

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028
UNITED STATES

TITLE

GAME TALK SERVICE BUS

FILING FEE RECEIVED 1115	FEES: Authority has been given in Paper No.__________ to charge/credit DEPOSIT ACCOUNT No.__________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other ____________ □ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	("7297062").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:17
S2	2	("5762552").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:24
S3	10	(("5179517") or ("5674128") or ("5800269") or ("6089982") or ("6280328")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:51
S4	1	("re37885").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:07
S5	2	("5762552").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:09
S6	2	("20070191102").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:10
S7	2	("6945870").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:25
S8	3	("6,916,247").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:26

S9	6991	(463/25,42).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:53
S10	7842	(235/115,380,382).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:54
S11	220	(902/3,23).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:54
S12	1283	(340/5.8,5.82,323).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:54
S13	13372	(709/205,218,219).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:55
S14	29364	S9 or S10 or S11 or S12 or S13	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 10:57
S15	86	("20020090934" | "20020174444" | "20030037335" | "20030087683" | "20030100370" | "20030100371" | "20030171140" | "20050032577" | "20050054448" | "20050059494" | "20050113172" | "20050233811" | "20050282637" | "20060183537" | "20060270478" | "20070180371" | "20070184896" | "4335809" | "5179517" | "5667440" | "5674128" | "5759102" | "5762552" | "5800269" | "5970143" | "6048269" |	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 10:58

		"6077163" | "6089982" | "6135887" | "6142876" | "6219836" | "6251014" | "6273821" | "6280328" | "6409602" | "6463530" | "6710895" | "6732920" | "6749510" | "6908391" | "6916247" | "6921331" | "6945870").PN.				
S16	4	("6210274" | "6428413").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 10:59
S17	6	("20040185936" | "20060030383" | "20070191102").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 10:59
S18	2	("20070191102").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 10:59
S19	4	game near4 plac$4 near5 wager same protocol and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:08
S20	0	game near4 plac$4 near5 wager same (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:10
S21	90	game near4 plac$4 near5 wager and (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:10
S22	4	("20010014881" | "6219836"). PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:28

S23	161970	(HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:51
S24	6	HTTP near4 (reply or replies or request) with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:51
S25	136	SOAP with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52
S26	1	SOAP near2 protocol with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52
S27	6	SOAP near2 protocol same game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52

EAST Search History (Interference)

<This search history is empty>

5/24/2011 3:40:43 PM
C:\ Documents and Settings\ btiv\ My Documents\ EAST\ Workspaces \ 11842147_game_communication_different_protocol.wsp

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~2711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] j	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

	1	Office Action of 12-06-2010 in related application 11/115,888	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147	11842147 - GAU: 2451
	Filing Date	2007-08-21	
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit	~~3711~~ 2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBV5805CIP	

	1	EP Examination Report of February 18, 2009 in related application EP 02 780 726.2	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3711~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	RE37885	E	2002-10-15	Acres	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 j	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11842147	
	Filing Date	2007-08-21	
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit	~~3711~~ 2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBV5805CIP	

	1	Office Action of 01/04/2011 in related application 11/844,201

f you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

xaminer Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a itation if not in conformance and not considered. Include copy of this form with next communication to applicant.

See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent documer Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11184214
	Filing Date	2007-08-20
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6210274		2001-04-03	Carlson	
	2	6428413		2002-08-06	Carlson	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□
If you wish to add additional Foreign Patent Document citation information please click the Add button								
NON-PATENT LITERATURE DOCUMENTS								

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11184214 11842147 - GAU: 2451
	Filing Date	2007-08-20
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451
PTO/SB/08a (08-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070191102	A1	2007-08-16	Coliz et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number³	Country Code² i	Kind Code⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T⁵
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T⁵

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147 11842147 - GAU: 2451
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3711~~ 2451
Examiner Name	Tiv, B
Attorney Docket Number	CYBV5805CIP

	1	international Preliminary Examination Report of March 4, 2010 in related PCT application PCT/US2008/073559	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147 11842147 - GAU: 2451
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	3711
	Examiner Name	
	Attorney Docket Number	CYBV5805CIP

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ alan young /	Date (YYYY-MM-DD)	2010-06-02
Name/Print	Alan W. YOUNG	Registration Number	37970

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3711~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010014881	A1	2001-08-16	Drummond Jay Paul	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number³	Country Code² i	Kind Code⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T⁵
	1	00/54214	WO	A1	2000-09-14	Bionetrix Systems Corp		□
	2	98/08581	WO	A1	1998-03-05	Barcelou David M		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147 11842147 - GAU: 2451	
	Filing Date	2007-08-21	
	First Named Inventor	Thierry BRUNET DE COURSSOU	
	Art Unit	~~3711~~ 2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBV5805CIP	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Communication pursuant to Article 94(3) EPC of April 9, 2010 in related EP application 02789831.1	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

PTO/SB/08a (08-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3714~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010014881	A1	2001-08-16	Drummond Jay Paul	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1	00/54214	WO	A1	2000-09-14	Bionetrix Systems Corp		□
	2	98/08581	WO	A1	1998-03-05	Barcelou David M		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147 11842147 - GAU: 2451
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3714~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Communication pursuant to Article 94(3) EPC of April 9, 2010 in related EP application 02789831.1	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451

PTO/SB/08a (09-07)

Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3744~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6219836	B2	2001-04-17	B. Wells et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147 11842147 - GAU: 2451
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

	1	Communication pursuant to Article 94(3) EPC of April 6, 2010 in related EP application 02780726.2	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451

PTO/SB/08a (03-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~3711~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147 11842147 - GAU: 2451
Filing Date	2007-08-21
First Named Inventor	Thierry BRUNET DE COURSSOU
Art Unit	~~2711~~ 2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBV5805CIP

	1	Communication pursuant to Article 94(3) EPC of April 6, 2010 in related EP application 02784552.8	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99**)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4335809	A	1982-06-22	J. L. Wain	
	2	5667440	A	1997-09-16	Sasaki et al.	
	3	6135887	A	2000-10-24	L. L. Pease	
	4	6219836	B1	2001-04-17	B. Wells et al.	
	5	6251014	B1	2001-06-26	J. Stockdale et al.	
	6	6273821	B1	2001-08-14	Moriguchi	
	7	6077163		2000-06-20	Walker et al.	
	8	6749510		2004-06-15	Giobbi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147	11842147 - GAU: 2451
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit	2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBS5805CIP	

	9	6280328		2001-08-28	Holch et al.	
	10	6089982		2000-07-18	Holch et al.	
	11	5800269		1998-09-01	Holch et al.	
	12	5674128		1997-10-07	Holch et al.	
	13	5179517		1993-01-12	Sarbin et al.	
	14	6916247	B2	2005-07-12	Gatto et al.	
	15	5759102	A	1998-06-02	Pease et al.	
	16	5762552	A	1998-06-09	Vuong et al.	
	17	5970143	A	1999-10-19	Schneier et al.	
	18	6048269	A	2000-04-11	Burns et al.	
	19	6908391	B2	2005-06-21	Gatto et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147	11842147 - GAU: 2451
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit	2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBS5805CIP	

	20	6463530	B1	2002-10-08	Sposato	
	21	6945870	B2	2005-09-20	Gatto et al.	
	22	6142876	A	2000-11-07	Cumbers	
	23	6710895	B1	2004-03-23	Gatto et al.	
	24	6732920	B2	2004-05-11	Gatto et al.	
	25	6921331	B2	2005-07-26	Gatto et al.	
	26	6409602		2002-06-25	Wiltshire et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020137217	A1	2002-09-26	R. E. Rowe	
	2	20020147040	A1	2002-10-10	Walker et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	11842147 11842147 - GAU: 2451
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBS5805CIP

	3	20020174444	A1	2002-11-21	Gatto et al.	
	4	20030037335	A1	2003-02-20	Gatto et al.	
	5	20020090934	A1	2002-07-11	Eliott R.D. Mitchelmore	
	6	20030087683	A1	2003-05-08	Gatto et al.	
	7	20030100369	A1	2003-05-29	Gatto et al.	
	8	20030100370	A1	2003-05-29	Gatto et al.	
	9	20030100371	A1	2003-05-29	Gatto et al.	
	10	20030100372	A1	2003-05-29	Gatto et al.	
	11	20030171140	A1	2003-09-11	Gatto et al.	
	12	20050032577	A1	2005-02-10	Christopher W. Blackburn et al.	
	13	20050054448	A1	2005-03-10	Gary Frerking et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147	11842147 - GAU: 2451
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit	2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBS5805CIP	

	14	20050059494	A1	2005-03-17	Keith Donald Kammler	
	15	20050113172	A1	2005-05-26	Xiaoqiang D. Gong	
	16	20050233811	A1	2005-10-20	Gatto et al.	
	17	20050282637	A1	2005-12-22	Gatto et al.	
	18	20060183537	A1	2006-08-17	Scott Dickerson	
	19	20060270478	A1	2006-11-30	William J. Barhydt et al.	
	20	20070180371	A1	2007-08-02	Keith Donald Kammler	
	21	20070184896	A1	2007-08-09	Scott Dickerson	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1	1004970	EP	A2	2000-05-31	International Game Technology		□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11842147 11842147 - GAU: 2451
	Filing Date	2007-08-20
	First Named Inventor	Thierry Brunet de Courssou
	Art Unit	2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBS5805CIP

	2	1004970	EP	A3	2000-05-31	International Game Technology		□
	3	1074955	EP	A2	2001-02-07	Maygay Machines Limited		□
	4	1074955	EP	A3	2001-02-07	Maygay Machines Limited		□
	5	1231577	EP	A2	2001-11-09	WMS Gaming Inc.		□
	6	1231577	EP	A3	2001-11-09	WMS Gaming Inc.		□
	7	19941504	DE	A1	2001-03-01	Internet Special Services		□
	8	1120757	EP	A2	2001-08-01	International Game Technoology		□
	9	1120757	EP	A3	2001-08-01	International Game Technoology		□
	10	1087323	EP	A1	2001-03-28	Nokia Corporation		□
	11	0182176	WO	A	2001-11-01	Gaming System Technologies		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147	11842147 - GAU: 2451
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit	2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBS5805CIP	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	0141892	WO	A2	2001-06-14	Smart Card Integrators, Inc.		□
	2	0141892	WO	A3	2001-06-14	Smart Card Integrators, Inc.		□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

11842147 - GAU: 2451

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(**Not for submission under 37 CFR 1.99)**

Application Number	11842147
Filing Date	2007-08-20
First Named Inventor	Thierry Brunet de Courssou
Art Unit	2451
Examiner Name	Tiv, B.
Attorney Docket Number	CYBS5805CIP

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Supplemental European Search Report mailed November 28, 2006, in related European Application No. 02784522.	□
	2	Supplemental European Search Report mailed November 16, 2006, in corresponding European Application No. 02780726.	□
	3	Supplemental European Search Report mailed December 4, 2006, in related European Application No. 02789831.	□
	4	European Search Report mailed November 24, 2006, in related European Application No. 02782356.6	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	Thierry Brunet de Courssou
	Art Unit	2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11842147 11842147 - GAU: 2451	
	Filing Date	2007-08-20	
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit	2451	
	Examiner Name	Tiv, B.	
	Attorney Docket Number	CYBS5805CIP	

	1	W3C, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) W3C Recommendation 27 April 2007"; http://www.w3.org/TR/REC-soap12-part1-20070427/.	□
	2	BizTalk Labs, "BizTalk Services and Internet Service Bus Technologies."	□
	3	BizTalk Labs, "BizTalk Connectivity Serices."	□
	4	Object Management Group, "CORBA BASICS."	□
	5	Wilkipedia, "RSS."	□
	6	Microsoft Corporation, msdn, "What is Windows Communication Foundation?" 2007.	□
	7	XML-RPC.Com, "simple cross-platform distributed computing, based on the standards of the Internet. XML-RPC Specification."	□
	8	International Search Report mailed February 26, 2003, in related International Application No. PCT/US02/37537, filed November 22, 2002.	□
	9	Written Opinion mailed August 28, 2003, in related International Application No. PCT/US02/37537, filed November 22, 2002.	□
	10	International Preliminary Examination Report mailed February17, 2004, in related International Application No. PCT/ US02/37537, filed November 22, 2002.	□
	11	International Search Report mailed February 25, 2003, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11842147
	Filing Date		2007-08-20
	First Named Inventor	Thierry Brunet de Courssou	
	Art Unit		2451
	Examiner Name	Tiv, B.	
	Attorney Docket Number		CYBS5805CIP

	12	Written Opinion mailed September 4, 2003, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□
	13	International Preliminary Examination Report mailed February 11, 2004, in related International Application No. PCT/US02/37536, filed November 22, 2002.	□
	14	International Search Report mailed January 30, 2003, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	15	Written Opinion mailed August 27, 2003, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	16	International Preliminary Examination Report mailed August 12, 2004, in related International Application No. PCT/US02/37528, filed November 22, 2002.	□
	17	International Search Report mailed February 28, 2003, in related International Application No. PCT/US02/37538, filed November 22, 2002.	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

PTO/SB/08a (05-07)
Approved for use through 09/30/2007 OMB 0651-0031
U S Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 j	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11842147
	Filing Date	2007-08-21
	First Named Inventor	Thierry BRUNET DE COURSSOU
	Art Unit	~~3714~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBV5805CIP

	1	Canadian Office Action of Sep. 30, 2008 in related Canadian patent application 2,468,026 (Attorney Docket CYBV5805CA).	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST 3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U S Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	BRUNET de COURSSOU, Thierry
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBS5805CIP

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070191102	A1	2007-08-16	Coliz et al.	
	2	20060030383	A1	2006-02-09	Rosenberg et al.	
	3	20040185936	A1	2004-09-23	Block et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number	11842147
	Filing Date	2007-08-20
	First Named Inventor	BRUNET de COURSSOU, Thierry
	Art Unit	~~3711~~ 2451
	Examiner Name	Tiv, B.
	Attorney Docket Number	CYBS5805CIP

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Notification of Transmittal of the International Search Report And the Written Opinion of the International Searching Authority, Or the Declaration in corresponding PCT application PCT/US08/73559, mailed 05 Dec. 2008.	□

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Backhean Tiv/ (05/24/2011)	Date Considered	05/24/2011

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BT/

Search Notes	Application/Control No. 11842147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

SEARCHED

Class	Subclass	Date	Examiner
463	25,42	5/24/11	BT
235	115, 380, 382	5/24/11	BT
902	3,23	5/24/11	BT
340	5.8, 5.82, 323	5/24/11	BT
709	205, 218, 219	5/24/11	BT

SEARCH NOTES

Search Notes	Date	Examiner
INVENTOR'S NAME SEARCH PALM	5/24/11	BT
EAST TXT SEARCH	5/24/11	BT
NPL SEARCH (GOOGLE, WIKIPEDIA)	5/24/11	BT

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/BACKHEAN TIV/ Examiner.Art Unit 2451	

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	05/24/2011								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	05/24/2011								
	36	✓								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

86915 7590 09/20/2011

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

EXAMINER	
TIV, BACKHEAN	
ART UNIT	PAPER NUMBER
2451	
MAIL DATE	DELIVERY MODE
09/20/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Applicant-Initiated Interview Summary	**Application No.** 11/842,147	**Applicant(s)** BRUNET DE COURSSOU, THIERRY	
	Examiner BACKHEAN TIV	**Art Unit** 2451	

All participants (applicant, applicant's representative, PTO personnel):

(1) BACKHEAN TIV.

(3) Alan Young(37,970).

(2) _____.

(4) _____.

Date of Interview: 15 September 2011.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Holch, Vuong.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The applicant describes the invention as a distributed gaming system where, there are multiple nodes/gaming systems that publishes network services, e.g.high level function, advertisements, etc, and a second node subscribes to the high level function, e.g advertisements, and when there are changes to the advertisements, it is sent to all the nodes that subscribed to that high level function, it appears to overcome the prior art and deemed allowable.
.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Backhean Tiv/
Examiner, Art Unit 2451

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:	)	Examiner: TIV, Backhean
	)	
Thierry Brunet de Courssou	)	Art Unit: 2451
	)	
Serial No.: 11/842,147	)	Confirmation No.: 2880
	)	
Filed: Aug. 21, 2007	)	Customer No.: 22430
	)	
For: **GAME TALK SERVICE BUS**	)	
	)	
Atty. Docket No.: CYBS5805CIP	)	**AMENDMENT**
AP00060-023	)	

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Responsive to the Office Action of **June 08, 2011**, please amend the above-identified application as follows:

Amendments to the Specification begin on page **2** of this paper;

Amendments to the **Claims** begin at page **18** of this paper, and

The **Remarks** begin at page **27** of this paper.

REMARKS

At the outset, the undersigned wishes to thank Exr. Tiv for his time and courtesy during the recent telephone interview of September 15, 2011. As agreed during the interview, independent claim 1 and its dependent claims are allowable.

The present amendment is responsive to the Office Action of June 08, 2011 and is filed concurrently with the fee for a one-month extension of time.

The Specification was objected to for a number of informalities. Claim 38 was objected to for a typographical error in the indication of dependency. The claims were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-41 of US patent 6,916,247, claims 1-45 of US patent 6,945,870 and claims 1-105 of US patent 7,297,062 and provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claims 1-75 of copending application 11/844,201. Claims 10, 14, 15 were rejected as being indefinite under 35 USC §112(2). Claims 1, 2, 5, 8-13, 17-22 and 24-41 were rejected as being unpatentable under 35 USC §103(a) over Holch et al. in view of Vuong et al. Claims 3, 4, 6, 7, 14-16 and 23 were rejected as being unpatentable under 35 USC §103(a) over Holch et al., Vuong et al. and Official Notice.

The Specification has been amended as requested.

The dependency of claim 38 has been suitably amended.

Terminal Disclaimers are filed herewith relative to patents 6,916,247, 6,945,870 and 7,297,062. The filing of a Terminal Disclaimer over pending US application 11/844,201 is held in abeyance until such time as the application issues and the final form and scope of the claims can be determined.

Claims 10, 14, 15 were rejected under 35 USC §112(2) as being indefinite. Claims 10, 14 and 15 are canceled herewith. Reconsideration and withdrawal of these rejections are respectfully requested.

Claims 1, 2, 5, 8-13, 17-22 and 24-41 were rejected as being unpatentable under 35 USC §103(a) over Holch et al. in view of Vuong et al. Reconsideration and withdrawal of these rejections are respectfully requested.

The Office, at page 7 of the outstanding Office Action, states that Holch et al., at Col. 6, lines 21-52, teaches:

> **a communication bus;**
>
> **at least one first node, each including a first computer coupled to the communication bus;**
>
> **at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:**
>
> **publish the at least one high-level function;**
>
> **provide the at least one high-level function upon receiving a request to consume the at least one high-level function;**
>
> **enable execution of the at least one high-level function upon receiving a request for execution;**
>
> **perform a call back upon receiving a request to consume or execute the at least one high-level function, and**
>
> **return a reply subsequent to receiving a request for execution of the at least one high-level function;**

The office maintains that remainder of the claim; namely…

> **at least one second node, each including a second computer coupled to the communication bus, and**

> **at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively:**
>
> **subscribe to or consume the published or provided at least one high-level function;**
>
> **request that the at least one first node execute the at least one high-level function;**
>
> **accept the reply subsequent to receiving a reply from the at least one first node, and**
>
> **accept the call-back upon receiving a call-back from the at least one first node.**

… is taught by Vuong et al.

The passage of Holch at Col. 6 of Holch et al. from line 21 to line 52 is sufficiently short so as to be reproduced herein below in its entirety:

> **Referring to FIG. 5a, after opening a player account and obtaining a player I.D. card, a player logs onto a player terminal 100 by inserting the I.D. card into the magnetic card reader 206 (step 500). Alternatively, the system does not require player I.D. cards, so the player simply enters his/her assigned player account number using keypad 208. The player terminal 100, which has been executing attract mode graphics, reads the information from the I.D. card, displays the player's name (step 502), sends the player account number to the account server 400, and requests the account server 400 to verify the player's account number. Account server 400 receives the account number and, referring to the account file database 404, determines whether the player account number is valid (step 504). If not, player terminal 100 informs the player and either requests the player to reenter the account number or terminates the session (step 506).**
>
> **If account server 400 determines that the account number is valid, player terminal 100 requests the player to enter his/her PIN (step 508). Player terminal 100 preferably encrypts the PIN and forwards the encrypted PIN to the account server 400 (step 510). Account server 400 receives the PIN and determines whether the PIN is valid and corresponds to the player's account number (step 512). If the PIN is not valid or does not correspond to the player's account number, player terminal 100 either requests the player reenter the PIN, or terminates the session (step 514). If the PIN is valid, player terminal 100 displays a graphical selection of video games on video display 212 (step 516). As described, the video games may include keno, lotto, bingo, etc.**

This passage tells us that a player logs on by inserting his or her ID card in a magnetic card reader or provides an account number. The account number, whether obtained from the ID card or otherwise provided by the player, is sent to the account server where it is authenticated. If the account number is not authentic, the session is terminated or the player is requested to re-enter the account number. If the account number is valid, the account server requests the player's PIN, which is encrypted and sent to the account server. If the PIN is valid and corresponds to the account number, the gaming machine displays a selection of video games on the display. If the PIN is determined to be invalid, the player is requested to re-enter the PIN or the session is terminated.

Therefore, this passage details how the account server requests the player's account number and PIN and causes the gaming machine to display a selection of video games if both are valid and correspond to one another or terminates the session if not.

Claim 1 recites:

> **a communication bus;**
>
> **at least one first node, each including a first computer coupled to the communication bus;**
>
> **at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:**
>
> **publish the at least one high-level function;**
>
> **provide the at least one high-level function upon receiving a request to consume the at least one high-level function;**
>
> **enable execution of the at least one high-level function upon receiving a request for execution;**
>
> **perform a call back upon receiving a request to consume or execute the at least one high-level function, and**
>
> **return a reply subsequent to receiving a request for execution of the at least one high-level function;**

The Office has not identified any service oriented software executing in the first computer of the first node, and much less any service oriented software that is configured to selectively

- publish the at least one high-level function;
- provide the at least one high-level function upon receiving a request to consume the at least one high-level function;
- enable execution of the at least one high-level function upon receiving a request for execution;
- perform a call back upon receiving a request to consume or execute the at least one high-level function, and/or
- return a reply subsequent to receiving a request for execution of the at least one high-level function

as claimed herein. The Office has only pointed to a process whereby an account server requests the player's account number and PIN and causes the gaming machine to display a selection of video games if both are valid and correspond to one another or terminates the session if not.

The claimed <u>network service oriented software</u> is described, for example, beginning at paragraph **[0076]** of the specification of the present application:

> **[0076] ...A more modern control model is object-oriented, whereby a module may offer network services for consumption by other modules. Widely used standards for such object-oriented models include, for example, Distributed Common Object Module ("DCOM", developed by Microsoft Corporation) and Simple Object Access Protocol "SOAP", a**

> **vendor independent protocol based on eXtensible Markup Language ("XML").**

Paragraphs [0102] and [0103] define the terms "network services", the meaning of consuming services and providing services, as such terms and functionalities are recited in the claims:

> **[0102] Network Services deliver loose coupling services between service requestors and service providers. *Service requestors* "consume" services provided by *services providers*. Publication of service descriptions play a central role to enable service requestors to discover available services and bind to them. The service descriptions allow service requestors to bind to the service provider. The service requestor obtains service descriptions through a variety of techniques, from the simple "e-mail me the service description" approach to techniques such as Microsoft DISCO and sophisticated service registries like UDDI.**
>
> **[0103] Network services offer a network distributed objects/services infrastructure for transparent activations and accessing of remote objects/services. Objects are typically the EGD's peripherals such as a note acceptor, and the services are the functions performed by the peripheral that are accessible externally via the IP network such as the value of the banknote entered. The central server is typically a service requestor. Peripherals are commonly service providers as well as service requestors (consuming services provided by the central server). In the same way, the central server is a services requestor and a services provider.**

Holch et al. simply does not teach or suggest any such network service-oriented software, as claimed herein.

Holch et al., moreover, does not teach or suggest any publishing function, and much less any publishing function by a network service oriented software, as recited in independent claim 1. The publishing function carried out by the claimed first node is described in the specification at paragraph [0088]:

> **[0088] ... the term publishing a service (or services) encompasses within its scope the functionality of providing a service (or services), and the term subscribing to a service (or services) encompasses within its scope the functionality of consuming or invoking a service (or services). The binding term is associated with the capability for allowing the publisher/provider to perform an asynchronous callback to the**

> **subscriber/consumer when a subscribed service (or services) is/are available (data update for example). The term publishing a service (or services) includes within its scope the functionality of exposing a service (or services).**

The publish-subscribe functions of the claimed first and second nodes are described in paragraphs [0121] to [0126] and shown in Figs. 21-25. The Holch et al. reference does not disclose any publishing or subscribing function at all.

The Office contends that the second half of independent claim 1, drawn to the second node, is disclosed in Vuong et al. – particularly from Col. 4, line 63 to Col. 5, line 35. This passage is reproduced below:

> **Referring to the drawings more particularly by reference numbers, FIG. 1 shows a preferred embodiment of an interactive network system 10 of the present invention providing remote real-time interactive gambling. Interactive network system 10 comprises a first plurality of gaming tables 12 and a second plurality of gaming machines 14 coupled by a network system 16. In the preferred embodiment, casino board games, such as craps, roulette or baccarat, are conducted by a casino employee at gaming tables 12 within the confines of an established casino. Gaming machines 14 are electronic systems through which a player can, in real-time, play one of the board games at one of the gaming tables 12 from a remote location. Network system 16 comprises at least one computer means that performs network management functions and transmission means which are more particularly described below. In one preferred embodiment, gaming machines 14 and network system 16 are located in the premise of a casino substantially proximate to gaming tables 12 such as on a balcony above the casino gaming area where gaming tables 12 are located. In this manner a player using one of the gaming machines 14 has an expansive view of the gambling area while their gaming machine 14 provides a close-up view of the action at the selected one of gaming tables 12. Alternatively, gaming machines 14 are positioned in clusters adjacent to several gaming tables 12. In another preferred embodiment, gaming machines 15, a modified version of gaming machine 14, are located at a remote site outside of the casino.**
>
> **The interactive network system 10 is expandable in a hiearcheal manner. For example, interactive network system 10 may be coupled to a second interactive network system 18 by satellite, ISDN, telephone or cable transmission networks 20 for video and audio feeds and for digital communications. Network manager 40 provides the gateway to the second interactive network system 18. Digital communication transmissions between interactive networks 10 and 18 and between network manager 40, gaming table 12 and gaming machines 14 are preferably encrypted for security purposes using commercially available or proprietary encryption algorithms.**

This passage describes the available games, unspecified "network management functions", the location of the gaming tables and machines and describes, in a general manner, the communication means used by the interactive network system 10 (satellite, ISDN, telephone or cable). This passage also discloses that the network manager provides a gateway to a second system 18. The communications between the network manager and the gaming machines are encrypted. There is no publication or subscription functionality taught or suggested by Vuong et al. whether considered alone or in combination with the primary reference to Holch et al. It is respectfully submitted, therefore, that Vuong et al. does not teach or suggest what the Office asserts that it does and does not teach or suggest the claimed subject matter.

Additionally, Holch et al. does not teach or suggest (and the Office has not pointed to any passage in Holch et al. teaching such) to provide, execute or reply to a high-level function upon receiving a request to consume or execute the same, respectively. Holch et al. also does not teach or suggest performing a call back upon receiving a request to consume or execute a high-level function, nor has the Office pointed to any portion of the Holch et al. disclosure that teaches or suggest performing the claimed call back upon receiving a request to consume or execute a high-level function, as recited by the claim. The secondary reference to Vuong et al. does not remedy the shortcomings of the Holch et al. reference, as such functionality is neither taught nor suggested therein, even when the two references are considered in combination for all they would have taught or suggested to one of ordinary skill in the art at the time of the invention.

The Office has not pointed to any specific passages, teachings or suggestions in either of the applied references that would support a *prima facie* case of obviousness. Indeed, the Office has not pointed to any teaching or suggested in the applied combination of a first service oriented software being configured to selectively:

- publish the at least one high-level function;
- provide the at least one high-level function upon receiving a request to consume the at least one high-level function;
- enable execution of the at least one high-level function upon receiving a request for execution;
- perform a call back upon receiving a request to consume or execute the at least one high-level function, and
- return a reply subsequent to receiving a request for execution of the at least one high-level function.

... as recited in claim 1.

The Office has also not pointed to any teaching or suggested in the applied combination of a second service oriented software being configured, upon execution of the at least one function call, being configured to selectively:

- subscribe to or consume the published or provided at least one high-level function;
- request that the at least one first node execute the at least one high-level function;
- accept the reply subsequent to receiving a reply from the at least one first node, and
- accept the call-back upon receiving a call-back from the at least one first node.

... as also recited in independent claim 1. Failing such, it is respectfully submitted that reconsideration and withdrawal of the 35 USC §103(a) rejections applied to independent claim 1 and its dependent claims are warranted.

On page 11 of the outstanding Office Action, independent claims 25, 28 and 35 were rejected "for the same reasons as set forth in claims 1, 2, 5, 8-13, 17-22, 24".

Independent claim 25 recites:

> **a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and**
>
> **a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.**

As detailed above, the Holch et al. and Vuong et al. references, whether considered singly or in combination, do not teach or suggest any gaming machine that is configured to publish, execute or provide any high-level functions, nor any gaming machine configured to selectively subscribe to or consume any high-level function published or otherwise provided by the first gaming machine and/or selectively request that the first gaming machine execute anything – and much less a high-level function, as recited in independent claim 25. Indeed, there does not appear to be any teaching or suggestion in Holch that the game terminals communicate with anything other than the game server 102. Likewise, there does not appear to be any teaching or suggestion in Vuong et al. of the gaming machines communicating to or with anything other than the network managers 40.

It is, therefore, respectfully submitted that the 35 USC §103(a) rejections of claim 25 and its dependent claims should be reconsidered and withdrawn. The same is, therefore, respectfully requested.

Independent claim 28 recites:

> ...
>
> **publishing, by the first gaming machine, a first high-level function over the communication bus;**
>
> **providing a node coupled to the communication bus;**

> **receiving, from the node, a request to subscribe to the published first high-level function;**
>
> **accepting the subscription request;**
>
> **initiating a gaming session on the first gaming machine, and**
>
> **responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus.**

Again, there is no teaching or suggestion in the applied combination of references of any steps of publishing or subscribing, by any gaming machine, for any purpose. Moreover, there is no teaching or suggestion of the applied combination of any gaming machine accepting a request to subscribe to anything, and much less a second gaming machine accepting a request to subscribe to a high-level function published by a first gaming machine, as recited in independent claim 28.

It is, therefore, respectfully submitted that the 35 USC §103(a) rejections of claim 28 and its dependent claims should be reconsidered and withdrawn. The same is, therefore, respectfully requested.

Lastly, independent claim 35 recites:

> **providing a first node and coupling the first node to the communication bus;**
>
> **publishing, by the first node, a high-level function over the communication bus;**
>
> **providing a first gaming machine coupled to the communication bus;**
>
> **receiving, from the first gaming machine, a request to subscribe to the published high-level function;**
>
> **accepting the subscription request;**
>
> **initiating a gaming session on the first gaming machine, and**
>
> **responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus.**

It is respectfully submitted that the Holch et al. – Vuong et al. combination does not teach or suggest the recited steps of independent claim 35. Indeed, the applied combination does not teach or suggest, as detailed above, any gaming machine receiving or accepting a request to subscribe to a published high-level function, as claimed herein. Also, the Office has not pointed out where, in either of the two applied references or the combination as a whole, call-backs are taught or suggested, which call-backs being configured to <u>return a result of an execution of a high-level function to a first gaming machine</u>. Again, it is respectfully submitted that the Office has failed to make the requisite *prima facie* case of obviousness. Reconsideration and withdrawal of the 35 USC §103(a) rejections applied to the claims are, therefore, respectfully requested.

In view of the above-remarks, it is respectfully submitted that claims 3, 4, 6, 7, 16 and 23, rejected over the combination applied above and further in view of Official Notice, are allowable at least by virtue of their dependency upon their respective independent claims, each of which has been distinguished over the Holch et al. – Vuong et al. combination applied thereto.

Reconsideration and withdrawal of the 35 USC §103(a) rejections applied to the claims are, therefore, respectfully requested.

Applicants' attorney believes that the present application is now in condition for allowance. If any unresolved issues remain, the Examiner is respectfully invited to contact the undersigned attorney of record at the telephone number indicated below, and whatever is required will be done at once.

Respectfully submitted,

Date: October 3, 2011 By:______________________________

Alan W. Young
Attorney for Applicants
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

E:\YLF\CLIENTS\CYBS\5805\CIP\5805CIP AMDT RESP TO OA OF 06-08-2011.doc

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) CYBS5805CIP

In re Application of: Thierry BRUNET DE COURSSOU

Application No.: 11/842,147

Filed: Aug. 21, 2007

For: GAME TALK SERVICE BUS

The owner*, MUDALLA TECHNOLOGY, INC., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 6,945,870 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:
expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 37,970

/ alan young / — Signature
Otober 3, 2011 — Date

Alan W. YOUNG
Typed or printed name

650-851-7210
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	11842147
Filing Date:	21-Aug-2007
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Filer:	Alan W. Young
Attorney Docket Number:	CYBS5805CIP

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	150	150

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory or terminal disclaimer	1814	3	160	480
	Total in USD ($)			**630**

Electronic Acknowledgement Receipt

EFS ID:	11102248
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Alan W. Young
Filer Authorized By:	
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	03-OCT-2011
Filing Date:	21-AUG-2007
Time Stamp:	17:49:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$630
RAM confirmation Number	4259
Deposit Account	503159
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		5805CIPAMDTRESPTOOAOF06-08-2011.pdf	13547960 2283a20f7b338b8842695b589fa9d57af7f198b1	yes	42

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	17
Claims	18	26
Applicant Arguments/Remarks Made in an Amendment	27	39
Terminal Disclaimer Filed	40	40
Terminal Disclaimer Filed	41	41
Terminal Disclaimer Filed	42	42

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	32014 cbfb3052ede54ba8535657cb87ed4852f37aa341	no	2

Warnings:

Information:

Total Files Size (in bytes):	13579974

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/26 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) CYBS5805CIP

In re Application of: Thierry BRUNET DE COURSSOU

Application No.: 11/842,147

Filed: Aug. 21, 2007

For: GAME TALK SERVICE BUS

The owner*, MUDALLA TECHNOLOGY, INC, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,297,062 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 37,970

/ alan young /
Signature

October 03, 2011
Date

Alan W. YOUNG
Typed or printed name

650-851-7210
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/26 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) CYBS5805CIP

In re Application of: Thierry BRUNET DE COURSSOU

Application No.: 11/842,147

Filed: Aug. 21, 2007

For: GAME TALK SERVICE BUS

The owner*, MUDALLA TECHNOLOGY, INC., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 6,916,247 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. □ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 37,970

/ alan young /
Signature

October 3, 2011
Date

Alan W. YOUNG
Typed or printed name

650-851-7210
Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/842,147	Filing Date 08/21/2007	□ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**10/03/2011**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 38	Minus	** 41	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	**0**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DEBORAH NASH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE SPECIFICATION

Please amend paragraph [0001] as follows:

[0001] This is a continuation-in part of application Serial No. 10/120,635, filed April 10, 2002, which claims the benefit under 35 U.S.C. §119(e) of provisional application Serial No. 60/332,593, filed November 23, 2001, both applications of which are hereby incorporated herein by reference in their entireties. **This application is also related in subject matter to commonly assigned US patents 6,916,247, 6,945,870 and 7,297,062 and to commonly assigned US pending application 11/844,201 filed Aug. 23, 2007.**

Please amend paragraph [0012] as follows:

[0012] The service oriented protocol is the Service Oriented Architecture Protocol (SOAP), for example. The communication bus may include loosely coupled and/or tightly coupled nodes. The loosely coupled nodes may include nodes coupled via Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and/or satellite link, for example. The tightly coupled nodes may include nodes coupled via inter-process communication, USB, Bluetooth, RS-232, RS-422 and/or IEEE1394 ~~Firewire~~ **FIREWIRE** **connection protocols**, for example. The at least one high-level function may include a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and/or an outcome determination function, to name but a few of the possible high-level functions. The at least one first node may include a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and/or an automatic teller machine, for example.

Please amend paragraph [0013] as follows:

[0013] The at least one second node may include, for example, a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and/or an automatic teller machine. The first and/or second service oriented protocol may include asynchronous notification of events, COM+, DCOM, ~~Microsoft Remoting~~ **MICROSOFT REMOTING**, ~~Microsoft~~ **MICROSOFT** .NET, ~~Corba~~ **CORBA**, SOAP, IBM SOA and/or UDDI **protocols**, for example. Security over the communication bus may be provided by implementing the IPSec protocol, the VPN tunneling protocol and/or the SSL protocol, for example.

Please amend paragraph [0050] as follows:

[0050] Figure 2 illustrates a gaming and identification verification machine 200 that accepts and redeems cash. It is to be understood that the gaming machine 200 is but one possible implementation of such gaming machines and that embodiments of the present invention are not limited thereto. Indeed, the system 100 may include any mix of any gaming and/or entertainment machines of most any kind. The gaming and identification verification machine 200 may include a display 202, a coin acceptor 204, a banknote acceptor 206, a coin hopper 210, a gaming machine identification (hereafter, "ID") device 212 and a plurality of user interaction means 208, which may include buttons, trackballs and/or joysticks, for example. The gaming machine ID device 212 is commonly used for identifying players that subscribe to a loyalty program to benefit from advantages and promotions offered by the gaming operator. Figure 3 illustrates an exemplary cash-less gaming machine 300 that does not accept or redeem cash. It is to be understood that the gaming machine 300 is but one possible implementation of such a cashless gaming machine and embodiments of the present invention are not limited thereto. For cash-less operation, a gaming device ID device(s) 304, 306 is/are necessary. The gaming machine ID device 304, 306 may include a magnetic card reader, a SmartCard reader and writer, a barcode reader, a ticket printer, a biometric reader, a touch-screen, keyboard or keypad to enable players to enter a PIN (Personal Identification Number) and/or a "Pay" button. The gaming machine identification device 304, 306 may further include an ID token reader to read other forms of advanced ID devices such as ID buttons, ID key-chains (such as disclosed, for example in commonly assigned US design patent entitled "Personal Communicator and Secure ID Device" patent number D441,765 issued on May 8, 2001) as well as secure communication means for securely communicating with, for example, personal wallets, hand held PCs or computer wrist-watch via infra red, magnetic field, capacitive charges or RF (~~**Bluetooth**~~ **BLUETOOTH**, IEEE 802.11 **communication protocols**, etc.) for player identification purposes. According to one embodiment of the present invention, a player initially establishes a player account with the central server(s) 112 and receives a player ID card or ID token bearing the player's account number and other relevant information. Alternatively, gaming machine 200, 300, may include a printer 314 (Figure 3) to provide the player with a printed ticket 312 including a human and/or a machine-readable ID code. Alternatively, the printed ticket 312 may be provided by the PVU 500, 600 or 700 and read by the gaming machine 200, 300 via a ticket reader 316. Alternatively still, the player may register a biometric feature such as fingerprint, voiceprint and/or face print, and a PIN to be entered whenever confirmation of identity is required. All of these ID devices may allow the player to remain anonymous; in that case, the player's personal information is not requested and the assigned or chosen ID is associated with a numbered account instead of a personal account. Wager debits and prize credits are controlled by the central server(s) 112. Players may redeem any account balance by pressing the "Pay Button" (which may halt the current gaming session) and by claiming the funds from a cashier that is connected with the central server(s) 112. A machine coded (e.g., bar coded) printed ticket 312 may be generated by the gaming machine 200, 300 as additional means for claiming the funds or to begin a new game session on another gaming machine 200, 300 by causing the ticket reader 316 of the other gaming machine 200, 300 to scan the machine code on the printed ticket 312.

Please amend paragraph [0075] as follows:

[0075] According to embodiments of the present invention, some or all of the specialized devices may have their hardware aggregated such as to present only one coupling interface. For example, video displays 802, non-video displays 804, interactive controls 806 and card reader 818 may be aggregated into a single specialized device mounted in, on or coupled to the gaming machine. For example a player tracking device running ~~Windows CE~~ **WINDOWS CE operating system** may be loosely coupled via the communication network to a high-level software module running in the central server, the high-level software module implementing a player tracking management function.

Please amend paragraph [0080] as follows:

[0080] The game service bus according to embodiments of the present invention provides high level applications and specialized devices with a uniform set of mechanisms for negotiating service messages on the communication bus such as naming, discovery, message routing, publish and subscribe eventing, message transformations, workflows, communication recovery from nodes powering-off then on again, and so on. The game service bus may be deployed within a casino property via private Intranet or across casino properties via public Internet (using secure communication means such as VPN, SSL or IPSec, for example). ~~Microsoft~~ **MICROSOFT** "Biztalk Services" (www.biztalk.net) may advantageously be used to quickly deploy a service bus across properties. Biztalk Services is an Internet Service Bus, i.e. a fabric that interconnects distributed applications.

Please amend paragraph [0089] as follows:

[0089] In a service oriented architecture (based on SOAP, CORBA, IBM SOA and Web-services, for example), services may be discovered using service discovery protocols. Service discovery protocols are network protocols which allow automatic detection of devices and services offered by these devices on a computer network. There are many service discovery protocols including, for example, DNS Service Discovery (DNS-SD), Service Location Protocol (SLP), Simple Service Discovery Protocol (SSDP) as used in Universal Plug and Play (UPnP), Universal Description, Discovery and Integration (UDDI) for Webservices, ~~Jini~~ JINI for ~~Java~~ JAVA objects, ~~Bluetooth~~ **BLUETOOTH** Service Discovery Protocol (SDP), WS-Discovery (Web Services Dynamic Discovery), Internet Storage Name Service (iSNS), Web Proxy Autodiscovery Protocol and Dynamic Host Configuration Protocol, to name but a representative few.

Please amend paragraph [0094] as follows:

[0094] An embodiment of the present invention includes the use of the IP protocol for intercommunication between each of the modules shown in Figure 9. Other existing or future protocols may also be used such as, for example, IPX from ~~Novel~~ **NOVEL**; however, the IP protocol is universally used for the Internet and many communicating products and components support it. The payment and identification devices may be coupled to the Network Access Point or IP Converter 1004 by an RS232, RS485, USB, I2C, 802.11, ~~Blue Tooth~~ **BLUETOOTH**, Ethernet, ~~Fire Wire~~ **FIREWIRE** or most any standardized interface.

Please amend paragraph [0096] as follows:

[0096] According to another embodiment of the present invention, the specialized devices may be configured to offer asynchronous notification of events directly to the central server(s) 112 over a communication network, such as shown at 102, for example. Figure 20 shows a simplified diagram wherein a specialized device, coupled to the central server(s) 112 by a network, sends asynchronous notifications packets to the central server(s) 112 following an event being received by the specialized device or an event generated by the specialized device. For asynchronous notification of events, the server(s) 112 may register (subscribe) with the specialized devices for the list of events that are of interest. Then, the event notification process running in the specialized device may produce a call back to the server(s) 112 (thus the name callback) in order to pass details on the event information when it occurs. A mechanism to un-register (unsubscribe) may be provided wherein the server(s) may inform the specialized device to stop sending asynchronous notification of events. A preferred embodiment of the asynchronous notification of events is the callback feature of COM+, DCOM, REMOTING technologies from ~~Microsoft~~ **MICROSOFT** and the callback capability of SOAP, although other technologies may be implement within the context of embodiments of the present invention.

Please amend paragraph [0100] as follows:

[0100] Figure 12 represents an extension of Figure 11, in which the specialized devices are directly capable of network communication using, for example, technology developed for smart IP peripherals, according to a still further embodiment of the present invention. Smart IP peripherals are commonly called Internet Appliances. According to an embodiment of the invention, the specialized devices may each be controlled by a processor capable of supporting an operating system such as ~~Microsoft Windows CE, Microsoft~~ MICOROSFT WINDOWS CE, MICROSOFT Embedded XP or Embedded Linux; IP networking may be carried out via a wired or wireless link. With such advanced operating system, applications may be loaded from the network. Therefore, applications need not be stored locally within the specialized device, thereby avoiding software upgrade issues. Indeed, application software may be loaded into the gaming machines 200, 300, 400, any specialized device thereof from a remote server 112 and/or from a PVU 500, 600, 700. Similarly, application software may be loaded into the PVUs 500, 600, 700 and/or into any specialized devices therein from a remote server 112. Moreover, the entire operating system of the present gaming machine may be replaced over the network 1202. The operating system may be booted from the network 1202 using PXE (Preboot Execution Environment), for example.

Please amend paragraph [0101] as follows:

[0101] Figure 13 represents the APVU 700 equipped with IP-Ready specialized devices. These specialized devices are preferably interchangeable with the IP-Ready specialized devices that equip the present gaming machine. Therefore, the APVU's specialized devices may interact directly with the central server(s) 112 via network services, thus benefiting of the same advantages as the gaming machine. As shown, the APVU 700 may incorporate hardware and corresponding software modules for a microphone 1302, a sound system 1304, a video camera 728, a display 1308, a keypad 1310, an alarm system 1312, a active security system 1314 for the internal safe, a power supply 1316 and an Uninterruptible Power Supply ("UPS"). Network Services, as referred to herein, relate to service-oriented architectures such as **MICROSOFT** Microsoft DCOM, Common Object Request Broker Architecture (CORBA), ~~Microsoft .NET~~ MICROSOFT.NET and Sun ~~Java 2~~ JAVA 2 Platform, Enterprise Edition (J2EE), for example. ~~Microsoft .NET~~ MICROSOFT.NET and Sun J2EE are also commonly referred as "Web Services" and offer a universal solution over the Internet using XML, SOAP, Web Services Description Language (WSDL) and Universal Description, Discovery and Integration (UDDI) standardized technologies. UDDI nodes enables developers to publish web services and enables their software to search for and bind to services offered by others.

Please amend paragraph [0102] as follows:

[0102] Network Services deliver loose coupling services between service requestors and service providers. Service requestors "consume" services provided by services providers. Publication of service descriptions play a central role to enable service requestors to discover available services and bind to them. The service descriptions allow service requestors to bind to the service provider. The service requestor obtains service descriptions through a variety of techniques, from the simple "e-mail me the service description" approach to techniques such as ~~Microsoft~~ MICROSOFT DISCO and sophisticated service registries like UDDI.

Please amend paragraph [0104] as follows:

[0104] For embodiments of the present invention, ~~Microsoft~~ MICROSOFT DCOM is a currently preferred technology, as DCOM support is already integrated into ~~Microsoft Windows CE and Embedded XP~~ MICROSOFT WINDOWS CE and EMBEDDED XP, although embodiments of the present invention may be readily configured using other technologies, as those of skill in this art may appreciate. In the long term, ~~Microsoft .NET~~ MICROSOFT.NET web services over a private IP network (or VPN over Internet) may become the preferred technology, as it offers flexible and dynamic discovery of Net/Web services. The notion of a private or non-operator UDDI node is critical to the emergence of a dynamic style of a service-oriented architecture. As of this writing, Microsoft MICROSOFT has announced support of .NET web services in ~~Windows CE.NET~~ WINDOWS CE.NET.

Please amend paragraph [0106] as follows:

[0106] The advantages of the configuration described above include significantly increased data integrity (fully on-line system, fault/disaster tolerant central server(s) 112), significantly strengthened fraud control (fully on-line system, centralized audit log, centralized code execution, quality code, centralized authentication), significantly increased stability (server class operating system, quality code, fault tolerant central server(s) 112), immediate code upgrade capability, accurate and instantly available audit (all the gaming machine critical events are instantly logged in the centralized audit log 840). Moreover, the hardware necessary to support the execution the video entertainment/games engine software module may be a very economical yet extremely multimedia capable game console such as ~~Microsoft Xbox® or Sony PlayStation®~~ MICROSOFT XBOX® or SONY PLAYSTATION®, for example.

Please amend paragraph [0119] as follows:

[0119] According to one embodiment of the present invention, ~~Microsoft~~ MICROSOFT DCOM may be advantageously used; DCOM support is already integrated into ~~Microsoft Windows CE and Embedded XP~~ MICROSOFT WINDOWS CE and EMBEDDED XP. In the long term, ~~Microsoft .NET~~ MICROSOFT.NET web services over a private IP network (or VPN over Internet) may become the preferred technology, as it offers flexible and dynamic discovery of Net/Web services. The notion of a private or non-operator UDDI node is critical to the emergence of a dynamic style of a service-oriented architecture. As of this writing, ~~Microsoft~~ MICROSOFT has announced support of .NET web services in ~~Windows CE.NET~~ WINDOWS CE.NET. These network technologies are encapsulated in the ~~Microsoft~~ MICOROSOFT WCF – Windows Communication Foundation available in ".NET Framework 3.0" and later versions.

Please amend paragraph [0121] as follows:

[[0121] Figure 21 illustrates a view of the service based gaming system according to an embodiment of the present invention including a plurality of nodes 2104, 2106, 2108, 2110, 2112 and 2114 arranged such as to offer one service publisher 2128 and multiple service subscribers

2130, 2132, 2134, 2136 and 2138. The network 2102 is representative of a physical communication medium that may be loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH** **communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2116, 2118, 2120, 2122, 2124 and 2126 may be included in each node to allow the communication of services. The publisher 2128 may publish (or provide) services that one or a plurality of subscribers (or consumers) may consume, over the network 2102. The services provided by the publishing node 2104/2128 may be (a) high level functions such as from a business application server, a bonusing server, a customer loyalty server, a progressive jackpot server and a player tracking server, or (b) services from a specialized device, e.g. a network connected printer, a network connected bill acceptor, a player tracking combo (video display + touch-screen + card reader) and devices connected to a network bridge USB to Ethernet or RS232 to Ethernet. The services provided by the publishing node 2104/2128 may be consumed independently by multiple subscribing nodes 2106/2130, 2108/2132, 2110/2134, 2112/2136 and/or 2114/2138.

Please amend paragraph [0122] as follows:

[0122] Figure 22 illustrates a view of a service based gaming system, according to an embodiment of the present invention. As shown, the service based gaming system may include a plurality of nodes 2204, 2206, 2208, 2210, 2212 and 2214 arranged such as to offer multiple service publishers 2228, 2230, 2232, 2234 and 2236 and one service subscriber 2238. The network 2202 is representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2216, 2218, 2220, 2222, 2224 and 2226 may be included in each node to allow the communication of services. The services provided by the publishing node 2204/2228, 2206/2230, 2208/2232, 2210/2234 and/or 2212/2236 may be (a) high level functions such as from a business application server, a bonusing server, a customer loyalty server, a progressive jackpot server and a player tracking server, or (b) services from a specialized device, e.g. a network connected printer, a network connected bill acceptor, a player tracking combo (video display + touch-screen + card reader) and devices connected to a network bridge USB to Ethernet or RS232 to Ethernet. The services provided by the publishing nodes 2204/2228, 2206/2230, 2208/2232, 2210/2234 and 2212/2236 may be consumed independently by one subscribing node 2214/2238; for example, network connected printers installed in gaming machines may publish a range of services and a maintenance server may subscribe to, e.g., a paper jam alert and the paper low alert services such that the maintenance server may forward a job order to a technician on his or her mobile device.

Please amend paragraph [0123] as follows:

[0123] Figure 23 illustrates a view of a service based gaming system according to another embodiment of the present invention that may include a plurality of nodes 2302, 2304, 2306, 2308, 2310, 2312, 2314, 2316 and 2318 arranged such as to offer multiple service publishers 2336, 2340, 2346 and 2350 and multiple service subscribers 2338, 2342, 2344 and 2348. As described relative to Figs. 21 and 22, the network 2302 may be representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2320, 2322, 2324, 2326, 2328, 2330, 2332 and 2334 may be included in each node to allow the communication of services.

Please amend paragraph [0124] as follows:

[0103] Figure 24 illustrates a view of a service based gaming system according to an embodiment of the present invention. As shown, the service based gaming system of Figure 24 may include a plurality of nodes 2404, 2406 and 2408, wherein each node is arranged such as to offer one or more of: one service publisher, multiple service publishers, one service subscriber and multiple service subscribers. The network 2402 is representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2410, 2412 and 2414 may be included in each node to allow the communication of services. For example, node 2404 may include a central media server that may be configured to publish, for example, music content 2416, advertising video content 2418, promotional video content 2420 and a live TV feed 2422 to authorized participating nodes in the distributed gaming system. Node 2406 may include, for example, a billboard in a bar section wherein one network connected streaming plasma display 2424 may subscribe to the live video TV feed 2422 and the network connected ambience audio system may subscribe to the music content 2416. Node 2408 may include, for example, a gaming machine wherein an instance of a media player process 2430 may subscribe to the live video TV feed 2422 and another instance of a media player process 2432 may subscribe to the advertising video content 2418, and the video contents may be displayed simultaneously on the video gaming display or displays through a separate video window or 3D viewport. The gaming machine 2408 may publish 2428 its gaming meters using the GSA G2S protocol (Game Standard Association Game-to-System protocol), and any authorized node may subscribe to receive the gaming meters such as a casino management system (whose primary function is to satisfy regulatory accounting), a game download server, a security server, a marketing server, a player tracking server and/or a maintenance server, for example.

Please amend paragraph [0128] as follows:

[0104] Embodiments of the present invention offer a modular architecture for an on-line gaming system that may readily accommodate the wide variety of regulatory requirements encountered around the world. The strongest open security standards may be used. The very complex software code is located in the high-level software modules that may advantageously be developed using an advanced unified integrated development environment (such as, for example, ~~Microsoft .NET~~ MICROSOFT.NET). The various elements may be arranged in a tightly coupled configuration, loosely coupled configuration or in a mixture of tightly and loosely coupled configuration without requiring the high-level software modules to be entirely redesigned, retested and re-certified. In most cases, the high-level software modules may be re-used without modification thus saving enormous cost and development, validation and testing time. A gaming system may be constructed using a wide variety of computer hardware and software platforms, and make use of the latest multimedia technologies to attract the younger generation of players used to flashy and networked games. IP-Ready specialized devices using Internet appliance technologies offer tremendous benefit as the gaming machines, entertainment machines and payment verification units become a simple shell; the devices may be fully managed by the central server(s) 112. An advantageous embodiment of the invention is one in which the processing of all the high-level software modules, including graphics rendering, is carried out by the central server(s) 112, which relies on a server-class operating system and fault tolerant computing platform. Consequently, embodiments of the present invention provide an architecture that overcomes the technical lag, security limitations and lack of stability of the prior art.

Please amend paragraph [0130] as follows:

[0130] Embodiments of the present invention also offer a modular architecture for an on-line gaming system that may readily accommodate the wide variety of regulatory requirements encountered around the world. The strongest open security standards may be used. The very complex software code is located in the high-level software modules that may advantageously be developed using an advanced unified integrated development environment (such as, for example, Microsoft .NET). The various elements may be arranged in a tightly coupled configuration, loosely coupled configuration or in a mixture of tightly and loosely coupled configuration without requiring the high-level software modules to be entirely redesigned, retested and re-certified. Similarly, a subset of the specialized devices may have its hardware aggregated such as to present only one coupling interface. Embodiments of video displays 802, non-video displays 804, interactive controls 806 and card reader 818 may be aggregated into a single specialized device mounted in the gaming machine, for example a player tracking device running ~~Windows CE~~ WINDOWS CE operating system that is loosely coupled via the communication network to a high-level software module running in the central server, the high-level software module implementing a central player tracking management function. In most cases, the high-level software modules may be re-used without modification, thereby affording significant saving in costs and development, validation and testing time. A gaming system may be constructed using a wide variety of computer hardware and software platforms, and make use of the latest multimedia technologies to attract the younger generation of players used to flashy and networked games. IP-Ready specialized devices using Internet appliance technologies offer tremendous benefit as the gaming machines, entertainment machines and payment verification units become a simple shell; as the devices may be fully managed by the central server(s) 112. An advantageous embodiment of the invention is one in which the processing of all the high-level software modules, including graphics rendering, is carried out by the central server(s) 112, which relies on a server-class operating system and fault tolerant computing platform. Consequently, embodiments of the present invention provide an architecture that overcomes the technical lag, security limitations and lack of stability of the conventional gaming systems.

IN THE CLAIMS:

1. **(Original)** A distributed gaming system, comprising:

a communication bus;

at least one first node, each including a first computer coupled to the communication bus;

at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:

publish the at least one high-level function;

provide the at least one high-level function upon receiving a request to consume the at least one high-level function;

enable execution of the at least one high-level function upon receiving a request for execution;

perform a call back upon receiving a request to consume or execute the at least one high-level function, and

return a reply subsequent to receiving a request for execution of the at least one high-level function;

at least one second node, each including a second computer coupled to the communication bus, and

at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively:

subscribe to or consume the published or provided at least one high-level function;

request that the at least one first node execute the at least one high-level function;

accept the reply subsequent to receiving a reply from the at least one first node, and

accept the call-back upon receiving a call-back from the at least one first node.

2. **(Original)** The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call.

3. **(Original)** The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a HTTP request.

4. **(Original)** The distributed gaming system of claim 1, wherein the first service oriented software is configured to enable execution of the at least one high-level function upon receiving a request for execution via a HTTP request.

5. **(Original)** The distributed gaming system of claim 1, wherein the first service oriented software is configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call.

6. **(Original)** The distributed gaming system of claim 1, wherein the first service oriented software is configured to return a HTTP reply subsequent to receiving a HTTP request for execution of the at least one high-level function.

7. **(Original)** The distributed gaming system of claim 1, wherein the service oriented protocol is the Service Oriented Architecture Protocol (SOAP).

8. **(Original)** The distributed gaming system of claim 1, wherein the communication bus includes loosely coupled and/or tightly coupled nodes.

9. **(Original)** The distributed gaming system of claim 8, wherein the loosely coupled nodes include nodes coupled via at least one of Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and satellite link.

10. **(Canceled)**

11. **(Original)** The distributed gaming system of claim 1, wherein the at least one high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and an outcome determination function.

12. **(Original)** The distributed gaming system of claim 1, wherein the at least one first node includes one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine.

13. **(Original)** The distributed gaming system of claim 1, wherein the at least one second node includes at least one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

14. **(Canceled)**

15. **(Canceled)**

16. **(Original)** The distributed gaming system of claim 1, wherein security over the communication bus is provided by implementation of at least one of the IPSec protocol, the VPN tunneling protocol and the SSL protocol.

17. **(Original)** The distributed gaming system of claim 1, wherein the at least one second node includes a gaming machine.

18. **(Original)** The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine.

19. **(Original)** The distributed gaming system of claim 1, wherein the at least one first node includes a gaming machine.

20. **(Original)** The distributed gaming system of claim 1, wherein the at least one first node is included inside a gaming machine.

21. **(Original)** The distributed gaming system of claim 1, wherein the at least one second node is a gaming machine played by a player and is configured to execute at least one function call during a game session.

22. **(Original)** The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine played by a player and is configured to execute at least one function call during a game session.

23. **(Original)** The distributed gaming system of claim 1, wherein the at least one first node is configured for load balancing with another one of the at least one first node.

24. **(Original)** The distributed gaming system of claim 1, wherein the negotiating of service messages on the communication bus include at least one of naming, discovery, message routing, publishing eventing, subscribing eventing, message transformations, workflows, and communication recovery from nodes powering-off then on again.

25. **(Original)** A distributed gaming system, comprising:

a communication bus;

a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and

a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.

26. **(Original)** The distributed gaming system of claim 25, wherein the first gaming machine is further configured to perform a call back upon receiving a request to consume or execute the at least one high-level function, and return a reply and wherein the second gaming machine is further configured to accept the reply subsequent to receiving the call-back from the first gaming machine.

27. **(Original)** The distributed gaming system of claim 25, further including a service-oriented device coupled to the communication bus, the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine, the service oriented device being configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function.

28. **(Original)** A method for distributed gaming over a communication bus, comprising:

providing a first gaming machine and coupling the first gaming machine to the communication bus;

publishing, by the first gaming machine, a first high-level function over the communication bus;

providing a node coupled to the communication bus;

receiving, from the node, a request to subscribe to the published first high-level function;

accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus.

29. **(Original)** The method of claim 28, wherein the receiving step is carried out with the node including a second gaming machine.

30. **(Original)** The method of claim 28, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

31. **(Original)** The method of claim 28, wherein the high-level function includes at least one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

32. **(Original)** The method of claim 28, further comprising a step of receiving, from the node, a request that the first gaming machine executes the high-level function.

33. **(Original)** The method of claim 28, further comprising a step of the first gaming machine performing a call back upon receiving the request to consume or execute the high-level function.

34. **(Original)** The method of claim 28, wherein the second providing step is further carried out with the node being configured to selectively publish, subscribe, provide, execute and request that the first gaming machine execute the high level function.

35. **(Original)** A method for distributed gaming over a communication bus, comprising:

providing a first node and coupling the first node to the communication bus;

publishing, by the first node, a high-level function over the communication bus;

providing a first gaming machine coupled to the communication bus;

receiving, from the first gaming machine, a request to subscribe to the published high-level function;

accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus.

36. **(Original)** The method of claim 35, wherein the receiving step is carried out with the first node including a second gaming machine.

37. **(Original)** The method of claim 35, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

38. **(Currently Amended)** The method of ~~claim 354~~ claim 35, wherein the high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

39. **(Original)** The method of claim 35, further comprising a step of receiving, from the first gaming machine, a request that the node execute the first high-level function.

40. **(Original)** The method of claim 35, further comprising a step of the node performing a call back upon receiving the request to consume or execute the high-level function.

41. **(Original)** The method of claim 35, wherein the second providing step is further carried out with the first gaming machine being configured to selectively publish, subscribe, provide, execute and request that the node execute the high level function.

Application Number	**Application/Control No.** 11/842,147	**Applicant(s)/Patent under Reexamination** BRUNET DE COURSSOU, THIERRY	

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 10/3/11	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

ANDRE ROBINSON

3 TDS WERE APPRVD.

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

86915 7590 05/02/2012
Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

EXAMINER	
TIV, BACKHEAN	

ART UNIT	PAPER NUMBER
2451	

MAIL DATE	DELIVERY MODE
05/02/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 11/842,147	**Applicant(s)** BRUNET DE COURSSOU, THIERRY	
	Examiner BACKHEAN TIV	**Art Unit** 2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2011*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-9,11,12 and 16-41* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *1-9,11,12,16-24 and 28-41* is/are allowed.

7)☒ Claim(s) *25 and 27* is/are rejected.

8)☒ Claim(s) *26* is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Detailed Action

Claims 1-9, 11,12, 16-41 are pending in this application. Claims 10, 13-15 have been cancelled. This is in response to the Amendments/Remarks filed on 10/3/11. This action is made **FINAL.**

Specification

The substitute specification filed on 10/3/11, is acknowledge.

Terminal Disclaimer

The 3 terminal disclaimer filed on 10/3/11 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 25,27 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,674,128 issued to Holch et al.(Holch) in view of US Patent 5,762,552 issued to Vuong et al.(Vuong).

As per claim 25, Holch teaches distributed gaming system, comprising: a communication bus; a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function(col.6, lines 21-37), and

Holch does not explicitly teach a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.

Vuong teaches a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function(col.4, line 63-col.5, line 35).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention to modify the teachings of Holch to include the teachings of Vuong in order to have a remote gaming system that allows remote players to place wagers in a real-time game(Vuong, col.1, lines 5-10).

One ordinary skill in the art would have been motivated to combine the teachings of Holch and Vuong in order to have a remote gaming system that allows remote players to place wagers in a real-time game(Vuong, col.1, lines 5-10).

As per claim 27, a distributed gaming system of claim 25, further including a service-oriented device coupled to the communication bus, the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine, the service oriented device being configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function(Holch, col.6, lines 21-37, Vuong, col.4, line 63-col.5, line 35). See claim 25 for motivation to combine.

Allowable Subject Matter

Claims 1-9, 11,12, 16-24, 28-41 allowed.

Claim 26 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

Applicant's arguments filed 10/3/11 have been fully considered but they are not persuasive.

The applicant argues in substance that the prior art does not teach, gaming machine publish, execute, and provide at least one high-level function.

In reply, as defined by the applicant specification,

> [0097] Each gaming machine, according to still further embodiments, may publish player tracking services that (a) reads the player tracking card inserted in a card reader specialized device, (b) displays player tracking information on at least one of the player display (e.g. via a dedicated video display, via pop-up overlapping windows over a player video display, via a sliding overlapping windows over a player video display, via alpha-blended outlined data, icons or sprites over a player video display, or any other mechanisms to overlay information over a player video display), and (c) interacts with the player (e.g. via a touch-screen, a keypad, a pointing device, a joystick, biometric input). A central player tracking management system (that may advantageously leverage on intelligence data retrieved from the casino property hospitality network and servers) may subscribe to the player tracking services (offered on each

gaming machine) in order for the central player tracking high level applications to interact directly with a player at the gaming machine.

In which Holch, explicitly teaches a user inserting a card into the gaming machine((a) readying player tracking card), and where the account information of the user is displayed((b) displaying player information on a display), and where the user enter his/her pin((c) interacts with player via keypad)) which is similar to para.0097.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in its entirety as potentially teaching of all or part of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Backhean Tiv whose telephone number is (571) 272-5654. The examiner can normally be reached on M-T 7-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Backhean Tiv/
Primary Examiner, Art Unit 2451

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER	
	Examiner BACKHEAN TIV	Art Unit 2451	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,573,248 A	11-1996	Parra et al.	273/274
*	B	US-2001/0014881 A1	08-2001	Drummond et al.	705/43
*	C	US-6,334,614 B1	01-2002	Breeding, John G.	273/292
*	D	US-6,383,078 B1	05-2002	Yacenda, Michael W.	463/41
*	E	US-RE37,885 E	10-2002	Acres et al.	463/42
*	F	US-6,567,854 B1	05-2003	Olshansky et al.	709/229
*	G	US-2003/0103644 A1	06-2003	Klayh, John	382/100
*	H	US-6,595,859 B2	07-2003	Lynn, Scott W.	463/42
*	I	US-2003/0177187 A1	09-2003	Levine et al.	709/205
*	J	US-2005/0027382 A1	02-2005	Kirmse et al.	700/091
*	K	US-6,945,870 B2	09-2005	Gatto et al.	463/29
*	L	US-2006/0003835 A1	01-2006	Olive, Scott	463/025
*	M	US-2006/0030399 A1	02-2006	Baerlocher, Anthony J.	463/020

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER	
	Examiner BACKHEAN TIV	Art Unit 2451	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,297,062 B2	11-2007	Gatto et al.	463/42
*	B	US-7,374,486 B2	05-2008	Baerlocher, Anthony J.	463/20
*	C	US-2008/0171601 A1	07-2008	Kirmse et al.	463/42
*	D	US-2008/0194317 A1	08-2008	Baerlocher, Anthony J.	463/20
*	E	US-2008/0214280 A1	09-2008	Baerlocher, Anthony J.	463/20
*	F	US-2009/0143133 A1	06-2009	Baerlocher, Anthony J.	463/20
*	G	US-7,546,602 B2	06-2009	Hejlsberg et al.	719/313
*	H	US-2010/0203959 A1	08-2010	Olive, Scott	463/27
*	I	US-7,802,276 B2	09-2010	Swix et al.	725/14
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

SEARCHED

Class	Subclass	Date	Examiner
463	25,42	5/24/11	BT
235	115, 380, 382	5/24/11	BT
902	3,23	5/24/11	BT
340	5.8, 5.82, 323	5/24/11	BT
709	205, 218, 219	5/24/11	BT

SEARCH NOTES

Search Notes	Date	Examiner
INVENTOR'S NAME SEARCH PALM	5/24/11	BT
EAST TXT SEARCH	5/24/11	BT
NPL SEARCH (GOOGLE, WIKIPEDIA)	5/24/11	BT
Update Search	5/1/12	BT

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

/BACKHEAN TIV/ Examiner.Art Unit 2451	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2458	game near4 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/05/01 15:25
L3	21	game near4 (advertisement or progessive or reward) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/05/01 15:25
L4	19	game near4 (progessive or reward) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/05/01 15:26
L5	0	game near4 (progessive) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/05/01 15:26
S1	2	("7297062").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:17
S2	2	("5762552").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:24
S3	10	(("5179517") or ("5674128") or ("5800269") or ("6089982") or ("6280328")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:51
S4	1	("re37885").PN.	US-PGPUB;	OR	OFF	2011/05/24

			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
						10:07

S5	2	("5762552").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:09

S6	2	("20070191102").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:10

S7	2	("6945870").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:25

S8	3	("6,916,247").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:26

S9	6991	(463/25,42).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:53

S10	7842	(235/115,380,382).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:54

S11	220	(902/3,23).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:54

S12	1283	(340/5.8,5.82,323).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
				OR	OFF	2011/05/24
						10:54

			IBM_TDB			

S13	13372	(709/205,218,219).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:55

S14	29364	S9 or S10 or S11 or S12 or S13	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:57

S15	86	("20020090934" | "20020174444" | "20030037335" | "20030087683" | "20030100370" | "20030100371" | "20030171140" | "20050032577" | "20050054448" | "20050059494" | "20050113172" | "20050233811" | "20050282637" | "20060183537" | "20060270478" | "20070180371" | "20070184896" | "4335809" | "5179517" | "5667440" | "5674128" | "5759102" | "5762552" | "5800269" | "5970143" | "6048269" | "6077163" | "6089982" | "6135887" | "6142876" | "6219836" | "6251014" | "6273821" | "6280328" | "6409602" | "6463530" | "6710895" | "6732920" | "6749510" | "6908391" | "6916247" | "6921331" | "6945870").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:58

S16	4	("6210274" | "6428413").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:59

S17	6	("20040185936" | "20060030383" | "20070191102").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:59

S18	2	("20070191102").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:59

S19	4	game near4 plac$4 near5 wager same protocol and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						13:08

S20	0	game near4 plac$4 near5 wager same (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:10

S21	90	game near4 plac$4 near5 wager and (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:10

S22	4	("20010014881" | "6219836").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:28

S23	161970	(HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:51

S24	6	HTTP near4 (reply or replies or request) with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:51

S25	136	SOAP with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:52

S26	1	SOAP near2 protocol with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:52

S27	6	SOAP near2 protocol same game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:52

S28	0	malware near3 reboot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
				OR	ON	2012/01/19 13:46

			DERWENT; IBM_TDB			

S29	92	malware same reboot	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/19 13:46

S30	270	game and subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S31	0	game near5 machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S32	18	gamewith machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S33	0	game with machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S34	20	game same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S35	2	("5674128").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/01/20 10:22

EAST Search History (Interference)

<This search history is empty>

5/1/2012 3:29:43 PM
C:\ Users\ btiv\ Documents\ EAST\ Workspaces\ 11842147_game_communication_different_protocol.wsp

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** ☒ **CPA** ☒ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	05/24/2011	05/01/2012							
	1	✓	=							
	2	✓	=							
	3	✓	=							
	4	✓	=							
	5	✓	=							
	6	✓	=							
	7	✓	=							
	8	✓	=							
	9	✓	=							
	10	✓	-							
	11	✓	=							
	12	✓	=							
	13	✓	=							
	14	✓	-							
	15	✓	-							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							
	21	✓	=							
	22	✓	=							
	23	✓	=							
	24	✓	=							
	25	✓	✓							
	26	✓	O							
	27	✓	✓							
	28	✓	=							
	29	✓	=							
	30	✓	=							
	31	✓	=							
	32	✓	=							
	33	✓	=							
	34	✓	=							
	35	✓	=							

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** ☒ **CPA** ☒ **T.D.** □ **R.1.47**

CLAIM		**DATE**									
Final	Original	05/24/2011	05/01/2012								
	36	✓	=								
	37	✓	=								
	38	✓	=								
	39	✓	=								
	40	✓	=								
	41	✓	=								

PATENT
1140-026-1-CIP (AP00060)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Thierry Brunet de Courssou	:	Art Unit: 2451
	:	
Serial No.: 11/842,147	:	Confirmation No.: 2880
	:	
Filed: August 21, 2007	:	Attorney Docket No.: 1140-026-1-CIP
	:	
For: GAME TALK SERVICE BUS	:	Examiner: Tiv, Backhean
	:	

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AFTER FINAL

In response to the Office Action dated May 02, 2012, please amend the above-identified application as follows.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks and/or Arguments begin on page 9 of this paper.

CLAIMS

1. (Original) A distributed gaming system, comprising:

a communication bus;

at least one first node, each including a first computer coupled to the communication bus;

at least one first service oriented software executing in the first computer of each first node, the first service oriented software including at least one high-level function and a first service oriented protocol, the first service oriented protocol being configured to negotiate service messages over the communication bus, the first service oriented software being configured to selectively:

publish the at least one high-level function;

provide the at least one high-level function upon receiving a request to consume the at least one high-level function;

enable execution of the at least one high-level function upon receiving a request for execution;

perform a call back upon receiving a request to consume or execute the at least one high-level function, and

return a reply subsequent to receiving a request for execution of the at least one high-level function;

at least one second node, each including a second computer coupled to the communication bus, and

at least one second service oriented software executing in the second computer of each second node, the second service oriented software including at least one function call and a second service oriented protocol configured to negotiate service messages over the communication bus, the second service oriented software being configured, upon execution of the at least one function call, to selectively:

subscribe to or consume the published or provided at least one high-level function;

request that the at least one first node execute the at least one high-level function;

accept the reply subsequent to receiving a reply from the at least one first node, and

accept the call-back upon receiving a call-back from the at least one first node.

2. (Original) The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a remote procedure call.

3. (Original) The distributed gaming system of claim 1, wherein the first service oriented software is configured to provide the at least one high-level function upon receiving a request to consume the at least one high-level function via a HTTP request.

4. (Original) The distributed gaming system of claim 1, wherein the first service oriented software is configured to enable execution of the at least one high-level function upon receiving a request for execution via a HTTP request.

5. (Original) The distributed gaming system of claim 1, wherein the first service oriented software is configured to perform a call back upon receiving a request to consume or execute the at least one high-level function via a remote procedure call.

6. (Original) The distributed gaming system of claim 1, wherein the first service oriented software is configured to return a HTTP reply subsequent to receiving a HTTP request for execution of the at least one high-level function.

7. (Original) The distributed gaming system of claim 1, wherein the service oriented protocol is the Service Oriented Architecture Protocol (SOAP).

8. (Original) The distributed gaming system of claim 1, wherein the communication bus includes loosely coupled and/or tightly coupled nodes.

9. (Original) The distributed gaming system of claim 8, wherein the loosely coupled nodes include nodes coupled via at least one of Ethernet, Wi-Fi, Internet, radio-link, RS-422, micro-wave link and satellite link.

10. (Canceled) The distributed gaming system of claim 8, wherein the tightly coupled nodes include nodes coupled via at least one of inter-process communication, USB, Bluetooth, RS-232, RS-422 and IEEE1394 Firewire.

11. (Original) The distributed gaming system of claim 1, wherein the at least one high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function and an outcome determination function.

12. (Original) The distributed gaming system of claim 1, wherein the at least one first node includes one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine.

13. (Original) The distributed gaming system of claim 1, wherein the at least one second node includes at least one of a gaming machine, an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

14. (Canceled) The distributed gaming system of claim 1, wherein the first service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI.

15. (Canceled) The distributed gaming system of claim 1, wherein the second service oriented protocol includes one of asynchronous notification of events, COM+, DCOM, Microsoft Remoting, Microsoft .NET, Corba, SOAP, IBM SOA and UDDI.

16. (Original) The distributed gaming system of claim 1, wherein security over the communication bus is provided by implementation of at least one of the IPSec protocol, the VPN tunneling protocol and the SSL protocol.

17. (Original) The distributed gaming system of claim 1, wherein the at least one second node includes a gaming machine.

18. (Original) The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine.

19. (Original) The distributed gaming system of claim 1, wherein the at least one first node includes a gaming machine.

20. (Original) The distributed gaming system of claim 1, wherein the at least one first node is included inside a gaming machine.

21. (Original) The distributed gaming system of claim 1, wherein the at least one second node is a gaming machine played by a player and is configured to execute at least one function call during a game session.

22. (Original) The distributed gaming system of claim 1, wherein the at least one second node is included inside a gaming machine played by a player and is configured to execute at least one function call during a game session.

23. (Original) The distributed gaming system of claim 1, wherein the at least one first node is configured for load balancing with another one of the at least one first node.

24. (Original) The distributed gaming system of claim 1, wherein the negotiating of service messages on the communication bus include at least one of naming, discovery, message routing, publishing eventing, subscribing eventing, message transformations, workflows, and communication recovery from nodes powering-off then on again.

25. (Canceled) A distributed gaming system, comprising:

a communication bus;

a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and

a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function.

26. (Currently Amended) ~~The distributed gaming system of claim 25~~ A distributed gaming system, comprising:

a communication bus;

a first gaming machine coupled to the communication bus; the first gaming machine being configured to selectively publish, execute and provide at least one high-level function, and

a second gaming machine coupled to the communication bus, the second gaming machine being configured to selectively subscribe to or consume the at least one high-level function published or provided by the first gaming machine, and selectively request that the first gaming machine execute the at least one high-level function, wherein the first gaming machine is further configured to perform a call back upon receiving a request to consume or execute the at least one high-level function, and return a reply and wherein the second gaming machine is further configured to accept the reply subsequent to receiving the call-back from the first gaming machine.

27. (Currently Amended) The distributed gaming system of claim 26 ~~25~~, further including a service-oriented device coupled to the communication bus, the service oriented device including at least one of a payment verification unit, a specialized device, an IP enabled peripheral, a server, a server farm, a computer device, and an automatic teller machine, the service oriented device being configured to selectively publish, subscribe, provide, execute and request that either the first or the second gaming machine execute the at least one high level function.

28. (Original) A method for distributed gaming over a communication bus, comprising:

providing a first gaming machine and coupling the first gaming machine to the communication bus;

publishing, by the first gaming machine, a first high-level function over the communication bus;

providing a node coupled to the communication bus;

receiving, from the node, a request to subscribe to the published first high-level function;

accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first gaming machine, the call backs returning a result of the execution of the first high-level function to the node over the communication bus.

29. (Original) The method of claim 28, wherein the receiving step is carried out with the node including a second gaming machine.

30. (Original) The method of claim 28, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

31. (Original) The method of claim 28, wherein the high-level function includes at least one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

32. (Original) The method of claim 28, further comprising a step of receiving, from the node, a request that the first gaming machine executes the high-level function.

33. (Original) The method of claim 28, further comprising a step of the first gaming machine performing a call back upon receiving the request to consume or execute the high-level function.

34. (Original) The method of claim 28, wherein the second providing step is further carried out with the node being configured to selectively publish, subscribe, provide, execute and request that the first gaming machine execute the high level function.

35. (Original) A method for distributed gaming over a communication bus, comprising:

providing a first node and coupling the first node to the communication bus;
publishing, by the first node, a high-level function over the communication bus;
providing a first gaming machine coupled to the communication bus;
receiving, from the first gaming machine, a request to subscribe to the published high-level function;
accepting the subscription request;

initiating a gaming session on the first gaming machine, and

responsive to updates occurring during the gaming session, providing call backs, by the first node, the call backs returning a result of the execution of the high-level function to the first gaming machine over the communication bus.

36. (Original) The method of claim 35, wherein the receiving step is carried out with the first node including a second gaming machine.

37. (Original) The method of claim 35, wherein the receiving step is carried out with the node including at least one of an entertainment machine, a payment verification unit, a specialized device, an IP enabled device, a server, a server farm, a computer device, and an automatic teller machine.

38. (Previously Presented) The method of claim 35, wherein the high-level function includes one of a business function, an audit function, an authentication function, a biometric identification function, a graphics rendering computation function, and an outcome determination function.

39. (Original) The method of claim 35, further comprising a step of receiving, from the first gaming machine, a request that the node execute the first high-level function.

40. (Original) The method of claim 35, further comprising a step of the node performing a call back upon receiving the request to consume or execute the high-level function.

41. (Original) The method of claim 35, wherein the second providing step is further carried out with the first gaming machine being configured to selectively publish, subscribe, provide, execute and request that the node execute the high level function.

REMARKS

In the Office Action dated May 2, 2012, the Examiner rejected claims 25 and 27 and objected claim 26 as being dependent upon a rejected base claim. The Examiner indicated that claim 26 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

By this amendment, claim 26 has been amended to overcome the Examiner's objection and to place it into allowable form. The dependency of claim 27 has been amended to make claim 27 depend from claim 26. Claim 25 has been canceled. Therefore, the claims as now amended should be in allowable form.

The allowance of claims 1-9, 11, 12, 16-24, and 28-41 is noted with appreciation.

CONCLUSION

In view of the foregoing amendments and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action are respectfully solicited. An early allowance is hereby requested.

Respectfully submitted,

12 July 2012

/Richard E. Billion 32836/

Richard E. Billion
Registration No. 56,809
CLISE, BILLION & CYR, PA
605 US Highway 169 South
Minneapolis, MN 55441
(763) 587-7080

Electronic Acknowledgement Receipt

EFS ID:	13241943
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Richard E. Billion./Megan Miller
Filer Authorized By:	Richard E. Billion.
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	12-JUL-2012
Filing Date:	21-AUG-2007
Time Stamp:	19:08:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73(b).	373b.pdf	429494 a634a8f95cc672d76f89f66532de2be9658efa25	no	2

Warnings:

Information:

2	Power of Attorney	IGTSignedPoA.pdf	76497 6e5409907b880c45339854985b72dc16966145cb	no	1
Warnings:					
Information:					
3		Response_Filed_07122012.pdf	52877 e0f2d75a5aeb8c1f68217a42d58f433751db8f91	yes	9

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment After Final	1	1
Claims	2	8
Applicant Arguments/Remarks Made in an Amendment	9	9

Warnings:	
Information:	
Total Files Size (in bytes):	558868

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: IGT

Application No./Patent No.: 11/842,147 Filed/Issue Date: 21 August 2007

Titled: GAME TALK SERVICE BUS

IGT , a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. □ the assignee of the entire right, title, and interest in;

2. □ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is ________ %); or

3. □ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. □ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel ________, Frame ________, or for which a copy therefore is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Thierry Brunet De Courssou To: Cyberview Technology, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 019770 , Frame 0501 , or for which a copy thereof is attached.

2. From: Cyberview Technology, Inc. To: Mudalla Technology, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 025204 , Frame 0141 , or for which a copy thereof is attached.

3. From: Mudalla Technology, Inc. To: IGT
The document was recorded in the United States Patent and Trademark Office at
Reel 027546 , Frame 0720 , or for which a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Richard E. Billion 32836/ 12 July 2012
Signature Date

Richard E. Billion Attorney for Assignee
Printed or Typed Name Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 100204

OR

□ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 100204

OR

□ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

International Game Technology
6355 S. Buffalo Drive
Las Vegas, NV 89113

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	Rao Coca	Date	11/11/11
Name	T. Rao Coca	Telephone	702-669-7777
Title	Vice President		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/842,147	Filing Date 08/21/2007	□ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter “0” in column 2.

APPLICATION AS AMENDED – PART II

	(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	**07/12/2012**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 37	Minus	** 41	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD’L FEE	**0**	OR	TOTAL ADD’L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD’L FEE		OR	TOTAL ADD’L FEE	

* If the entry in column 1 is less than the entry in column 2, write “0” in column 3.
** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 20, enter “20”.
*** If the “Highest Number Previously Paid For” IN THIS SPACE is less than 3, enter “3”.
The “Highest Number Previously Paid For” (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/WANDA MEREDITH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

86915 7590 07/18/2012

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

EXAMINER	
TIV, BACKHEAN	
ART UNIT	PAPER NUMBER
2451	

DATE MAILED: 07/18/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

TITLE OF INVENTION: GAME TALK SERVICE BUS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	10/18/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

86915 7590 07/18/2012

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

TITLE OF INVENTION: GAME TALK SERVICE BUS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	10/18/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
TIV, BACKHEAN	2451	709-205000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ______________________

2 ______________________

3 ______________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ______________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

86915 7590 07/18/2012

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

EXAMINER	
TIV, BACKHEAN	
ART UNIT	PAPER NUMBER
2451	

DATE MAILED: 07/18/2012

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1013 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1013 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 11/842,147	**Applicant(s)** BRUNET DE COURSSOU, THIERRY	
	Examiner BACKHEAN TIV	**Art Unit** 2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7/12/12*.

2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-9, 11-13, 16-24, 26-41 (renumbered as claims 1-37)*.

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE “MAILING DATE” of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER’S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. □ CORRECTED DRAWINGS (as “replacement sheets”) must be submitted.

   (a) □ including changes required by the Notice of Draftsperson’s Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner’s Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner’s comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. □ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

/Backhean Tiv/
Primary Examiner, Art Unit 2451

Detailed Action

Claims 1-9, 11-13, 16-24, 26-41 are pending in this application. Claims 10,14,15,25 have been cancelled. This is a response to the After-Final Amendments filed on 7/12/12.

REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance: The prior art singly or in combination does not teach all the limitations of claims 1-9, 11-13, 16-24, 26-41. See Arguments filed on 10/3/11.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BACKHEAN TIV whose telephone number is (571)272-5654. The examiner can normally be reached on M-TH 7-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on (571) 272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Backhean Tiv/
Primary Examiner, Art Unit 2451

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER
	Examiner BACKHEAN TIV	Art Unit 2451 Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,573,248 A	11-1996	Parra et al.	273/274
*	B	US-2001/0014881 A1	08-2001	Drummond et al.	705/43
*	C	US-6,334,614 B1	01-2002	Breeding, John G.	273/292
*	D	US-6,383,078 B1	05-2002	Yacenda, Michael W.	463/41
*	E	US-RE37,885 E	10-2002	Acres et al.	463/42
*	F	US-6,567,854 B1	05-2003	Olshansky et al.	709/229
*	G	US-2003/0103644 A1	06-2003	Klayh, John	382/100
*	H	US-6,595,859 B2	07-2003	Lynn, Scott W.	463/42
*	I	US-2003/0177187 A1	09-2003	Levine et al.	709/205
*	J	US-2005/0027382 A1	02-2005	Kirmse et al.	700/091
*	K	US-6,945,870 B2	09-2005	Gatto et al.	463/29
*	L	US-2006/0003835 A1	01-2006	Olive, Scott	463/025
*	M	US-2006/0030399 A1	02-2006	Baerlocher, Anthony J.	463/020

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 11/842,147	Applicant(s)/Patent Under Reexamination BRUNET DE COURSSOU, THIER
	Examiner BACKHEAN TIV	Art Unit 2451 — Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,297,062 B2	11-2007	Gatto et al.	463/42
*	B	US-7,374,486 B2	05-2008	Baerlocher, Anthony J.	463/20
*	C	US-2008/0171601 A1	07-2008	Kirmse et al.	463/42
*	D	US-2008/0194317 A1	08-2008	Baerlocher, Anthony J.	463/20
*	E	US-2008/0214280 A1	09-2008	Baerlocher, Anthony J.	463/20
*	F	US-2009/0143133 A1	06-2009	Baerlocher, Anthony J.	463/20
*	G	US-7,546,602 B2	06-2009	Hejlsberg et al.	719/313
*	H	US-2010/0203959 A1	08-2010	Olive, Scott	463/27
*	I	US-7,802,276 B2	09-2010	Swix et al.	725/14
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

OK TO ENTER: /BT/ (07/14/2012)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Thierry Brunet de Courssou	:	Art Unit: 2451
Serial No.: 11/842,147	:	Confirmation No.: 2880
Filed: August 21, 2007	:	Attorney Docket No.: 1140-026-1-CIP
For: GAME TALK SERVICE BUS	:	Examiner: Tiv, Backhean

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AFTER FINAL

In response to the Office Action dated May 02, 2012, please amend the above-identified application as follows.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks and/or Arguments begin on page 9 of this paper.

OK TO ENTER: /BT/ (07/14/2012)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2880

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/842,147	08/21/2007 **RULE**	709	2451	CYBS5805CIP

APPLICANTS

Thierry Brunet de Courssou, Henderson, NV;

** **CONTINUING DATA** *************************

This application is a CIP of 10/120,635 04/10/2002 PAT 7,297,062
which claims benefit of 60/332,593 11/23/2001

** **FOREIGN APPLICATIONS** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
08/31/2007

		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed □ Yes ☑ No 35 USC 119(a-d) conditions met □ Yes ☑ No Verified and Acknowledged /BACKHEAN TIV/ Examiner's Signature	□ Met after Allowance Initials	NV	23	~~41~~ 37	4

ADDRESS

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028
UNITED STATES

TITLE

GAME TALK SERVICE BUS

FILING FEE RECEIVED 1115	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other ________________ □ Credit

Issue Classification	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

ORIGINAL	
CLASS	**SUBCLASS**
709	205

CROSS REFERENCE(S)

CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
709	218	219			
463	25	42			
235	115	380	382		

INTERNATIONAL CLASSIFICATION

CLAIMED					**NON-CLAIMED**				
G	0	6	F	15 / 16 (2006.0)					

□ Claims renumbered in the same order as presented by applicant ☒ CPA ☒ T.D. □ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	14	17	29	33										
2	2	15	18	30	34										
3	3	16	19	31	35										
4	4	17	20	32	36										
5	5	18	21	33	37										
6	6	19	22	34	38										
7	7	20	23	35	39										
8	8	21	24	36	40										
9	9		25	37	41										
	10	22	26												
10	11	23	27												
11	12	24	28												
12	13	25	29												
	14	26	30												
	15	27	31												
13	16	28	32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 37	
/BACKHEAN TIV/ Primary Examiner.Art Unit 2451 (Primary Examiner)	7/14/12 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 23

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** ☒ **CPA** ☒ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	05/24/2011	05/01/2012	07/14/2012						
1	1	✓	=	=						
2	2	✓	=	=						
3	3	✓	=	=						
4	4	✓	=	=						
5	5	✓	=	=						
6	6	✓	=	=						
7	7	✓	=	=						
8	8	✓	=	=						
9	9	✓	=	=						
	10	✓	-	-						
10	11	✓	=	=						
11	12	✓	=	=						
12	13	✓	=	=						
	14	✓	-	-						
	15	✓	-	-						
13	16	✓	=	=						
14	17	✓	=	=						
15	18	✓	=	=						
16	19	✓	=	=						
17	20	✓	=	=						
18	21	✓	=	=						
19	22	✓	=	=						
20	23	✓	=	=						
21	24	✓	=	=						
	25	✓	✓	-						
22	26	✓	O	=						
23	27	✓	✓	=						
24	28	✓	=	=						
25	29	✓	=	=						
26	30	✓	=	=						
27	31	✓	=	=						
28	32	✓	=	=						
29	33	✓	=	=						
30	34	✓	=	=						
31	35	✓	=	=						

Index of Claims	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

☐ **Claims renumbered in the same order as presented by applicant** ☒ **CPA** ☒ **T.D.** ☐ **R.1.47**

CLAIM		DATE								
Final	Original	05/24/2011	05/01/2012	07/14/2012						
32	36	✓	=	=						
33	37	✓	=	=						
34	38	✓	=	=						
35	39	✓	=	=						
36	40	✓	=	=						
37	41	✓	=	=						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	("7297062").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:17
S2	2	("5762552").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:24
S3	10	(("5179517") or ("5674128") or ("5800269") or ("6089982") or ("6280328")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/04/07 08:51
S4	1	("re37885").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:07
S5	2	("5762552").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:09
S6	2	("20070191102").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:10
S7	2	("6945870").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	OFF	2011/05/24 10:25
S8	3	("6,916,247").PN.	US-PGPUB;	OR	OFF	2011/05/24

			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
						10:26

S9	6991	(463/25,42).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:53

S10	7842	(235/115,380,382).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:54

S11	220	(902/3,23).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:54

S12	1283	(340/5.8,5.82,323).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:54

S13	13372	(709/205,218,219).CCLS.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2011/05/24
						10:55

S14	29364	S9 or S10 or S11 or S12 or S13	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:57

S15	86	("20020090934" | "20020174444" | "20030037335" | "20030087683" | "20030100370" | "20030100371" | "20030171140" | "20050032577" | "20050054448" | "20050059494" | "20050113172" | "20050233811" | "20050282637" | "20060183537" | "20060270478" | "20070180371" | "20070184896" | "4335809" | "5179517" | "5667440" | "5674128" | "5759102" | "5762552" | "5800269" | "5970143" | "6048269" | "6077163" | "6089982" | "6135887" | "6142876" | "6219836" | "6251014" | "6273821" | "6280328" |	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24
						10:58

		"6409602" | "6463530" | "6710895" | "6732920" | "6749510" | "6908391" | "6916247" | "6921331" | "6945870").PN.				

S16	4	("6210274" | "6428413").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 10:59

S17	6	("20040185936" | "20060030383" | "20070191102").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 10:59

S18	2	("20070191102").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 10:59

S19	4	game near4 plac$4 near5 wager same protocol and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:08

S20	0	game near4 plac$4 near5 wager same (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:10

S21	90	game near4 plac$4 near5 wager and (HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:10

S22	4	("20010014881" | "6219836").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:28

S23	161970	(HTTP or SOAP) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2011/05/24 13:51

S24	6	HTTP near4 (reply or replies or request)	US-PGPUB;	OR	ON	2011/05/24

		with game and (@ad<="20011123" or @rlad<="20011123")	USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB			13:51
S25	136	SOAP with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52
S26	1	SOAP near2 protocol with game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52
S27	6	SOAP near2 protocol same game and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2011/05/24 13:52
S28	0	malware near3 reboot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/01/19 13:46
S29	92	malware same reboot	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/01/19 13:46
S30	270	game and subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/01/20 10:17
S31	0	game near5 machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT; IBM_TDB	OR	ON	2012/01/20 10:17
S32	18	gamewith machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB; USPAT; USOCR; FPRS; EPO; DERWENT;	OR	ON	2012/01/20 10:17

			IBM_TDB			

S33	0	game with machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S34	20	game same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/01/20 10:17

S35	2	("5674128").PN.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	OFF	2012/01/20 10:22

S36	2458	game near4 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/01 15:25

S37	21	game near4 (advertisement or progessive or reward) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/01 15:25

S38	19	game near4 (progessive or reward) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/01 15:26

S39	0	game near4 (progessive) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO;
			DERWENT;
			IBM_TDB
				OR	ON	2012/05/01 15:26

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L1	8515	(463/25,42).CCLS.	US-PGPUB;
			USPAT;
			UPAD
				OR	OFF	2012/07/14 09:19

L2	8438	(235/115,380,382).CCLS.	US-	OR	OFF	2012/07/14

			PGPUB;
			USPAT;
			UPAD
						09:19

L4	15813	(709/205,218,219).CCLS.	US-PGPUB;
			USPAT;
			UPAD
				OR	OFF	2012/07/14 09:19

L5	14	gamewith machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			UPAD
				OR	ON	2012/07/14 09:20

L6	0	game with machine same subscrib$4 near5 (advertisement or progessive or reward) and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			UPAD
				OR	ON	2012/07/14 09:20

L7	20	game near4 (advertisement or progessive or reward) near3 jackpot and (@ad<="20011123" or @rlad<="20011123")	US-PGPUB;
			USPAT;
			UPAD
				OR	ON	2012/07/14 09:20

L8	2	l7 and (l1 or l2 or l4)	US-PGPUB;
			USPAT;
			UPAD
				OR	ON	2012/07/14 09:21

7/14/2012 9:21:39 AM
C:\ Users\ btiv\ Documents\ EAST\ Workspaces\ 11842147_game_communication_different_protocol.wsp

Search Notes	**Application/Control No.** 11842147	**Applicant(s)/Patent Under Reexamination** BRUNET DE COURSSOU, THIERRY
	Examiner BACKHEAN TIV	**Art Unit** 2451

SEARCHED

Class	Subclass	Date	Examiner
463	25,42	5/24/11	BT
235	115, 380, 382	5/24/11	BT
902	3,23	5/24/11	BT
340	5.8, 5.82, 323	5/24/11	BT
709	205, 218, 219	5/24/11	BT

SEARCH NOTES

Search Notes	Date	Examiner
INVENTOR'S NAME SEARCH PALM	5/24/11	BT
EAST TXT SEARCH	5/24/11	BT
NPL SEARCH (GOOGLE, WIKIPEDIA)	5/24/11	BT
Update Search	5/1/12	BT

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
235	115,380,382	7/14/2012	BT
463	25,42	7/14/2012	BT
709	205,218,219	7/14/2012	BT

	/BACKHEAN TIV/ Primary Examiner.Art Unit 2451

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

86915 7590 07/18/2012

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Megan M. Miller	(Depositor's name)
/Megan M. Miller/	(Signature)
7 August 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP	2880

TITLE OF INVENTION: GAME TALK SERVICE BUS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	10/18/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
TIV, BACKHEAN	2451	709-205000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Clise, Billion & Cyr, P.A.
2 Richard E. Billion
3 ____________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
IGT	RENO, NV

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 50-3141 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☒ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Richard E. Billion 32836/ Date 7 August 2012

Typed or printed name Richard E. Billion Registration No. 32,836

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	11842147
Filing Date:	21-Aug-2007
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Filer:	Richard E. Billion./Megan Miller
Attorney Docket Number:	CYBS5805CIP

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1740	1740
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**2040**

Electronic Acknowledgement Receipt

EFS ID:	13440948
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Richard E. Billion./Megan Miller
Filer Authorized By:	Richard E. Billion.
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	07-AUG-2012
Filing Date:	21-AUG-2007
Time Stamp:	18:13:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2040
RAM confirmation Number	5290
Deposit Account	503141
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Issue Fee Payment (PTO-85B)	IssueFee.pdf	102673 1e6713d493dab4651006fd6171f9779a0008e749	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31684 758c705f5b47d8f9fd59240fdc3be80314e556fb	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	134357	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

content 2416. Node 2408 may include, for example, a gaming machine wherein an instance of a media player process 2430 may subscribe to the live video TV feed 2422 and another instance of a media player process 2432 may subscribe to the advertising video content 2418, and the video contents may be displayed simultaneously on the video gaming display or displays through a separate video window or 3D viewport. The gaming machine 2408 may publish 2428 its gaming meters using the GSA G2S protocol (Game Standard Association Game-to-System protocol), and any authorized node may subscribe to receive the gaming meters such as a casino management system (whose primary function is to satisfy regulatory accounting), a game download server, a security server, a marketing server, a player tracking server and/or a maintenance server, for example.

Change(s) applied
to document,
/R.L./
8/8/2012

Please amend paragraph [0128] as follows:

128

[0~~104~~] Embodiments of the present invention offer a modular architecture for an on-line gaming system that may readily accommodate the wide variety of regulatory requirements encountered around the world. The strongest open security standards may be used. The very complex software code is located in the high-level software modules that may advantageously be developed using an advanced unified integrated development environment (such as, for example, ~~Microsoft .NET~~ MICROSOFT.NET). The various elements may be arranged in a tightly coupled configuration, loosely coupled configuration or in a mixture of tightly and loosely coupled configuration without requiring the high-level software modules to be entirely redesigned, retested and re-certified. In most cases, the high-level software modules may be re-used without modification thus saving enormous cost and development, validation and testing time. A gaming system may be constructed using a wide variety of computer hardware and physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2320, 2322, 2324, 2326, 2328, 2330, 2332 and 2334 may be included in each node to allow the communication of services.

Change(s) applied to document, /R.L./ 8/8/2012

Please amend paragraph [0124] as follows:

[0~~103~~] 124 Figure 24 illustrates a view of a service based gaming system according to an embodiment of the present invention. As shown, the service based gaming system of Figure 24 may include a plurality of nodes 2404, 2406 and 2408, wherein each node is arranged such as to offer one or more of: one service publisher, multiple service publishers, one service subscriber and multiple service subscribers. The network 2402 is representative of a physical communication medium that may be a loosely coupled (e.g. LAN, WAN, Ethernet, Internet, Wi-Fi, ~~Bluetooth~~ **BLUETOOTH communication protocol**, USB-to-LAN adapters or a combination of them), tightly coupled (i.e. interprocess communication within a device or via USB) or a combination of loosely coupled and tightly coupled communication mediums. A SOAP communication stack 2410, 2412 and 2414 may be included in each node to allow the communication of services. For example, node 2404 may include a central media server that may be configured to publish, for example, music content 2416, advertising video content 2418, promotional video content 2420 and a live TV feed 2422 to authorized participating nodes in the distributed gaming system. Node 2406 may include, for example, a billboard in a bar section wherein one network connected streaming plasma display 2424 may subscribe to the live video TV feed 2422 and the network connected ambience audio system may subscribe to the music

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/842,147	09/11/2012	8266212	CYBS5805CIP	2880

86915 7590 08/22/2012

Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 1385 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Thierry Brunet de Courssou, Henderson, NV;

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 100204

OR

□ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 100204

OR

□ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

International Game Technology
6355 S. Buffalo Drive
Las Vegas, NV 89113

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	Rao Coca	Date	11/11/11
Name	T. Rao Coca	Telephone	702-669-7777
Title	Vice President		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	13639079
Application Number:	11842147
International Application Number:	
Confirmation Number:	2880
Title of Invention:	GAME TALK SERVICE BUS
First Named Inventor/Applicant Name:	Thierry Brunet de Courssou
Customer Number:	86915
Filer:	Richard E. Billion./Anise Krull
Filer Authorized By:	Richard E. Billion.
Attorney Docket Number:	CYBS5805CIP
Receipt Date:	31-AUG-2012
Filing Date:	21-AUG-2007
Time Stamp:	14:56:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73(b).	373b.pdf	429810 e1fa0e2d39a813c8030015df4ea80a66706cc247	no	2

Warnings:

Information:

2	Power of Attorney	IGTSignedPoA.pdf	76497 6e5409907b880c45339854985b72dc16966145cb	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	506307	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: International Game Technology

Application No./Patent No.: 11/842,147 Filed/Issue Date: 21 August 2007

Titled:
GAME TALK SERVICE BUS

International Game Technology, a Corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. □ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is ________ %); or

3. □ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. □ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel ____________, Frame ____________, or for which a copy therefore is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: THIERRY BRUNET DE COURSSOU To: CYBERVIEW TECHNOLOGY, INC.
The document was recorded in the United States Patent and Trademark Office at
Reel 019770, Frame 0501, or for which a copy thereof is attached.

2. From: CYBERVIEW TECHNOLOGY, INC. To: MUDALLA TECHNOLOGY, INC.
The document was recorded in the United States Patent and Trademark Office at
Reel 025204, Frame 0141, or for which a copy thereof is attached.

3. From: MUDALLA TECHNOLOGY, INC. To: IGT
The document was recorded in the United States Patent and Trademark Office at
Reel 027546, Frame 0720, or for which a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Richard E. Billion 32836/ 31 August 2012
Signature Date

Richard E. Billion Attorney for Assignee
Printed or Typed Name Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/842,147	08/21/2007	Thierry Brunet de Courssou	

CONFIRMATION NO. 2880

POA ACCEPTANCE LETTER

OC000000056424824

100204
Clise, Billion & Cyr, P.A./IGT
605 US Hwy 169 N Suite 300
Plymouth, MN 55441

Date Mailed: 09/10/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/31/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/dtvernon/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/842,147	08/21/2007	Thierry Brunet de Courssou	CYBS5805CIP

CONFIRMATION NO. 2880

POWER OF ATTORNEY NOTICE

86915
Young Law Firm, P.C.
4370 Alpine Road, Suite 106
Portola Valley, CA 94028

OC000000056424805

Date Mailed: 09/10/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/31/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/dtvernon/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas on the following

□ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:21-cv-331	DATE FILED 4/6/2021	U.S. DISTRICT COURT Western District of Texas

PLAINTIFF IGT and IGT Canada Solutions ULC	DEFENDANT Zynga Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 See Attachment 1		
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Attachment 1 to Form AO 120

IGT & IGT Canada Sols. ULC v. Zynga Inc. (W.D. Tex.)

Patent or Trademark No.	Date of Patent or Trademark	Holder of Patent or Trademark
8,708,791	Apr. 29, 2014	IGT
9,159,189	Oct. 13, 2015	IGT Canada Solutions ULC
7,168,089	Jan. 23, 2007	IGT
7,303,473	Dec. 4, 2007	IGT
8,795,064	Aug. 5, 2014	IGT
8,266,212	Sept. 11, 2012	IGT