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.
13/366,197	08/26/2014	8817984	47583.3	5655

27683 7590 08/06/2014

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

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 187 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):

Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	Herewith
				Filing Date	Herewith
				Applicant(s)	Paul Miller
				Art Unit	Not yet assigned
				Examiner Name	Not yet assigned
SHEET	1	OF	1	Attorney Docket Number	47583.3

U. S. PATENT DOCUMENTS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1	2011/0082768 A1	04-07-2011	Ori Eisen
	2	7,373,669 B2	05-13-2008	Ori Eisen
	3	2011/0113388 A1	05-12-2011	Eisen, et al.
	4	2008/0244744 A1	10-02-2008	Thomas, et al.
	5	2007/0214151 A1	09-13-2007	Thomas, et al.
	6	~~2007/024801 A1~~	05-31-2007	Thomas, et al. 2007/0124801
	7	7,908,662 B2	03-15-2011	Ric B. Richardson
	8	2010/0229224 A1	09-10-2010	Craig S. Etchegoyen
	9	2009/0138975 A1	05-28-2009	Ric B. Richardson
	10	7,937,467 B2	05-03-2011	Timothy P. Barber
	11	7,330,871 B2	02-12-2008	Timothy P. Barber

Change(s) ~~applied~~ to document, /M.F.O./ 5/30/2014

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published

Examiner Signature	/Dao Ho/	Date Considered	09/06/2013

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

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)

27683 7590 04/21/2014
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

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.

Pia S. Kamath	(Depositor's name)
	(Signature)
July 21, 2014 via EFS Web	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/21/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2497	380-255000

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 Haynes and Boone, LLP
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: MSIGNIA, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Irvine, California

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date July 21, 2014

Typed or printed name David Bowls Registration No. 39,915

Electronic Patent Application Fee Transmittal

Application Number:	13366197
Filing Date:	03-Feb-2012
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Filer:	David B. Bowls/Pia Kamath
Attorney Docket Number:	47583.3

Filed as Small 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	2501	1	480	480
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt

EFS ID:	19632444
Application Number:	13366197
International Application Number:	
Confirmation Number:	5655
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Pia Kamath
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.3
Receipt Date:	21-JUL-2014
Filing Date:	03-FEB-2012
Time Stamp:	14:23:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	648
Deposit Account	081394
Authorized User	BOWLS, DAVID B.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

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)	IssueFeeTransmittal.pdf	88088 b07398dcafae7441f8905938f28500863f30ef6d	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32111 b37addb62c032b621e5fd67cafb6363cb39348e6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	120199		

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

27683 7590 04/21/2014

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER
HO, DAO Q

ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 04/21/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/21/2014

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 ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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)

27683 7590 04/21/2014
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

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.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

TITLE OF INVENTION: CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/21/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, DAO Q	2497	380-255000

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

27683 7590 04/21/2014

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2497	

DATE MAILED: 04/21/2014

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 187 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 187 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.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B 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.

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. 13/366,197	Applicant(s) MILLER ET AL.	
	Examiner DAO HO	Art Unit 2497	AIA (First Inventor to File) Status No

-- 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 *01/06/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
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 *13-14, 16-25, 27-30, 32-34*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   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. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ 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).
6. ☐ 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. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *04/11/2014* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/DAO HO/
Examiner, Art Unit 2497

DETAILED ACTION

The present application is being examined under the pre-AIA first to invent provisions.

Claim Rejections - 35 U.S.C. § 112:

Applicants' arguments with respect to 112 1st paragraph with rejection of claims 13-34 have been fully considered and are persuasive. The rejection of 112 1st paragraph of claims 13-34 have been withdrawn in view of the amendment to claim.

Claim Rejections - 35 U.S.C. § 101:

Applicants' arguments with respect to claims 13-23 have been fully considered and are persuasive. The rejection of 35 USC §101 regarding claims 13-23 have been withdrawn in view of the amendment to claim.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney David Bowls on 04/11/2014.

The application has been amended as follows:

13. (Currently amended) A computer implemented method comprising:

selecting, by a hardware processor, a varying combination of minutia from a plurality of minutia types including software minutia of a device being challenged~~;~~, wherein selecting comprises choosing the selection of minutia to be a triplet of computer minutia types including a hardware minutia H, a firmware minutia F, and a software minutia S.

forming, by the hardware processor, a challenge that conveys enough information for the device being challenged to compute an actual response based on the selection of minutia from the plurality of device minutia types;

computing, by the hardware processor, a plurality of pre-processed responses possible, if the challenged device is valid, to receive from the challenged device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

sending, by the hardware processor, the challenge to the challenged device;

receiving, by the hardware processor, the actual response to the challenge from the challenged device;

comparing, by the hardware processor, the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating, by the hardware processor, the challenged device as identified by the values of the selection of minutia indicated by the pre-processed response that matches the actual response.

Claim 15. (Cancelled)

24. (Currently amended) A system comprising a server configured to communicate with a device, wherein:

the server selects a varying combination of minutia from a plurality of minutia types ~~including software minutia of the device;~~, wherein the combination of minutia is a triplet including a hardware minutia H, a firmware minutia F, and a software minutia S of the device;

the server forms a challenge that conveys enough information for the device to compute an actual response based on the selection of minutia from the plurality of device minutia types;

the server computes a plurality of pre-processed responses possible, if the challenged device is valid, to receive from the challenged device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

the server sends the challenge to the device;

the server receives the actual response to the challenge from the device;

the server compares the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, the server validates the device as identified by the values of the selection of minutia indicated by the pre-processed response that matches the actual response.

26. (Cancelled)

30. (Currently amended) A computer program product comprising a non-transitory computer readable medium having computer readable and executable code for instructing a hardware processor to perform a method, the method comprising:

selecting, by the hardware processor, a varying combination of minutia from a plurality of minutia types ~~including software minutia of a device being challenged;~~, wherein the plurality of types of computer minutia including hardware minutia H, firmware minutia F, and a software minutia S;

forming, by the hardware processor, a challenge that conveys enough information for the device being challenged to compute an actual response based on the selection of minutia from the plurality of device minutia types;

computing, by the hardware processor, a plurality of pro-processed responses possible if the challenged device is valid, to receive from the challenge device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

sending, by the hardware processor, the challenge to the challenged device;

receiving, by the hardware processor, the actual response to the challenge from the challenged device;

comparing, by the hardware processor, the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating, by the hardware processor, the challenged device as identified by the values of the selection of minutia indicated by the pre-

processed response that matches the actual response.

31. (Cancelled)

Allowable Subject Matter

Claims 13-14, 16-25, 27-30 and 32-34 are allowed.

The following is an examiner's statement of reasons for allowance:

Independent Claim(s) 13, 24, 30 and their respective dependent claims are allowable over prior arts since the prior arts taken individually or in combination fails to particular discloses, fairly suggest or render obvious the following italic limitations:

In claim(s) 13, 24 and 30:

"selecting, by the hardware processor, a varying combination of minutia from a plurality of minutia types, wherein selecting the types of minutia from a plurality of types of computer minutia including hardware minutia H, firmware minutia F, and a software minutia S." in combination with other limitations recited as specified in the independent claim(s).

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 DAO HO whose telephone number is (571) 270-5998. The examiner can normally be reached on Monday thru Thursday 8:00am - 6:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HADI ARMOUCHE can be reached on (571) 270-3618. 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.

/DAO HO/
Examiner, Art Unit 2497
04/16/2014

/PRAMILA PARTHASARATHY/
Primary Examiner, Art Unit 2497

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/366,197	MILLER ET AL.	
	Examiner	Art Unit	
	DAO HO	2497	

All participants (applicant, applicant's representative, PTO personnel):

(1) *DAO HO*. (3)_____.

(2) *David Bowls*. (4)_____.

Date of Interview: *11 April 2014*.

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: *13 and 15*.

Identification of prior art discussed: *Colella, Buffam, Spitzig et al.*.

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 and The Examiner discussed the claims filed on 01/06/2014 over the prior art rejection. The Examiner suggested to move depedent claim 15 into the independent claims for allowance. Agreement was reached.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of 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

/DAO HO/ Examiner, Art Unit 2497	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	894	((Paul) near2 (Miller)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:11
L2	13	((George) near2 (Tuvell)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:11
L3	906	1 2	US-PGPUB; USPAT; USOCR	OR	OFF	2014/04/16 18:12
L4	1	(challenge validat$3) with (minutia near5 value)	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:13
L5	124	(hardware same firmware same software) and minutia	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:14
L6	3	5 and (challenge same triplet)	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:14
L7	52	(plurality near2 minutia)	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:15
L8	4	7 and triplet	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:15
L9	1	8 AND ((H04L63/0876 OR H04L9/0861 OR H04L9/0866).CPC. OR (380/255).CCLS.)	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:17
L10	7	(triplet with minut$4).clm.	US-PGPUB; USPAT; USOCR	OR	ON	2014/04/16 18:18

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L11	7	(triplet with minut$4).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2014/04/16 18:18
L12	1	(minutia$ with value with key).clm.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/16 18:19

4/16/2014 6:19:58 PM
C:\Users\dho1\Documents\EAST\Workspaces\13366197.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	**Art Unit**
	DAO HO	2497

CPC						
Symbol					**Type**	**Version**
H04L		63	/	0876	F	20130101
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

/DAO HO/ Examiner.Art Unit 2497	04/16/2014	**Total Claims Allowed:**
(Assistant Examiner)	(Date)	19
		O.G. Print Claim(s) / O.G. Print Figure
(Primary Examiner)	(Date)	13 / 2A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	**Art Unit**
	DAO HO	2497

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
380	255	H	0	4	L	29 / 06 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											

/DAO HO/ Examiner.Art Unit 2497	04/16/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	19	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	13	2A

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	**Art Unit**
	DAO HO	2497

☐ 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	4	17	18	33										
-	2	5	18	19	34										
-	3	6	19												
-	4	7	20												
-	5	8	21												
-	6	9	22												
-	7	10	23												
-	8	11	24												
-	9	12	25												
-	10	-	26												
-	11	13	27												
-	12	14	28												
1	13	15	29												
2	14	16	30												
-	15	-	31												
3	16	17	32												

/DAO HO/ Examiner.Art Unit 2497	04/16/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	19	
		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	13	2A

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	Art Unit
	DAO HO	2497

✓	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	09/23/2013	04/16/2014							
-	1	N	-							
-	2	N	-							
-	3	N	-							
-	4	N	-							
-	5	N	-							
-	6	N	-							
-	7	N	-							
-	8	N	-							
-	9	N	-							
-	10	N	-							
-	11	N	-							
-	12	N	-							
1	13	✓	=							
2	14	✓	=							
-	15	✓	-							
3	16	✓	=							
4	17	✓	=							
5	18	✓	=							
6	19	✓	=							
7	20	✓	=							
8	21	✓	=							
9	22	✓	=							
10	23	✓	=							
11	24	✓	=							
12	25	✓	=							
-	26	✓	-							
13	27	✓	=							
14	28	✓	=							
15	29	✓	=							
16	30	✓	=							
-	31	✓	-							
17	32	✓	=							
18	33	✓	=							
19	34	✓	=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	Art Unit
	DAO HO	2497

CPC- SEARCHED		
Symbol	Date	Examiner
H04L63/0876	04/16/2014	dqh

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
380	255	09/22/2013	dqh
	update	04/16/2014	dqh

SEARCH NOTES		
Search Notes	Date	Examiner
see attached EAST search history	09/22/2013	dqh
inventor search in EAST	09/22/2013	dqh
class 380/255 with delimiter	09/22/2013	dqh
NPL: device authentiation using minutiae	09/22/2013	dqh
above searches update	04/16/2014	dqh

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	general interference and search of claims (PGPUB, UPAD)	04/16/2014	dqh

/DAO HO/ Examiner.Art Unit 2497	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Paul T. Miller, George A. Tuvell		
Assignee:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Serial No.:	13/366,197	Filing Date:	February 3, 2012
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.3	Confirmation No.:	5655

Irvine, California
January 6, 2014

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO OFFICE ACTION

In response to the Office action mailed October 7, 2013, Applicants submit the following amendments and remarks.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

IN THE CLAIMS

The following are claims 1-34:

1-12. (Canceled)

13. (Currently amended) A computer implemented method comprising:

selecting, by a hardware processor, ~~at least one type~~ a varying combination of minutia from a plurality of minutia types including software minutia of a device being challenged;

forming, by the hardware processor, a challenge that conveys enough information for the device being challenged to compute an actual response based on the selection of minutia from the plurality of device minutia types;

computing, by the hardware processor, a plurality of pre-processed responses possible, if the challenged device is valid, to receive from [[a]] the challenged ~~valid~~ device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

~~, wherein:~~

~~each pre-processed response is computed using a key; and~~

~~each key is computed using values that are possible for the selection of minutia types;~~

sending, by the hardware processor, the challenge to the challenged device;

receiving, by the hardware processor, ~~an~~ the actual response to the challenge from the challenged device;

~~, wherein:~~

~~the actual response is computed using an actual key;~~

~~the actual key is computed using:~~

~~a deduction of the selection of minutia types from the challenge; and~~

~~actual values of the selection of minutia types;~~

comparing, by the hardware processor, the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating, by the hardware processor, ~~the combination of~~ the challenged device as identified by ~~with the actual~~ values of the selection of minutia ~~types~~ indicated by the pre-processed response that matches the actual response.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

14. (Original) The method of claim 13, wherein selecting further comprises:

choosing the selection of minutia from a plurality of minutia including hardware minutia, firmware minutia, software minutia, geo-location data, calling app data, user secrets, or biometric information.

15. (Original) The method of claim 13, wherein selecting further comprises:

choosing the selection of minutia to be a triplet of computer minutia types including a hardware minutia H, a firmware minutia F, and a software minutia S.

16. (Original) The method of claim 13, further comprising:

choosing the selection of minutia according to a particular cataloging scheme of minutia.

17. (Original) The method of claim 13, further comprising:

choosing the selection of minutia using expectations for changes to the current device image.

18. (Original) The method of claim 13, further comprising:

choosing the selection of device minutia using knowledge of all industry updates that can occur on the device, whether or not actually occurring on the device.

19. (Original) The method of claim 13, further comprising:

choosing the selection of device minutia using knowledge of changes actually occurring on the device, wherein:

changes actually occurring on the device are inferred from the pre-processed responses, and

no information about actual values of the minutia currently on the device is carried by the actual response to the challenge.

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

20. (Original) The method of claim 13, wherein:

choosing the selection of device minutia includes choosing triplets according to a cataloging scheme that varies from one issuer of the challenge to another.

21. (Original) The method of claim 13, further comprising:

using knowledge of the current device image to choose the selection of device minutiae.

22. (Original) The method of claim 13, further comprising:

using the actual response to update knowledge of the current device image.

23. (Original) The method of claim 13, wherein processing a range of possible changes to a current device image further comprises:

pre-processing all possible responses from the device independently of receiving the actual response from the device.

24. (Currently amended) A system comprising a server configured to communicate with a device, wherein:

the server selects ~~at least one type~~ a varying combination of minutia from a plurality of minutia types including software minutia of the device;

the server forms a challenge that conveys enough information for the device to compute an actual response based on the selection of minutia from the plurality of device minutia types;

the server computes a plurality of pre-processed responses possible, if the challenged device is valid, to receive from [[a]] the challenged ~~valid~~ device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

~~, wherein:~~

~~each pre-processed response is computed using a key; and~~

~~each key is computed using values that are possible for the selection of minutia types;~~

the server sends the challenge to the device;

the server receives ~~an~~ the actual response to the challenge from the device;

~~, wherein:~~

~~the actual response is computed using an actual key;~~

~~the actual key is computed using:~~

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

~~a deduction of the selection of minutia types from the challenge; and~~

~~actual values of the selection of minutia types;~~

the server compares the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, the server validates ~~the combination of~~ the device as identified by ~~with~~ the ~~actual~~ values of the selection of minutia indicated by the pre-processed response that matches the actual response. ~~types.~~

25. (Original) The system of claim 24, wherein:

the second cryptographic key is varied by varying the selected set of minutia.

26. (Original) The system of claim 24, wherein:

the set of minutiae is a triplet including a hardware minutia H, a firmware minutia F, and a software minutia S.

27. (Original) The system of claim 24, wherein:

the server uses the actual response to update knowledge of the current device image without decoding any information about the current device image from the actual response.

28. (Original) The system of claim 24, wherein:

the server pre-processes all possible responses from the device independently of receiving the actual response from the device to calculate the plurality of pre-processed responses.

29. (Original) The system of claim 24, wherein:

the server uses knowledge of the current device image to select the set of minutiae.

30. (Currently amended) A computer program product comprising a non-transitory computer readable medium having computer readable and executable code for instructing a hardware processor to perform a method, the method comprising:

selecting, by the hardware processor, ~~at least one type~~ a varying combination of minutia from a plurality of minutia types including software minutia of a device being challenged;

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

forming, by the hardware processor, a challenge that conveys enough information for the device being challenged to compute an actual response based on the selection of minutia from the plurality of device minutia types;

computing, by the hardware processor, a plurality of pre-processed responses possible, if the challenged device is valid, to receive from [[a]] the challenged ~~valid~~ device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;

~~, wherein:~~

~~each pre-processed response is computed using a key; and~~

~~each key is computed using values that are possible for the selection of minutia types;~~

sending, by the hardware processor, the challenge to the challenged device;

receiving, by the hardware processor, ~~an~~ the actual response to the challenge from the challenged device;

~~, wherein:~~

~~the actual response is computed using an actual key;~~

~~the actual key is computed using:~~

~~a deduction of the selection of minutia types from the challenge; and~~

~~actual values of the selection of minutia types;~~

comparing, by the hardware processor, the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating, by the hardware processor, ~~the combination of~~ the challenged device as identified by ~~with the actual~~ values of the selection of minutia indicated by the pre-processed response that matches the actual response ~~types~~.

31. (Original) The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia from a plurality of types of computer minutia including hardware minutia H, firmware minutia F, or software minutia S.

32. (Original) The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia according to a particular cataloging scheme of minutia.

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

33. (Original) The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia using knowledge of all industry updates that can occur on the device, whether or not any particular update actually has occurred on the device.

34. (Original) The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia using expectations for changes to the current device image.

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

REMARKS

Claims 1-34 were pending in the present application. Claims 1-12 were withdrawn due to restriction/election and are hereby canceled without prejudice to their further prosecution. Claims 13, 24, and 30 are amended. Accordingly, upon entry of this amendment claims 13-34 will be pending.

Summary of the Office Action

Claims 13-34 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Claims 13-23 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Claims 13, 14, 16-25, 27-30, and 32-34 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication 2007/0174206 to Colella (referred to as "**Colella**") in view of U.S. Patent 6,185,316 to Buffam (referred to as "**Buffam**").

Claims 15, 26, and 31 were rejected under 35 U.S.C. 103(a) as being unpatentable over Colella in view of Buffam, further in view of U.S. Patent Application Publication 2010/0027834 to Spitzig et al. (referred to as "**Spitzig**").

Examiner Interview

Applicants wish to thank the Examiner for the telephone interview conducted between the Examiner and Applicants' representative on December 12, 2013. The section 112 and section 101 rejections were discussed and agreement was reached that proposed amendments should overcome these rejections. The section 103 rejections were discussed, along with the Colella, Buffam, and Spitzig references, and possible amendments to the claims. Applicants

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

have amended the claims in light of the Examiner's comments and suggestions. No further agreement was reached with regard to the section 103 rejections.

Amendments to the Claims

Claims 13, 24, and 30 are amended, support for which can be found in the figures (e.g., Figure 2) and the specification as originally filed, for example, at page 8, lines 1-15:

> Since the computer itself is uniquely identified, it represents a safer method of identifying customers (e.g., users or subscribers). By forming cryptographic keys which use minutia found on the computer, the computer itself (as defined by its minutia) is validated, not a static key stored or intended to be stored only on the computer. The discovery and copying of a single value (the secret key) is significantly easier than the discovery and copying of a very large range of computer minutia values. In addition, the writing of a single key in a computer's memory effectively counterfeits the uniqueness of a computer identified by a single, static stored value. To counterfeit a dynamic key crypto-identified computer, it would be necessary to intercept various methods to learn the minutiae values of the computer. Several direct and related methods may exist for learning the value of a particular computer minutia; to effectively counterfeit the computer, it may be that all methods for accessing all computer minutia values would need to be intercepted and the fraudulent response returned. Furthermore, since the dynamic key crypto system expects certain computer minutia values to change, a successfully counterfeited computer would also need to ensure the fraudulent computer minutia values change in an expected manner (emphasis added);

at page 20, lines 4-13:

> Although it may be the case that certain combinations of hardware, firmware, and software values may be incompatible (e.g., a particular software update might require a particular firmware update) the example of Figure 2 assumes that all updates are independent so that the total number of permutations of acceptable device characteristic values for the particular computer 18 being challenged is the product of the number of acceptable possibilities for each component, Hx, Fy, Sz, of the triplet Hx-Fy-Sz, or 1*9*20 = 180, as indicated at step 2007. The number of acceptable permutations for a selected combination of minutia, then, can be smaller than the number of possible permutation for the same triplet and significantly smaller than the total number of permutations for all minutiae, as shown by this example, e.g., 180 out of potentially millions of possible minutia values and 180 out of the potentially infinite number of permutations as indicated at step 2005 (emphasis added);

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

at page 20, lines 20-21:

> Selection of the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging a particular device may vary, not only from computer 18 to computer 18 and service provider 14 to service provider 14, but, for example, each time the same computer 18 is challenged on behalf of the same service provider 14. The intelligent minutia selection 114 may employ a number of considerations in selecting the combination of minutia to be used for a particular challenge of a particular computer 18 and service user 20. As shown step 2010, intelligent selection of the combination of minutia (e.g., Hx, Fy, Sz for the example) may be based on need for uniqueness, predictability . . . (emphasis added);

at page 21, line 11-13:

> intelligent minutia selection 114 process chooses the minutia nearly randomly to widely and unpredictably sample various computer minutia 64 and secrets and biometric minutia 26 (emphasis added);

at page 22, lines 12-14:

> Thus, the challenge cryptographically encodes enough information for the computer 18 being challenged to determine which minutia should be used in computing its actual response;

at page 11, lines 12-17:

> Identification based on a hash from a subset of minutia taken from a very wide range of minutia found or collected by the computer including hardware, firmware, software, user secrets, and user biometrics. The authentication can be performed as an intelligent challenge and response which indexes minutiae and, when compared to possible responses from anticipated minutiae, can ascertain minutia changes without having to actually exchange the minutiae between the computer and dynamic key crypto services (emphasis added);

at page 7, lines 3-5:

> The dynamic key cryptography system according to one embodiment anticipates changes to the minutia caused by updates and natural usage of the computer and practically eliminates false negatives that block valid users from a network service (emphasis added);

at page 10, lines 4-6:

> To achieve fault tolerance over a possibly changing set of minutia, anticipated changes to minutia and multiple subsets of minutia that provide back-up to any single subset can be used (emphasis added);

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

at page 11, lines 19-22:

> the anticipated and expected changes to the minutia used including non-computer factors such as user PIN entry, geo-location, and biometrics. Different minutia can be intelligently chosen for the challenge to achieve a response that yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation (emphasis added);

at page 12, lines 18-25:

> One embodiment uses a computer identity provider service to collect computer minutia information from the industry and uses this data to anticipate possible changes and permutations to minutiae on registered computers. By anticipating changes in minutiae found on the hardware, firmware, and software elements of a computer, embodiments are more fault-tolerant to natural changes in the computer. In this manner, embodiments can anticipate changes to minutiae and, through a challenge and response exchange between a computer and dynamic key crypto service, synchronize changes to minutiae without actually exchanging the minutiae between the computer and dynamic key crypto service (emphasis added);

and at page 22, line 29 through page 23, line 3:

> Because every allowable response to a challenge is therefore known (e.g., computed at step 2030) before the challenge is sent to the computer 18, the actual response that will be received from the computer 18 to the challenge may be among the range of pre-processed acceptable responses (and therefore among the acceptable changes) computed by the dynamic key crypto provider 10 that is challenging the computer 18 (emphasis added).

Applicants submit that no new matter is added.

Rejections under 35 U.S.C. 112

Independent claims 13, 24, and 30 are amended in such a way that the section 112 rejections have become moot. Therefore, Applicants respectfully request that the section 112 rejections to claims 13-34 be reconsidered and withdrawn.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

Rejections under 35 U.S.C. 101

Independent claim 13 is amended to address the section 101 rejections, as discussed during the Examiner interview. In addition to the method being limited to performance by a

hardware processor, Applicants believe that claim 13 should also be regarded as being tied to a machine or device, namely, the device being challenged. In light of the amendments, Applicants believe that clams 13-23 should be considered as being directed to statutory subject matter, and therefore, Applicants respectfully request that the section 101 rejections to claims 13-23 be reconsidered and withdrawn.

Rejections under 35 U.S.C. 103

Claims 13, 14, 16-25, 27-30, and 32-34 were rejected under 35 U.S.C. 103(a) as being unpatentable over **Colella** in view of **Buffam**.

Applicants submit that no combination of Colella and Buffam either discloses or suggests:

> selecting . . . a varying combination of minutia from a plurality of device minutia types including software minutia of a device being challenged;
> forming . . . a challenge that conveys enough information for the device being challenged to compute an actual response based on the selection of minutia from the plurality of device minutia types;
> computing . . . a plurality of pre-processed responses possible, if the challenged device is valid, to receive from the challenged device such that the plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of the selection of minutia from the plurality of device minutia types;
> sending . . . the challenge to the challenged device;
> receiving . . . the actual response to the challenge from the challenged device;
> comparing . . . the actual response to the pre-processed responses for a match; and
> based on whether or not a match was found, validating . . . the challenged device as identified by values of the selection of minutia indicated by the pre-processed response that matches the actual response (emphasis added),

as recited by Applicants' amended claim 13.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

Colella teaches reliance on (as opposed to Applicants' selecting) fingerprint minutia (see, e.g., Abstract; paragraph [0037] "ESP distributes SIID fingerprint authentication devices

to the participating banks. . . [e]ach registered user is then provided with a SITD fingerprint scanner"). Fingerprint minutia is only one type of minutia, namely features of a person's physical fingerprint, and, even if broadly considered as biological or biometric minutia, is still only one type of minutia, and thus distinguishable from Applicants' plurality of minutia types.

Moreover Applicants have further limited the plurality of minutia types to "device" minutia types such as software of a device, which is further distinguishable from biological minutia such as finger print minutia.

In addition, because Colella uses only fingerprint minutia (a single type), there is no variation in the type of minutia used, further distinguishing Colella from Applicants' "selecting a varying combination of minutia from a plurality of device minutia types".

Thus, Colella has no need to teach, as in Applicants' claim 13, "comput[ing] an actual response based on the selection of minutia" and does not so teach even in light of "the passcode is divisible, e.g., that the appropriate finger code corresponds to the appropriate finger, respectively" (Colella, paragraph [0041]), which only reiterates that only one type (fingerprint) of minutia is being used. Thus, Applicants' claim 13 is further distinguished from Colella.

Colella teaches "SIIDs 90, are useless until activated" and "[a]t the activation scan the fingerprints are scanned, and a portion of the digitized fingerprint data is stored locally on the SIID device 90 for later comparison" (paragraphs [0041]-[0042]). Later comparison, of course, relies on fingerprint minutia not changing (as is commonly accepted as a biological fact) and, thus, is contradictory to, as in Applicants' claim 13, "plurality of pre-processed responses anticipates acceptable changes on the challenged device to values of . . . the minutia." Thus, Applicants' limitations that "pre-processed responses anticipates acceptable changes [to values of minutia] on the challenged device" and "validating . . . the challenged device as identified by the values of . . . minutia indicated by the pre-processed response that

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

matches the actual response" is contrary to the principles of operation taught by Colella and thus Colella may be regarded as teaching away from Applicants' claim 13.

Thus, Applicants submit that claim 13 is patentable over Colella.

Because Colella teaches away from Applicants' claim 13, it would be illogical to combine Colella with any other reference and then to assert that Applicants' claim 13 is unpatentable over the combination of Colella with the reference. Nevertheless, Applicants submit that **Buffam** does not cure any of the deficiencies of Colella with regard to Applicants' claim 13 as amended. For example, Buffam relies on image points, whether true image points (TIPs) or false image points (FIPs) (see, e.g., col. 13, line 35 through col. 14, line 65), which, if interpreted as minutia, is only one type. Thus, with Buffam, there is no selection, no varying, and no computation of actual response based on selection as with Applicants' claim 13, as discussed above with reference to Colella.

In addition, Buffam's teaching that "[i]n general, the greater the number of FIPs used, the more difficult it is to correctly identify the entire FIP set without a priori knowledge of TIP or FIP placement, or both" (col. 14, lines 31-33) suggests that Buffam, like Colella, relies on absence of change, at least for the TIPs, and thus, as in Applicants' claim 13, that pre-processed responses anticipating acceptable changes to values of minutia on a challenged device and validating the challenged device by the values of minutia indicated by a pre-processed response that matches an actual response from the challenged device is contrary to the principles of operation taught by Buffam. Thus Buffam, like Colella, in addition to not curing the deficiencies of Colella also may be regarded as teaching away from Applicants' claim 13.

Thus, Applicants submit that claim 13 is patentable over both Colella and Buffam whether considered singly or in combination.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

Claims 15, 26, and 31 were rejected under 35 U.S.C. 103(a) as being unpatentable over Colella in view of Buffam, further in view of **Spitzig**.

Spitzig is cited for disclosing "an executable module integrated to perform data processing in created minutiae of software, hardware and firmware [Spit, ¶29]" (Office action, page 9, last paragraph). Spitzig at paragraph 29, however, states:

> Data processing--i.e., minutiae or metadata collection--at each phase is performed by an extractor module 56, an executable module integrated with and/or communicable with a process, device or utility (e.g., software, hardware, or firmware processes or tools) capable of operating during the time of a respective phase.

Thus, Applicants believe that Spitzig is referring here to implementation in software, hardware, or firmware of data processing for collection of minutia rather than to types of minutia themselves, and that Spitzig does not teach software, hardware, or firmware as different types of document minutia. Moreover, at paragraph 27, Spitzig teaches:

> As described with respect to the teachings presented herein, "minutiae data" may refer to any data representative of or descriptive of the physical or structural elements that define, characterize, or distinguish one document from another. . . . Minutiae data may include data generated, associated or conveyed during and throughout the life cycle of the document, including but not limited to data expressed or created during the time of document creation, definition, edition, versioning, . . . and physical manipulation. . . . the minutiae data may provide a persistent data record that may be retrieved as a function of the unique physical, structural and/or contextual elements associated with a document. No one minutiae item is sufficient for unique identification of a document, but rather, it is the collection of numerous matching minutiae that enables the unambiguous identification of a document (emphasis added).

Thus, Applicants submit that Spitzig suggests only one type of document minutia, namely data of any kind regarding the document. Even if Applicants grant different types of document minutia where Spitzig is disclosing, instead, multiple items of minutia, there is still no suggestion by Spitzig of selection of types, varying combinations, or computation of actual response based on selection of types as with Applicants' claim 13, as discussed above with reference to Colella. In addition, the reference to "persistent data record", as with Colella and

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612
Tel: (949) 202-3000
FAX (949) 202-3001

Buffam, suggests reliance on an absence of change in the document minutia, and thus, as in Applicants' claim 13, that pre-processed responses anticipating acceptable changes to values of minutia on a challenged device and validating the challenged device by the values of minutia indicated by a pre-processed response that matches an actual response from the challenged device is contrary to the principles of operation taught by Spitzig. Thus, Spitzig, like Buffam and Colella, in addition to not curing the deficiencies of Buffam and Colella also may be regarded as teaching away from Applicants' claim 13.

Therefore, Applicants submit that Applicants' claim 13 is patentable over Colella, Buffam, and Spitzig, and respectfully request that the section 103 rejections to claim 13 be reconsidered and withdrawn.

In light of the foregoing, Applicants believe that Applicants' claim 13 is patentable over any combination of Colella, Buffam, and Spitzig, and that Applicants' claims 24 and 30, which include limitations similar to those of claim 13, also are patentable over any combination of the references. The remaining claims, being dependent on their respective base claims 13, 24, and 30 are believed to be patentable for at least the same reasons as for claims 13, 24, and 30. Therefore, Applicants respectfully request that the section 103 rejections to claims 13-34 be withdrawn.

HAYNES AND BOONE, LLP
18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

CONCLUSION

In view of the foregoing, Applicants respectfully submit that claims 13-34 are in condition for allowance. Reconsideration and withdrawal of the rejections are respectfully requested and a timely Notice of Allowance is solicited.

If there are any questions regarding any aspect of the application, please call the undersigned at (949) 202-3011.

Certificate of Transmission

I hereby certify that this correspondence is being electronically transmitted via EFS Web to the Commissioner for Patents, on the date stated below.

January 6, 2014
Pia Kamath

Respectfully submitted,

David Bowls
Patent Agent
Reg. No. 39,915

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

Electronic Acknowledgement Receipt

EFS ID:	17833398
Application Number:	13366197
International Application Number:	
Confirmation Number:	5655
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Pia Kamath
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.3
Receipt Date:	06-JAN-2014
Filing Date:	03-FEB-2012
Time Stamp:	20:01:20
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		ResponsetoOfficeAction.pdf	986356 0808cbbfe7c500d2b3f81d4a07899c683cd4a9f0	yes	17

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Amendment Copy Claims/Response to Suggested Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	17
Warnings:			
Information:			
	Total Files Size (in bytes):	986356	

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/06 (09-11)
Approved for use through 1/31/2014. 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 13/366,197	Filing Date 02/03/2012	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 $310 ($155 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))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	01/06/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 22	Minus	** 34	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						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.

LIE
/DEBRA R. WYATT/

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.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

27683 7590 12/16/2013

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	
ART UNIT	PAPER NUMBER
2497	

MAIL DATE	DELIVERY MODE
12/16/2013	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.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/366,197	MILLER ET AL.	
	Examiner	Art Unit	
	DAO HO	2497	

All participants (applicant, applicant's representative, PTO personnel):

(1) *DAO HO*. (3)_____.

(2) *DAVID BOWLS (REG. NO.: 39,915)*. (4)_____.

Date of Interview: *12/12/2013*.

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: *13*.

Identification of prior art discussed: *Collela, buffam*.

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 and The Examiner discussed 112 1st paragraph and 101 rejection of claim 13, Applicant's will amended the claims to correct the issue. Agree was reached.
Regarding 103 rejection of claim 13, The Applicant's and The Examiner discussed the fingerprint minuta of Collela as opposed to plurality of minutia types of the invention. Applicant's agrees to amend the claims to specify the minutia types and add limitation to clarify the anticipation method and adding in the randomly selection of the minutia types to clarify the invention. Agree was reached..

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

/DAO HO/ Examiner, Art Unit 2497	/HADI ARMOUCHE/ Supervisory Patent Examiner, Art Unit 2497

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Paul T. Miller, George A. Tuvell		
Assignee:	mSignia, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Serial No.:	13/366,197	Filing Date:	February 3, 2012
Examiner:	Dao Q. Ho	Group Art Unit:	2497
Docket No.:	47583.3	Confirmation No.:	5655

Irvine, California
December 10, 2013

PROPOSED AGENDA FOR EXAMINER INTERVIEW

In regard to the Office action mailed October 7, 2013, Applicants, via their representative, would like to discuss the references Collela and Buffam, particularly in regard to "fingerprint minutia" as opposed to "plurality of minutia types" as recited in Applicants' claims.

Applicants would also like to discuss the section 101 and 112 rejections and the Spitzig reference.

Applicants would also like to discuss possible amendments to claim 1 in regard to the dynamic nature of Applicants' invention compared to the prior art.

HAYNES AND BOONE, LLP

18100 Von Karman, Suite 750
Irvine, CA 92612

Tel: (949) 202-3000
FAX (949) 202-3001

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.
13/366,197	02/03/2012	Paul Timothy Miller	47583.3	5655

27683 7590 10/07/2013

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

EXAMINER	
HO, DAO Q	

ART UNIT	PAPER NUMBER
2497	

MAIL DATE	DELIVERY MODE
10/07/2013	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. 13/366,197	Applicant(s) MILLER ET AL.	
	Examiner DAO HO	Art Unit 2493	AIA (First Inventor to File) Status No

-- 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 *02/03/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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 *06 September 2013*; 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) *1-34* is/are pending in the application.

5a) Of the above claim(s) *1-12* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *13-34* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

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).

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).

Certified copies:

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)).

* 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) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/03/2012, 05/20/2013*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Regarding the Election/Restrictions of Group I (Claims 1-12) and Group 2 (Claims 13-34) made over the phone with David Bowls on 09/06/2013.

Applicant's election without traverse of Group 2 (Claims 13-34) over the phone on 09/06/2013 is acknowledged.

This is a reply to the application filed on 09/06/2012, in which, **claims** 13-34 are pending. Claims 13, 24 and 30 are independent.

When making claim amendments, the applicant is encouraged to consider the references in their entireties, including those portions that have not been cited by the examiner and their equivalents as they may most broadly and appropriately apply to any particular anticipated claim amendments.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 02/03/2012 and 05/20/2013, has been reviewed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(a):
(a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly

connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), first paragraph:
The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 13-34 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Applicant's claiming "a deduction of the selection of minutia types from the challenge" in claims 13, 24 and 30; however, the specification does not fully disclose how the deduction is performed. Appropriate correction needed.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 13-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Based upon consideration of all the relevant factors with respect to the claim as a whole, claims 13-23 are held to claim an abstract idea, and are therefore rejected as

ineligible subject matter under 35 U.S.C. 101. The rationale for this finding is explained below:

Claim 13 is rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584,588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876). An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. **Claim 13** recites "selecting…, forming…, computing…, sending…, receiving.., comparing…" is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Thus the recited method is not tied to a particular machine or apparatus. Additionally, none of the recited steps transform a particular article into a different state or thing. Accordingly, the recited method is directed to nonstatutory subject matter. The mere recitation of the machine in the preamble with

an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.

Claims 14-23 are rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 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 13-14, 16-25, 27-30 and 32-34 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Colella (Pub. No.: US 2007/0174206 A1; hereafter Cole) in view of Buffam (Pat. No.: US 6,185,316 B1; hereinafter Buff).

Regarding **Claim 13**, Cole discloses a method comprising:

-selecting at least one type of minutia from a plurality of minutia types (selecting one of many minutia for authentication [Cole, ¶37, ¶41-¶42]);

-forming a challenge that conveys the selection of minutia types (a challenge is form with the selected minutia [Cole, ¶37, ¶41-¶42]);

-computing a plurality of pre-processed responses possible to receive from a valid device, wherein [Cole, ¶37, ¶41-¶42];

-each pre-processed response is computed using a key (each response are encrypted with a key [Cole, ¶37, ¶41-¶42]); and

-each key is computed using values that are possible for the selection of minutia types (the passcode is generated in part by the minutia [Cole, ¶37, ¶41-¶42]);

-sending the challenge to the device (the server prompts the user to identify themselves [Cole, ¶45]);

-receiving an actual response to the challenge from the device (receiving a response from the device [Cole, ¶45]), wherein:

-the actual response is computed using an actual key (response with the passcode encrypted and the same passkey [Cole, ¶47]);

-the actual key is computed using:

-a deduction of the selection of minutia types from the challenge (the passcode are divisible, which represent each segment of the fingerprint [Cole, ¶41]); and

-actual values of the selection of minutia types (the passcode are actual representation of the fingerprint [Cole, ¶41]);

-comparing the actual response to the pre-processed responses for a match (comparing the passcode with the stored passcode for matching [Cole, ¶47]); and

-based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types (if there is a match of passcode and fingerprint, the SIID is authorized and an authorization for perform the request [Cole, ¶42 & ¶47]). Cole might not clearly depict how the actual key is computed; however in a related and analogous art, Buff teaches these features.

Buff teaches a method to self-authentication using fingerprint [Buff, Abstract]. In particular, the encoding key is used to encrypt plaintext into ciphertext, and added the ciphertext

to the minutia points in the transient template, where each key representing a subset of the fingerprint; wherein the key is created from hashing the data point conditioner [Buff, fig. 1 and associated text]. It would have been obvious to one with ordinary skill in the art to modify Cole in view of Buff to computer the key based on the minutia type with the motivation for error correction.

Regarding **Claim 14**, Cole-Buff combination discloses choosing the selection of minutia from a plurality of minutia including hardware minutia, firmware minutia, software minutia, geo-location data, calling app data, user secrets, or biometric information (the SIID, passcode and biometric authentication [Cole, ¶42 & ¶47]).

Regarding **Claim 16**, Cole-Buff combination discloses choosing the selection of minutia according to a particular cataloging scheme of minutia (selecting the minutia of the fingerprint is based on the fingerprint scheme [Buff, 20:24-31, fig. 10]).

Regarding **Claim 17**, Cole-Buff combination discloses choosing the selection of minutia using expectations for changes to the current device image (selection of minutia based on changes in system parameters and policy [Buff, 22:22-37]).

Regarding **Claim 18**, Cole-Buff combination discloses choosing the selection of device minutia using knowledge of all industry updates that can occur on the device, whether or not

actually occurring on the device (selection of minutia based on changes in system parameters and policy [Buff, 22:22-37]).

Regarding **Claim 19**, Cole-Buff combination discloses choosing the selection of device minutia using knowledge of changes actually occurring on the device, wherein:

-changes actually occurring on the device are inferred from the pre-processed responses (the response is not prioritized [Cole, ¶47]), and

-no information about actual values of the minutia currently on the device is carried by the actual response to the challenge (only the passcode and fingerprint carried in the response [Cole, ¶47]).

Regarding **Claim 20**, Cole-Buff combination discloses choosing the selection of device minutia includes choosing triplets according to a cataloging scheme that varies from one issuer of the challenge to another (the challenge various based on the user's device [Cole, ¶45]).

Regarding **Claim 21**, Cole-Buff combination discloses using knowledge of the current device image to choose the selection of device minutiae (the challenge various based on the user's device [Cole, ¶45]).

Regarding **Claim 22**, Cole-Buff combination discloses using the actual response to update knowledge of the current device image (the challenge various based on the user's device [Cole, ¶45]).

Regarding **Claim 23**, Cole-Buff combination discloses wherein processing a range of possible changes to a current device image further comprises:

-pre-processing all possible responses from the device independently of receiving the actual response from the device (the response is pre-created which are independent from the actual receiving response [Cole, ¶41-¶42 and ¶47]).

The requirement of claims 24-25, 27-30 and 32-34 is substantially the same as the rejected claims 13-14 and 16-23.

Claims 15, 26 and 31 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Colella (Pub. No.: US 2007/0174206 A1; hereafter Cole) in view of Buffam (Pat. No.: US 6,185,316 B1; hereinafter Buff) further in view of Spitzig et al. (Pub. No.: US 2010/0027834 A1; hereinafter Spit).

Regarding **Claim 15, 26 and 31**, Cole-Buff combination does not explicitly discloses choosing the selection of minutia to be a triplet of computer minutia types including a hardware minutia H, a firmware minutia F, and a software minutia S; however, in a related and analogous art, Spit disclose this feature.

In particular, Spit discloses an executable module integrated to perform data processing in created minutiae of software, hardware and firmware [Spit, ¶29]. It would have been obvious to one with ordinary skill in the art at time of invention to modify Cole-Buff combination in view

of Spit to included software, hardware and firmware as minutiae with the motivation to perform authentication on various devices.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAO HO whose telephone number is (571) 270-5998. The examiner can normally be reached on Monday thru Thursday and 2nd Friday 8:00am - 6:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin can be reached on (571) 272-3862. 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.

/D. H./
Examiner, Art Unit 2493
09/22/2013

/Carl Colin/

Supervisory Patent Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 13/366,197	Applicant(s)/Patent Under Reexamination MILLER ET AL.	
	Examiner DAO HO	Art Unit 2493	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0174206 a1	07-2007	Colella, Brian	705/64
*	B	US-6,185,316 b1	02-2001	Buffam, William J.	382/115
*	C	US-2010/0027834 a1	02-2010	Spitzig et al.	382/100
	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	
	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.

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				*Complete if Known*	
				Application Number	13/366,197
				Filing Date	February 3, 2012
				Applicant(s)	Miller et al.
				Art Unit	2493
				Examiner Name	Ho, Dao Q.
SHEET	1	OF	1	Attorney Docket Number	47583.3

U. S. PATENT DOCUMENTS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		2011/0293094	12-01-2011	Os et al.
		2011/0296170	12-01-2011	Chen, Hu-Mu

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
		WO 2010/035202	04-01-2010	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Y

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published

Examiner Signature	/Dao Ho/	Date Considered	09/06/2013

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	Art Unit
	DAO HO	2493

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
380	255	09/22/2013	dqh

SEARCH NOTES		
Search Notes	Date	Examiner
see attached EAST search history	09/22/2013	dqh
inventor search in EAST	09/22/2013	dqh
class 380/255 with delimiter	09/22/2013	dqh
NPL: device authentiation using minutiae	09/22/2013	dqh

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/D.H./ Examiner.Art Unit 2493	

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			Complete if Known	
				Application Number	Herewith
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Filing Date	Herewith
				Applicant(s)	Paul Miller
				Art Unit	Not yet assigned
				Examiner Name	Not yet assigned
SHEET	1	OF	1	Attorney Docket Number	47583.3

U. S. PATENT DOCUMENTS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1	2011/0082768 A1	04-07-2011	Ori Eisen
	2	7,373,669 B2	05-13-2008	Ori Eisen
	3	2011/0113388 A1	05-12-2011	Eisen, et al.
	4	2008/0244744 A1	10-02-2008	Thomas, et al.
	5	2007/0214151 A1	09-13-2007	Thomas, et al.
	6	2007/024801 A1	05-31-2007	Thomas, et al.
	7	7,908,662 B2	03-15-2011	Ric B. Richardson
	8	2010/0229224 A1	09-10-2010	Craig S. Etchegoyen
	9	2009/0138975 A1	05-28-2009	Ric B. Richardson
	10	7,937,467 B2	05-03-2011	Timothy P. Barber
	11	7,330,871 B2	02-12-2008	Timothy P. Barber

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published

Examiner Signature	/Dao Ho/	Date Considered	09/06/2013

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /D.H./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	10	(US-20090310779-$ or US-20070174206-$ or US-20080175449-$ or US-20060104484-$ or US-20080235515-$ or US-20060031676-$ or US-20120201381-$).did. or (US-6185316-$ or US-6041133-$ or US-8375221-$).did.	US-PGPUB; USPAT	OR	OFF	2013/09/23 09:26
L3	4	2 and (firmware)	US-PGPUB; USPAT	OR	OFF	2013/09/23 09:26
L4	8	(minuti$3) with (firmware and hardware and software)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/23 09:30
L6	11	(US-20060031676-$ or US-20060104484-$ or US-20070174206-$ or US-20080175449-$ or US-20080235515-$ or US-20090310779-$ or US-20100027834-$ or US-20120201381-$).did. or (US-6041133-$ or US-6185316-$ or US-8375221-$).did.	US-PGPUB; USPAT	OR	OFF	2013/09/23 09:56
L7	9	6 and (chang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/09/23 09:56
S1	876	((PAUL) near2 (MILLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/06 11:24
S2	1	"13366197"	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/06 11:27
S3	11	("20070024801" | "20070214151" | "20080244744" | "20090138975" | "20100229224" | "20110082768" | "20110113388" | "7330871" | "7373669" | "7908662" | "7937467").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/06 11:27
S5	1647	380/255.ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/17 21:46
S6	34783	"380".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/09/17 21:47

S7	876	((PAUL) near2 (MILLER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/17 21:47
S8	2	S7 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/09/17 21:47
S10	11	("20070024801" | "20070214151" | "20080244744" | "20090138975" | "20100229224" | "20110082768" | "20110113388" | "7330871" | "7373669" | "7908662" | "7937467").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/17 22:07
S11	0	S10 and (minutia$)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/17 22:07
S13	4	(minutia$ with value with key)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/17 22:08
S14	11	("20070024801" | "20070214151" | "20080244744" | "20090138975" | "20100229224" | "20110082768" | "20110113388" | "7330871" | "7373669" | "7908662" | "7937467").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:20
S15	1	S14 and challenge	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:20
S16	38	(device near5 authenticat$5) with (minutia$2)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:25
S17	21	S16 and key	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:33
S18	1	(dynamic near4 key near4 crypto$7) same minutia$2	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:42
S19	101	(dynamic near4 key near4 crypto$7)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:43
S20	25	(device near5 authenticat$5) and S19	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 11:44
S22	26	minutia$2 with triplet	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 21:52
S23	1	(hardware near3 minutia$3) and (software near3 minutia$3) and (firmware near3 minutia$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/18 22:03
S24	465	(minuti$3 or fingerprint or manifest) with (firmware and hardware and software)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:03
S26	249	(minuti$3 or integrity) with (firmware and hardware and software)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:04

S27	1647	380/255.ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:04
S28	5	S27 and S26	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:04
S29	8	S26 and "6185678"	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:05
S33	68	S26 and ((minuti$3 integrity) near5 (firmware and hardware and software))	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:10
S35	101	(dynamic near4 key near4 crypto$7)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:11
S37	46	S33 and key	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:12
S38	38	(device near5 authenticat$5) with (minutia$2)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:14
S40	51935	(device near5 authenticat$5)	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:14
S41	21	S33 and S40	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:14
S43	1	S33 and triplet	US-PGPUB; USPAT; USOCR	OR	OFF	2013/09/19 11:17
S44	10	(US-20090310779-$ or US-20070174206-$ or US-20080175449-$ or US-20060104484-$ or US-20080235515-$ or US-20060031676-$ or US-20120201381-$).did. or (US-6185316-$ or US-6041133-$ or US-8375221-$).did.	US-PGPUB; USPAT	OR	OFF	2013/09/22 14:41
S46	3	S44 and ((deduct$3 remov$3) with minutia$3)	US-PGPUB; USPAT	OR	OFF	2013/09/22 14:42

EAST Search History (Interference)

<This search history is empty>

9/23/2013 10:21:19 AM
C:\Users\dho1\Documents\EAST\Workspaces\13366197.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13366197	MILLER ET AL.
	Examiner	Art Unit
	DAO HO	2493

✓	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	09/23/2013								
	1	N								
	2	N								
	3	N								
	4	N								
	5	N								
	6	N								
	7	N								
	8	N								
	9	N								
	10	N								
	11	N								
	12	N								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								

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. 5655

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/366,197	02/03/2012	380	2493	47583.3

APPLICANTS

Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/462,474 02/03/2011

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/16/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /DAO Q HO/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	11	34	4

ADDRESS

HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219
UNITED STATES

TITLE

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

FILING FEE RECEIVED		
1075	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).

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				*Complete if Known*	
				Application Number	13/366,197
				Filing Date	February 3, 2012
				Applicant(s)	Miller et al.
				Art Unit	2493
				Examiner Name	Ho, Dao Q.
SHEET	1	OF	1	Attorney Docket Number	47583.3

U. S. PATENT DOCUMENTS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		2011/0293094	12-01-2011	Os et al.
		2011/0296170	12-01-2011	Chen, Hu-Mu

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N
		WO 2010/035202	04-01-2010	KONIN-KLIJKE PHILIPS ELECTRONICS N.V.	Y

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published

Examiner Signature		Date Considered	

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

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Bowls, David B.
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219-7673
ETATS-UNIS D'AMERIQUE

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 47583-4	Date of mailing *(day/month/year)* 23 April 2013 (23-04-2013) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/022292	International filing date *(day/month/year)* 18 January 2013 (18-01-2013)
Applicant MSIGNIA, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Docketed: 5/2/13

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	KASTLOVA, Alena Tel: +49 (0)89 2399-2348 By:

Form PCT/ISA/220 (July 2010)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
47583-4		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/022292	18/01/2013	03/02/2012
Applicant		
MSIGNIA, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of:

   [X] 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))

   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant

   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**

   a. the figure of the **drawings** to be published with the abstract is Figure No. 1

   [ ] as suggested by the applicant

   [ ] as selected by this Authority, because the applicant failed to suggest a figure

   [X] as selected by this Authority, because this figure better characterizes the invention

   b. [ ] none of the figures is to be published with the abstract

Form PCT/ISA/210 (first sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/022292

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD.

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)
H04L

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)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010/035202 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; GUAJARDO MERCHAN JORGE [NL]; PETK) 1 April 2010 (2010-04-01) abstract page 1, line 1 - page 13, line 14 figures 1-6b	1-34
X	US 2011/293094 A1 (OS MARCEL VAN [US] ET AL) 1 December 2011 (2011-12-01) paragraphs [0055] - [0058]	1-34
X	US 2011/296170 A1 (CHEN HU-MU [TW]) 1 December 2011 (2011-12-01) abstract paragraphs [0002] - [0009], [0013] - [0039] figures 1,2	1-34

☐ 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 application or patent but 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	Date of mailing of the international search report
16 April 2013	23/04/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mariggis, Athanasios

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/022292

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010035202 A1	01-04-2010	CN 102165458 A	24-08-2011
		EP 2329423 A1	08-06-2011
		JP 2012503814 A	09-02-2012
		US 2011191837 A1	04-08-2011
		WO 2010035202 A1	01-04-2010
US 2011293094 A1	01-12-2011	NONE	
US 2011296170 A1	01-12-2011	TW 201143343 A	01-12-2011
		US 2011296170 A1	01-12-2011

Form PCT/ISA/210 (patent family annex) (April 2006)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2013/022292	18.01.2013	03.02.2012

International Patent Classification (IPC) or both national classification and IPC
INV. H04L9/08

Applicant
MSIGNIA, 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 and 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 usually 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 notifed 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.

Docketed: 5/2/13

By:

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Mariggis, Athanasios Telephone No. +49 89 2399-7118

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the 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 43bis.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 sequence listing filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ 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 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:

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)	Yes:	Claims	5, 7, 8, 10-12, 14-20, 26-28, 31-34
	No:	Claims	1-4, 6, 9, 13, 21-25, 29, 30
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-34
Industrial applicability (IA)	Yes:	Claims	1-34
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure:

D1: WO 2010/035202 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; GUAJARDO MERCHAN JORGE [NL]; PETK) 1 April 2010 (2010-04-01)

D2: US 2011/293094 A1 (OS MARCEL VAN [US] ET AL) 1 December 2011 (2011-12-01)

D3: US 2011/296170 A1 (CHEN HU-MU [TW]) 1 December 2011 (2011-12-01)

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of independent claims 1, 13, 24 and 30 is not new in the sense of Article 33(2) PCT.

2.1 Document D1 discloses, according to all features of independent claim 1 (the references in parentheses applying to this document), a method of dynamic key cryptography (see page 6, line 28 to page 7, line 24; figures 1, 4, 5 and 6b),

the method comprising:

- selecting a subset from a set of minutia[e] types (see page 7, lines 14 to 24; figure 6b);

- for a particular device, sending a challenge to the device (see page 7, lines 14 to 24; page 12, lines 24 to 30; figure 6b),

wherein:

-- the challenge includes information from which the device can collect actual values of minutia[e] corresponding to the selected subset of minutia[e] types in

order to form a cryptographic key (see page 6, line 28 to page 7, line 24; figures 1, 4, 5 and 6b);

-- the cryptographic key is never transmitted from the device across any communication channel (see page 6, line 28 to page 7, line 24; figures 1, 4, 5 and 6b); and

-- the cryptographic key is used to encrypt an actual response to the challenge (see page 13, lines 5 to 14; figures 1, 4, 5 and 6b);

- pre-processing a set of responses to the challenge based on tracking updates of minutia[e] from which the selected subset of minutia[e] types is selected (see page 8, line 8 to page 11, line 24; figures 1, 4, 5 and 6b),

wherein:

-- the set of pre-processed responses covers a range of all actual responses possible to be received from the particular device if the combination of the particular device with collected actual values of minutia[e] is valid (see page 8, line 8 to page 11, line 24; figures 1, 4, 5 and 6b);

- comparing the actual response from the particular device to the set of pre-processed responses (see page 8, line 8 to page 11, line 24; figures 1, 4, 5 and 6b); and

- validating the combination of the particular device with the collected actual values if the actual response is included in the set of pre-processed responses for the particular device (see page 8, line 8 to page 11, line 24; figures 1, 4, 5 and 6b).

Consequently, independent claim 1 is not novel over the disclosure of document D1 (Article 33(2) PCT).

2.2 It is furthermore noted that even if the applicant would interpret the disclosure of document D1 in a slightly different manner than the examiner has done in the above analysis, and based on his interpretations would come to the conclusion that there are differences between the subject-matter of present claim 1 and D1 which would then establish novelty, then these differences, even if they could be acknowledged as such, would only be of so minor nature that they could not be the basis for establishing the presence of any inventive step, as D1 discloses the same object and the same type of solution as the present

application, and claim 1 would, even with such a difference in interpretation, not meet the requirements of Articles 33(1) and 33(3) PCT.

2.3 For the sake of completeness, it is pointed out that documents D2 and D3 disclose in less detail, however, all the essential method steps of claim 1. In particular, see:

D2: Paragraphs [0055], [0056] and [0058].

D3: Abstract; paragraphs [0008], [0015], [0018] to [0021], [0026], [0036] and [0037]; figures 1 and 2.

2.4 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent method/apparatus claims 13, 24 and 30, which therefore are also considered not new or at least not inventive (Article 33(2) and (3) PCT).

3 The dependent claims do not contain any additional features, which either alone or in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to novelty or inventive step, because the subject-matter of these claims relates to minor design details and is either derivable from the cited prior art (see documents D1 to D3) or represents standard practice.

Filing a demand for international preliminary examination

In principle, the **WO/ISA** will be considered to be the written opinion of the International Preliminary Examining Authority (**IPEA**). Where the **WO/ISA** issued by the **EPO** as **ISA** gives a positive opinion on the international application and the invention to which it relates, filing a **demand** with the **EPO** as **IPEA** would normally be unnecessary, since a positive IPRP would anyway be established by the IB based on the WO/ISA (see also further below).

If the applicant wishes to file a **demand** (for example, to allow him to argue his case in international preliminary examination with regard to objections raised in a negative **WO/ISA** before the **IPEA** issues an **IPER**), this must be done before expiration of **3 months after the date of mailing of the ISR and WO/ISA** or **22 months after priority date,** whichever expires later (Rule 54*bis* PCT). Amendments under Art. 34 PCT can be filed with the IPEA, normally at the same time as filing the demand (Rule 66.1(b) PCT) or within the time limit set for reply to any written opinion issued during international preliminary examination by the **IPEA**.

If a **demand** is filed at the **EPO** as **IPEA** and no comments/amendments have been received by the time the **EPO** starts drawing up the **IPER** (Rule 66.4*bis* PCT), the **WO/ISA** will be transformed by the **IPEA** into an **IPER** (also called the **IPRP (Chapter II)** which would merely reflect the content of the **WO/ISA** (OJ 10/2011, 532). The **demand** can still be withdrawn (Art. 37 PCT).

Please also note that, when filing amendments under Art. 34 PCT, such amendments shall be accompanied by a letter which identifies the amendments made and also the basis for the amendments in the application as originally filed (Rule 66.8(a) PCT). Failure to comply with this requirement may result in the amendments being ignored in the **IPER (IPRP (Chapter II))**, see Rule 70.2(c-*bis*) PCT.

Filing a request for supplementary international search

The applicant may, with the **IB**, file a request for **supplementary international search** under Rule 45*bis*.1 PCT. The present **ISR** and **WO/ISA** may also be taken into account in the execution of that supplementary international search, provided that these are available to the Authority charged with this task before it starts the supplementary search (Rule 45*bis*.5 PCT).

This kind of request **cannot be filed specifying the ISA** who did the **international search**.

More information on this topic can be found in the **PCT Applicant's Guide**, Chapter 8 (http://www.wipo.int/pct/en/guide/ip08.html).

End of the international phase

Where no **demand** is filed, at the end of the international phase, the **IB** will transform the **WO/ISA** into the IPRP (PCT Chapter I) (Rule 44*bis* PCT), which will then be transmitted together with possible informal comments to the designated Offices. Where a demand is filed, the **WO/ISA** is not transformed into an **IPRP (Chapter I)** by the **IB**, but rather the **IPEA** will establish an **IPER**, (the IPER is the same as the IPRP (PCT Chapter II), see Rule 70.15 PCT).

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO/ISA)

General information

For all international applications, the competent International Searching Authority (**ISA**) will establish an international search report (**ISR**) accompanied by a written opinion of the International Searching Authority (**WO/ISA**). The **WO/ISA** may be responded to by

- filing informal comments with the **International Bureau of WIPO (IB)** (where no demand for international preliminary examination **(demand)** is filed)
- filing amendments under Art. 19 PCT (this can be done whether or not a **demand** is filed)
- filing amendments under Art. 34 PCT and/or formal observations in response to objections raised in the **WO/ISA** (where a **demand** *is* actually filed)

This document explains these possibilities.

Filing informal comments

After receipt of the **ISR and WO/ISA**, the applicant may file informal comments on the **WO/ISA, directly with the IB** (see International Search and Preliminary Examination Guidelines 2.15). These will be communicated to the designated/elected Offices, together with the International Preliminary Report on Patentability **(IPRP)** at 30 months from the priority date.

Amending claims under Art. 19 PCT

The applicant may file **amended claims** under Art. 19 PCT, **directly with the IB** by the later of the following dates:

- 2 months from the date of mailing of the **ISR** and the **WO/ISA**
- 16 months from the priority date

However, any such amendment received by the **IB** after the expiration of the applicable time limit shall be **considered to have been received on time** by the **IB**, if it reaches it **before** the technical preparations for international publication have been completed (the 15th day prior to the date of publication, see PCT Applicant's Guide, International Phase, 9.013).

For further information, please see Rule 46 PCT as well as form PCT/ISA/220.

Please also note that, when filing amended claims under Art. 19 PCT, such amendments shall be **accompanied by a letter** identifying the amendments made and also the basis for the amendments in the application as originally filed (Rule 46.5(b) PCT). Where a **demand** is filed, failure to comply with this requirement may result in the amendments being ignored in the International Preliminary Examination Report **(IPER)**, see Rule 70.2(c-*bis*) PCT.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2010 (01.04.2010)

PCT

(10) International Publication Number
WO 2010/035202 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2009/054120

(22) International Filing Date:
21 September 2009 (21.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08165202.6 26 September 2008 (26.09.2008) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUAJARDO MERCHAN, Jorge** [VE/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). **PETKOVIC, Milan** [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

(74) Agents: **VAN VELZEN, Maaike, M.** et al.; High Tech Campus 44, NL-5600 AE Eindhoven (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: AUTHENTICATING A DEVICE AND A USER

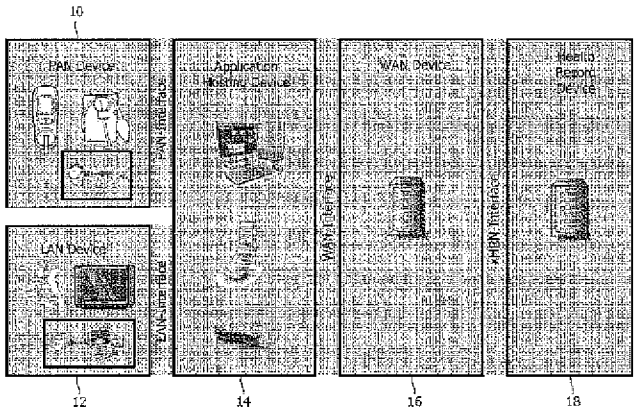

FIG. 1

(57) Abstract: A method of authenticating a device and a user comprises receiving a user input, generating a first key from the user input, performing a physical measurement of the device, obtaining helper data for the device, computing a second key from the physical measurement and the helper data, and performing an operation using the first and second keys. In a preferred embodiment, the method comprises performing a defined function on the first and second keys to obtain a third key. Additionally security can be provided by the step of receiving a user input comprising performing a biometric measurement of the user and the step of generating a first key from the user input comprises obtaining helper data for the user and computing the first key from the biometric measurement and the user helper data.

WO 2010/035202 A1

Authenticating a device and a user

FIELD OF THE INVENTION

This invention relates to a method of, and a system for, authenticating a device and a user. In one embodiment, the invention provides a combined device and patient authentication system for health services, especially those delivered as a part of a system in which the patient and healthcare provider are remote from one another and connected by an electronic system.

BACKGROUND OF THE INVENTION

An increasingly important trend in healthcare is one of consumer/patient involvement at all levels of healthcare. People are taking a more active role in their own health management. This trend of patient empowerment has already been widely supported. A number of solutions, (see for example, Capmed, http://www.phrforme.com/index.asp, Medkey, http://www.medkey.com/ and Webmd, http://www.webmd.com) have been introduced into the market that allow patients to collect their own health-related information and to store them on portable devices, computers, and in online services. These solutions are often referred to as Personal Health Record (PHR) services. Already a number of products in the market allow patients to enter automatically measurements and other medical data into their PHRs, see for example, Lifesensor, https://www.lifesensor.com/en/us/, and healthvault, http://search.healthvault.com/. For example a weight-scale sends its information via Bluetooth to a computer, from which the data is uploaded to a PHR. This allows patients to collect and manage their health data, but even more importantly to share the data with various healthcare professionals involved in their treatment.

Another important trend in healthcare is that the delivery of healthcare has gradually extended from acute institutional care to outpatient care and home care. Advances in information and communication technologies have enabled remote healthcare services (telehealth) including telemedicine and remote patient monitoring. A number of services in the market already deploy telehealth infrastructures where the measurement devices are connected via home hubs to remote backend servers. Health care providers use this architecture to remotely access the measurement data and help the patients. Examples are

disease management services (such as Philips Motiva and PTS) or emergency response services (Philips Lifeline).

Interoperability of measurement devices, home hubs and backend services becomes very important for enabling and further growth of this market. This need is recognized by the Continua health alliance, see http://www.continuaalliance.org, for example. As shown in Fig. 1, this initiative aim to standardize protocols between measurement devices, home hub (application hosting) devices, online healthcare/wellness services (WAN) and health record devices (PHRs/EHRs). In addition to data format and exchange issues, the Continua alliance is also addressing security and safety issues.

One of the basic security and safety problems in the domain of telehealth is the problem of user and device authentication/identification. Namely, when data remotely measured by patients is used by telehealth services or in the medical professional world, the healthcare providers need to place greater trust in information that patients report. In particular, they have to be ensured that a measurement is coming from the right patient and that appropriate device was used to take the measurement. Consider a blood pressure measurement; it is crucial to know that the blood pressure of a registered user is measured (not of his friends/children), and that the measurement was taken by a certified device and not a cheap fake device. This is very important, because otherwise there can result critical health care decisions based on wrong data.

In current practice, a device identifier (device ID) is either used as a user identifier (user ID) or as a means to derive a user ID (if multiple users are using the same device). For example, in the Continua system, as described in "Continua Health Alliance, Recommendations for Proper User Identification in Continua Version 1 – PAN and xHR interfaces (Draft v.01)", December 2007, at the PAN interface, as shown in Fig. 1, each Continua device is required to send its own unique device ID. The user ID is optional (and can be just simple as 1, 2, A, B). The valid user ID is obtained at the hub device (application hosting device), which can provide mapping between a simple user ID associated with a device ID to a valid user ID. There might be also measurement devices that can send a valid user ID next to the device ID. Then the mapping is not needed.

There are several problems with the current approach. For example, the current approach does not support authentication of users/devices, it only appends the user ID to the measurement. Data provenance is not established, as a healthcare provider later in the process cannot securely find which device was used to create the measurement. Next to that, the current mapping approach does not quickly lock the user and device ID together, but it

introduces room for mistakes. Either a user makes an unintended mistake (if manual mapping is required – the user has to select his ID (1 or A) at application hosting device or measurement device for each measurement) or the system can mix the users (the application designer should take special care to provide data management in a way to reduce the potential for associating measurements to the wrong user). In this type of arrangement, it is possible for a malicious user to introduce wrong measurements by impersonating the real user. Similarly, the device ID can be copied to forged devices, which can be easily introduced in the eco system. Then a user can use these devices to produce data that will look reliable but in fact will be unreliable.

It is therefore an object of the invention to improve upon the known art.

According to a first aspect of the present invention, there is provided a method of authenticating a device and a user comprising receiving a user input, generating a first key from the user input, performing a physical measurement of the device, obtaining helper data for the device, computing a second key from the physical measurement and the helper data, and performing an operation using the first and second keys.

According to a second aspect of the present invention, there is provided a system for authenticating a device and a user comprising a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component connected to the user interface and the query component, and arranged to generate a first key from the user input, to obtain helper data for the device, to compute a second key from the physical measurement and the helper data, and to perform an operation using the first and second keys.

According to a third aspect of the present invention, there is provided a method of registering a device and a user comprising receiving a user input, generating a first key from the user input, performing a physical measurement of the device, generating a second key and helper data for the device from the physical measurement, performing an operation using the first and second keys, and transmitting an output of the operation to a remote data store.

According to a fourth aspect of the present invention, there is provided a system for registering a device and a user comprising a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component arranged to generate a first key from the user input, to generate a second key and helper data for the device from the physical measurement, to perform an

operation using the first and second keys, and to transmit an output of the operation to a remote data store.

Owing to the invention, it is possible to bind the identity of a user and a device so as to certify that data originating from the device originates from the particular device and the particular user. This supports data quality assurance and reliability in personal healthcare applications. In this system, there is delivered a method to bind the identity of a user and a device identifier as early as possible, so as to certify that data originating from the device originates from the particular device and the particular user. To ensure proper device and user authentication/identification it is possible to use a Physically Uncloneable Function (PUF, described in detail below) in combination with a user input.

As a result there is covered the three problems from the prior art by providing respectively, close coupling of the user ID and the identification of the device used to take the measurement (the use of unregistered device/user is immediately detected), strong user authentication and anti-counterfeiting and strong device authentication. This has the following benefits, patient safety (diagnosis and health decisions are based on reliable data), reduction of costs (reuse of patient provided data in the consumer health and the professional healthcare domain) and convenience for the patient (they can take healthcare measurements at home).

In a preferred embodiment, the step of receiving a user input comprises performing a biometric measurement of the user and the step of generating a first key from the user input comprises obtaining helper data for the user and computing the first key from the biometric measurement and the user helper data. The user of a biometric measurement, such as a fingerprint, increases the security of the system and ensures that any data taken from an individual is authenticated as being from that specific individual, when the data is analyzed by a remote health system.

Advantageously, the method comprises performing a defined function on the first and second keys to obtain a third key. The security of the system can be increased if the two keys, one from the device and one from the user are combined together to create a third key, prior to any transmittal to a remote location. The combination can be performed according to a function of both inputs. Such function can be for example: (i) the concatenation of both strings, the XORing of both strings, the concatenation of both strings and subsequent hashing of the resulting string, the XORing of both strings and then hashing the resulting string, the encryption of one string according to an encryption algorithm (e.g.

the Advanced Encryption Standard) using as key one of the strings and as plaintext the second string, etc.

In a further embodiment, the step of receiving a user input comprises receiving a password and the step of generating a first key from the user input comprises computing the first key from the password. Rather than using biometric data, a simple password can be used to authenticate the user. Although this does not have the highest level of security associated with using the biometric data, this still provides a system that is an improvement over current known systems.

Ideally, the step of obtaining helper data for the device comprises computing the helper data from the first key and a stored component. The key for the device (the second key) is created from the physical measurement performed on the device and the helper data. If the helper data is reconstructed from the first key (from the user) and some stored component, then the security of the system of authenticating the device and user is increased, because the helper data is never stored in the clear.

Advantageously, the method further comprises obtaining a user share, obtaining a device share, and performing a defined function on the user share, device share, first and second keys to obtain a third key. The use of a user share and device share allows more than one device to be authenticated to a specific user, which increases the efficiency of the registration and authentication system.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 is a schematic diagram of a healthcare system,

Fig. 2 is a further schematic diagram of the healthcare system,

Fig. 3 is a schematic diagram of a device and user authentication system,

Fig. 4 is a flowchart of a registration procedure,

Fig. 5 is a flowchart of an authentication procedure,

Fig. 6a is a schematic diagram of a preferred embodiment of the authentication system, and

Fig. 6b is a further schematic diagram of a preferred embodiment of the authentication system, and

Fig. 7 is a schematic diagram of a further embodiment of the system.

DETAILED DESCRIPTION OF THE EMBODIMENTS

An example of a healthcare system is shown in Fig. 1. Various PAN (personal area network) devices 10 are shown such as a wristwatch and a blood pressure measuring device, which directly measure physiological parameters of a user. Additionally LAN (local area network) devices 12 are provided such as a treadmill which can also be used to gather healthcare information about the user. The PAN devices 10 and the LAN devices 12 are connected via suitable interfaces (wired and/or wireless) to an appropriate application hosting device 14, such a computer or mobile phone, which will be local to the PAN and LAN devices 10 and 12. This hosting device 14 will be running a suitable application which can gather and organize the outputs from the various PAN and LAN devices 10 and 12.

The application hosting device 14 is connected to a WAN (wide area network) device 16 such as a server. The WAN connection can be via a network such as the Internet. The server 16 is also connected via a suitable interface to a health record device 18, which is maintaining a health record for the users of the system. As discussed above, it is of paramount importance that the data recorded by the individual health records stored by the device 18 is assigned, firstly to the correct user, and additionally, that the device which recorded the data is known with absolute certainty. It is also advisable that the relevant PAN or LAN device 10 or 12 is also approved for use in the system.

Fig. 2 illustrates the system of Fig. 1, with a user 20 who is taking a measurement with a PAN device 10. Through the home hub 14, data can be communicated to the remote record device 18, which is maintaining the patient's record 22. The remote record device 18 also communicates directly with a GP record 24. In this example, the user 20 has wrongly identified themselves to the device 10, and is also using an incorrect device 10, for the measurement that they are trying to make. In a conventional system, this will result in an incorrect entry being made in their record 22, and could cause an incorrect alert to be raised with respect to the patient's condition.

In order to prevent the kind of error that is illustrated by Fig. 2, the system according to the present invention is summarized in Fig. 3. This Figure. shows a device 10 and the user 20, communicating with the remote healthcare device 18. The essential principle is that a key is derived from the user 20 and a key is derived from the device 10, and, in one embodiment, these are combined together and transmitted to the remote server 18 as a third key. The user 20 could supply a password, or in the preferred embodiment, there is performed a biometric measurement of the user 20 (such as a fingerprint) and the user key is

generated from this biometric measurement. The key from the device 10 is derived from a physical measurement of the device. One method of achieving this is to use a function known as a PUF, described below.

The system of Fig. 3 for authenticating the device 10 and the user 20 comprises a user interface arranged to receive a user input, a query component arranged to perform a physical measurement of the device, and a processing component connected to the user interface and the query component, and arranged to generate a first key from the user input, to obtain helper data for the device, to compute a second key from the physical measurement and the helper data, and to perform an operation using the first and second keys. These three components, the user interface, the query component and the processing component could all be contained within the device 10, or could be distributed amongst different devices. Indeed the functions of the processing component could be split between different processors contained in different devices.

A Physical Uncloneable Function (PUF) is a function that is realized by a physical system, such that the function is easy to evaluate but the physical system is hard to characterize and hard to clone, see for example R. Pappu, "Physical One-Way Functions", Ph.D. thesis, MIT, 2001. Since a PUF cannot be copied or modeled, a device equipped with a PUF becomes uncloneable. Physical systems that are produced by an uncontrolled production process (i.e. that contains some randomness) are good candidates for PUFs. The PUF's physical system is designed such that it interacts in a complicated way with stimuli (challenges) and leads to unique but unpredictable responses. A PUF challenge and the corresponding response are together called a Challenge-Response-Pair. It is possible for a PUF to have a single challenge, or a limited (small) number of challenges (less than 32 for example), or a large number of challenges (2^n challenges for n>5).

One example of a PUF is the so-called SRAM PUFs. As far as experiments have shown today, these PUFs are present on any device having an SRAM on board. It is based on the phenomenon that when an SRAM cell is started up, it starts up in a random state. However, when this is done multiple times, the SRAM starts up, most of the time, in the same state and can therefore be used as a type of PUF. S-RAM PUFs are described in more detail in ID685102. Other PUFs include an optical PUF, disclosed in the above reference and a delay PUF (see Gassend et al., Su et al. – IC PUFs (Delay PUF) CCS 2002, ACSAC 2002).

As previously mentioned, PUF responses are noisy and not fully random. Thus, a Fuzzy Extractor or Helper Data Algorithm (see J.-P. M. G. Linnartz and P. Tuyls,

"New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," in Audio-and Video-Based Biometrie Person Authentication — AVBPA 2003, ser. LNCS, J. Kittler and M. S. Nixon, Eds., vol. 2688. Springer, June 9-11, 2003, pp. 393–402 and Y. Dodis, M. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Advances in Cryptology —- EUROCRYPT 2004, ser. LNCS, C. Cachin and J. Camenisch, Eds., vol. 3027. Springer-Verlag, 2004, pp. 523–540.) is required to extract one (or more) secure keys from the PUF responses.

In the following, there is provided the intuition behind the algorithms. A fuzzy extractor requires two basic primitives, firstly information reconciliation or error correction and secondly privacy amplification or randomness extraction, which guarantees an output which is very close to being a uniformly distributed random variable. In order to implement those two primitives, helper data W is generated during the enrolment or registration phase. Later, during the key reconstruction or authentication phase, the key is reconstructed based on a noisy measurement Ri and the helper data W. During the enrolment phase (carried out in a trusted environment), a probabilistic procedure called Gen is run. This procedure takes as its input a PUF response R, and produces as output a key K and helper data W: $(K,W) \leftarrow Gen(R)$. In order to generate the helper data W, an error correcting code C is chosen such that at least t errors can be corrected. The number of errors to be corrected depends on the particular application and on the PUF properties.

Once an appropriate code has been chosen, the helper data W is generated by first choosing a random code word C_S from C and computing $W1 = C_S \oplus R$. Furthermore a universal hash function (see L. Carter and M. N. Wegman, "Universal Classes of Hash Functions," J. Comput. Syst. Sci., vol. 18, no. 2, pp. 143–154, 1979) h_i is chosen at random from a set H and the key K is defined as $K \leftarrow h_i(R)$. The helper data is then defined as $W = (W1, i)$. During the key reconstruction phase a procedure called Rep is run. It takes as input a noisy response R' and helper data W and reconstructs the key K (if R' originates from the same source as R) i.e. $K \leftarrow Rep(R',W)$. Reconstruction of the key is achieved by computing $C_S' = W1 \oplus R'$, decoding C_S' to C_S via the decoding algorithm of C, recovering $R = C_S \oplus W1$, and finally computing $K = h_i(R)$. The present method will work also with other types of helper data. For example, instead of XORing, it is possible to also perform a permutation.

It should be noted that the symbol $\oplus$ is used to indicate an XOR operation. The logical operation exclusive disjunction, also called exclusive or (XOR), is a type of logical disjunction on two operands that results in a value of "true", if and only if, exactly one of the operands has a value of "true".

Fuzzy extractor construction can also be used to generate unique identifiers or keys from biometric data. Instead of having a PUF response, there is used a person's biometric data. This can be further enhanced by computing the hash (say SHA-2) of K (where $K = h_i(R)$, and R is a biometric measurement). See T. Kevenaar, G.J. Schrijen, A. Akkermans, M. Damstra, P. Tuyls, M. van der Veen, Robust and Secure Biometrics: Some Application Examples. ISSE 2006 for an overview of different applications of this construction and Kevenaar, T.A.M, Schrijen, G.J., van der Veen, M., Akkermans, A.H.M. and Zuo, F.: Face Recognition with Renewable and Privacy Preserving Templates. Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2005), 17-18 Oct. 2005 Page(s): 21 – 26 for an example applied to biometrics based on face recognition.

As previously mentioned, the system of the present invention is designed to link a measurement to both a device ID and the particular user. A stable device ID can be derived from a PUF response and associated helper data. The helper data can be chosen randomly from code words of an error correcting code. In a preferred embodiment, the helper data is derived from both an error correcting code and from a string derived from a biometric measurement of the user. By constructing such helper data, it is possible to authenticate both the device and the user at once.

In a preferred embodiment, it is assumed that the following are available on the device that is being used, a PUF such that when challenge with Ci produces a response Ri, which is written as Ri ← PUF(Ci), a GenPUF algorithm which upon getting a PUF response Ri outputs (Ki,Wi), with (Ki,Wi) ← GenPUF(Ri), a RepPUF algorithm which upon getting a PUF response Ri' and helper data Wi outputs the key Ki if Ri and Ri' are sufficiently close, with Ki ← RepPUF(Ri',Wi), a GenBio algorithm which upon getting a biometric measurement BMu from user U outputs (Ku,Wu), with (Ku,Wu) ← GenBio(BMu), and a RepBio algorithm which upon getting a biometric measurement BMu from user U and helper data Wu outputs the key Ku if BMu and BMu' are sufficiently close, Ku ← RepBio(BMu',Wu). It is assumed that the device that is used to perform the measurements has a PUF embedded in it. This can be easily expected from any device containing, for example an SRAM memory, such as any microprocessor or microcontroller. Clearly, the algorithms GenPUF, GenBio, RepPUF, and RepBio can be implemented on the device but do not have to. They could be implemented on a second device. The first option is better from the security stand point. However, the second option makes it possible to implement the system for devices with limited processing capabilities.

Fig. 4 shows how the system would work in relation to a preferred embodiment of the registration procedure. Firstly, a group of users has a device i which measures some signal of users U1, U2, U3, …, Un. Prior to using the device for the first time, one of the users (Uj) runs the procedure GenPUF on the PUF of device i and obtains (Ki,Wi) ← GenPUF(Ri) corresponding to a response Ri originating from device i. This is the step S1 of the process. Note that this step does not need to be run by device i. In particular, this procedure can be run by a separate entity. The only thing needed by the entity to run GenPUF is the response Ri.

At the second step S2, the helper data Wi is stored in non-volatile memory of device i. An individual user, user Uj runs GenBio on his/her biometric (such as a fingerprint) and obtains Kuj, which is step S3. At step S4, this value is XORED with Wi to produce Wi,uj, which is stored in the device in user's Uj memory profile space, at step S5. In other words, Wi,uj = Wi XOR Kuj. A database is stored in the device with entries as follows: (Kuj; Wi,uj). The next step is step s6, in which for the user Uj there is computed a key Kij as a function of Ki and Kuj, written Kij ← f(Ki,Kuj). At step S7, this key is transmitted in a secure manner to the health service provider. Steps 3 to 7 are repeated for every user who wants to use the device. An alternative to storing the pairs (Kuj; Wi,uj) in the device's database is to store a pair (Uj, Wi,uj). This assumes that the user has a string Uj that identifies him. This is more secure since the key Kuj is not stored in the device but reconstructed every time that is needed. The string Uj can be any identifying information such as the name of the user, his social security number, driver's license number, email address, etc.

In summary, the method of registering a device and a user comprising receiving the user input (which could be a biometric measurement or a password), generating the first key from the user input, performing a physical measurement (such as a PUF) of the device, generating a second key and helper data for the device from the physical measurement, performing an operation using the first and second keys, and transmitting an output of the operation to a remote data store.

A preferred embodiment of an authentication procedure is shown in Fig. 5. The procedure is used after the user and device have registered, as per the flowchart of Fig. 4. User Uj desires to use device i to perform a measurement. Before being able to operate the device, the first step S1, is that the user Uj runs Kuj ← RepBio(BMuj',Wuj) and recovers Kuj. At step S2, the device i searches in its database for a match with Kuj. If it finds such a

match it continues to step 3, otherwise the device stops and tells the user to register first, in order to be able to use device i.

If there is a match, then at step S3, the device i XORs Kuj with Wi,uj to obtain Wi = Wi,uj XOR Kuj, followed by step S4, in which the device i runs Ki ← RepPUF(Ri',Wi) to recover Ki. At step S5, the device i computes a function of Ki and Kuj, written f(Ki,Kuj) resulting in a string Kij and, at step S6 the device i computes a Message Authentication Code (MAC) on the data measured with secret key Kij. Finally, at step S7, the device i sends the data and the MAC to the health service provider. The health service provider verifies the MAC and if the verification succeeds the data is accepted.

In this way a secure method of authenticating a device and a user is delivered. Neither the physical function of the device (in the preferred embodiment the PUF) nor the data from the user (in the preferred embodiment the biometric data) can be cloned or faked in any way, and the transmittal of these keys (or a single key derived from them both) to the health service provider allows both the device and user to be authenticated.

An alternative solution (Embodiment 2) to that provided by the procedures of flowcharts 4 and 5 is to perform separate authentication of the device and the patient and then combine these identifiers/keys or send them separately to the service provider. For example, it is possible to derive Ki from PUF, then derive Kuj from the user's biometrics and then combine the keys into a single key: Kij = Hash(Ki||Kuj). Based on this key (Kij) a MAC or a signature on the data can be computed before being sent to the service provider. However, this would fail to identify, in the beginning, a user that has not run the registration procedure before using the measuring device for the first time (i.e. the user has to register a new key, for each new device he obtains; and this registration has to be done with all service providers and/or health service infrastructures that use his data).

Other variations of the preferred embodiment are also possible. For example, the device does not perform the key reconstruction itself, but rather sends the measured signal together with a PUF response Ri' to a more powerful device, for example the home hub 14 in Fig. 2, where all the processing is performed. Note that in this particular case, there is no concern over the secrecy of the response. Rather the system is only interested in making sure that there is the correct data associated with the correct user and device.

The methodology above could also be adapted so that instead of computing a helper data Wi,uj, the device could simply store Wi and then compute Kij as the XOR of Ki and Kuj. However, this would fail to identify in the beginning a user that has not run the registration procedure before using the measuring device for the first time.

Another alternative could be that instead of using a symmetric-key based system the system can use an asymmetric key based system. Instead of considering Kij as a symmetric key, the system can use the secret-key of a public-key based system. Then in step S7 of the registration procedure (Fig. 4), instead of sending Kij to the service provider, the device can send the public-key associated with a secret-key Kij. This can be easily computed for typical public-key based systems.

In one embodiment there is performed a defined function on the first key from the user and the second key from the device to obtain a third key (Kij). The function used to compute Kij from Ki and Kuj could be, for example, a hash (SHA-1, SHA-2, MD5, RipeMD, etc.) of the concatenation of Ki and Kuj, an XOR of Ki and Kuj, an encryption of a constant string using as key Ki and Kuj, and encryption of Ki using Kuj as the encryption key of an encryption system, an encryption of Kuj using Ki as the encryption key of an encryption system, a value derived from a 2-out-n threshold scheme where two of the shares correspond to Ki and Kuj (see below for additional advantages of using threshold schemes), or any other function of Ki and Kuj appropriate for the application.

The preferred embodiment of the invention is shown in Fig. 6a and Fig. 6b. In Fig. 6a a processor 30 is connected to a device 10 and a user input device 32. The device 10 is a device for measuring the blood pressure of the user, and the user input device 32 is a device for measuring the fingerprint of the user, when the user places their finger into the device. The system of this Figure assumes that the registration process has already taken place and the user has performed the measurement of their blood pressure with the device 10. The user wishes to authenticate the acquired data prior to sending that acquired data to the third party health service provider.

Fig. 6b illustrates the actions taken by the processor 30. The user input 34, being a biometric measurement of the user's fingerprint is received by the processor 30, from the user input device 32. The PUF 36 is also received from a query applied to the device 10. Within the system is present a query component which makes a PUF query to the device 10. This component (not shown) could be built in within the device 10. The user input 34 is combined with user helper data 38 to generate a first key 40, and the PUF 36 is combined with device helper data 42 to generate a second key.

In this Figure, the key generation processes are shown as independent, but they could be configured in such a way that the key from one side is used to generate the helper data on the other side, and vice versa, as an extra security feature, using an additional stored component. The generation of the two keys 40 and 44 could occur simultaneously, or

in the case where the key of one is used to generate the helper data of the other, then the generation would occur sequentially. Either key could be generated first. The reference to the user's key as the first key 40 does not mean that it is the first key to be generated by the processor 30.

After the keys 40 and 44 have been generated then they are passed to an operation stage 46, which performs an operation using the two keys 40 and 44. This operation could take a number of different forms. In the simplest embodiment, the operation is the transmission of the two keys 40 and 44, with the acquired data about the user's blood pressure, to the third party service provider. Another option would be to combine the two keys 40 and 44 into a third key and transmit this third key with the data. A third option would be to encrypt the user's health data with either the two keys 40 and 44, or using something (such as a hash function output) derived from the two keys 40 and 44. Another option would be the generation of a digital signature using the keys 40 and 44 to sign the data before it is sent. In this way the data gathered by the user is authenticated using the two keys 40 and 44.

The key Kuj derived from the user, which in the preferred embodiment is a biometric measurement, could be derived from a password for example. The intent is to make the key that is used to sign dependent on something that User Uj has to provide or enter into the system. It does not necessarily have to be a biometric, although this would make it less likely to be vulnerable to impersonation attacks. This embodiment is shown in Fig. 7.

In this embodiment, the user 20 provides a user input which is a password 28. The device 10 generates a key from the password, and also performs a physical measurement of the device (using a PUF). The device accesses the helper data for the device and computes a second key from the physical measurement and the helper data, as discussed in detail above. The device then transmits the first and second keys (or a third key derived from these two keys) to the health service provider 18.

The system can also be adapted to generating a single per user key from multiple devices. In this embodiment, there is provided an approach that uses only one key per patient/user regardless of the number of devices that are used for obtaining data (in contrast to previous embodiments where one key per each user-device combination was necessary). For this construction it is possible to use threshold secret sharing, which is described in the following.

Threshold secret-sharing is described in Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997. A (t,n) threshold scheme (t<=n) is a method by which a trusted party computes secret shares S_i,

$1 <= i <= n$ from an initial secret S, and securely distributes S_i to user P_i, such that the following is true: any t or more users who pool their shares may easily recover S, but any group knowing only $t - 1$ or fewer shares may not. A perfect threshold scheme is a threshold scheme in which knowing only $t - 1$ or fewer shares provide no advantage (no information about S whatsoever, in the information-theoretic sense) to an opponent over knowing no shares.

Shamir's threshold scheme is based on polynomial interpolation, and the fact that a univariate polynomial $y = f(x)$ of degree $t - 1$ is uniquely defined by t points $(x_i; y_i)$ with distinct x_i (since these define t linearly independent equations in t unknowns). The coefficients of an unknown polynomial f(x) of degree less than t, defined by points $(x_i; y_i)$, $1 <= i <= t$, are given by the Lagrange interpolation formula:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j}.$$

Since $f(0) = a0 = S$, the shared secret may be expressed as:

$$S = \sum_{i=1}^{t} c_i y_i, \quad \text{where } c_i = \prod_{1 \le j \le t, j \ne i} \frac{x_j}{x_j - x_i}.$$

Thus each group member may compute S as a linear combination of t shares y_i, since the c_i are non-secret constants (which for a fixed group of t users may be pre-computed). Below is shown Shamir's (t,n) threshold scheme. Shamir's threshold scheme is provided as an example, however, other threshold secret sharing schemes can also be used, for example, Oded Goldreich, Dana Ron, Madhu Sudan: "Chinese remaindering with errors" IEEE Transactions on Information Theory 46(4): 1330-1338 (2000).

Mechanism Shamir's (t, n) threshold scheme

SUMMARY: a trusted party distributes shares of a secret S to n users.
RESULT: any group of t users which pool their shares can recover S.

1. *Setup.* The trusted party T begins with a secret integer $S \geq 0$ it wishes to distribute among n users.
   (a) T chooses a prime $p > \max(S, n)$, and defines $a_0 = S$.
   (b) T selects $t-1$ random, independent coefficients $a_1, \ldots, a_{t-1}, 0 \leq a_j \leq p-1$, defining the random polynomial over $\mathbb{Z}_p$, $f(x) = \sum_{j=0}^{t-1} a_j x^j$.
   (c) T computes $S_i = f(i) \bmod p$, $1 \leq i \leq n$ (or for any n distinct points i, $1 \leq i \leq p-1$), and securely transfers the share S_i to user P_i, along with public index i.
2. *Pooling of shares.* Any group of t or more users pool their shares (see Remark 12.70). Their shares provide t distinct points $(x, y) = (i, S_i)$ allowing computation of the coefficients a_j, $1 \leq j \leq t-1$ of $f(x)$ by Lagrange interpolation (see below). The secret is recovered by noting $f(0) = a_0 = S$.

Using Shamir's Threshold scheme it is possible to combine several keys (in this particular case two keys) to generate a single key as follows. This uses a 2-out-n threshold scheme as follows. The user computes a different key Ki for every device as has been described in the previous embodiments. The user also computes a key based on his biometric Kuj. The user defines a 2-out-n threshold scheme as follows:

The user chooses a prime p large enough such that Ki < p and Kuj < p. Alternatively, it is possible to choose a prime p large enough for security purposes, and based on this, compute strings Ki' and Kuj', which (when interpreted as integers) are less than p. One possible way to compute such strings is simply as Ki' = Hash(Ki) mod p and Kuj' = Hash(Kuj) mod p, for some hash function Hash. The user chooses a random key Kij such that 2 <= Kij <= p-1, and sets a0 = Kij. The user then chooses one independent and random coefficient a1 such that 1<= a1 <= p-1. Note that a1 must be non-zero (in contrast to the general Shamir's threshold scheme). The user computes a share Yuj as follows: Yuj = a1*Kuj' + a0. The user stores in device i Yuj (Yuj is the same for all devices). The user then computes a share Yi for device i as follows: Yi = a1*Ki' + a0. The user stores in device i Yi. The Yi is device dependent. This is repeated for every device i that the user wants to use.

If the system supports only symmetric-key authentication then the key Kij (corresponding to a0) is sent to the service provider. If the system is public-key based then a corresponding public key is derived using a0 as the secret key of the system and the public-key is sent to the service provider via a secure and authenticated channel. To provide the authentication in such a system, the user obtains their biometric dependent key and obtains a user share (Kuj', Yuj). The device computes its key Ki (by any of the methods described

above which might include the use of the user's biometric as well) and obtains a device share (Ki, Yi) for device i. Using Lagrange interpolation the key Kij is reconstructed from the two shares. The user uses Kij to compute a MAC or a signature on the data being sent to the service provider.

There are several advantages of the proposed system. Most importantly, the system allows for early coupling of device and user identifiers that can be obtained by strong authentication (for example using PUFs and biometrics). In the preferred embodiment, the key derivation is performed in one step which leads to higher reliability.

Furthermore, the system is advantageous because there it is necessary to register with the service provider only a single key per user. This supports separation of duties. The service provider or health service infrastructure does not have to take care of registration of measurement devices. A TTP (Trusted Third Party), such as a Continua certification centre, can perform the registration in a way that for each device a user has, the combined device/user key is the same, as described in the final embodiment. The TTP certifies the key which is registered by service providers and health service infrastructure. This is much simpler than continuously registering with the service provider the keys of each device the user has and will obtain (which is required by traditional approaches). Additionally, at the service provider and health service infrastructure site, the key management is much simpler as they have to deal with far fewer keys. They do not have to change much current practice of using one identifier/key per patient. Finally, depending on the embodiment chosen for the implementation, it is possible to identify a user which has not been registered before, which also contributes to the reliability of the measured data.

Next to that, there are important advantages of biometrics over other authentication approaches. Most importantly, some physiological measurements could serve a dual purpose. For example, measuring patient's vital signs (for example ECG) and at the same time using the measurement for patient authentication (biometric data can be extracted from the physiological measurement such as ECG). This methodology couples the measurement to the patient as strongly as possible. In addition, biometric data is more convenient and secure than a passwords or smartcards that can be forgotten or lost. Biometric data provides a stronger type of authentication when compared to smartcards or passwords, which can be easily handed over to other people.

CLAIMS:

1. A method of authenticating a device (10) and a user (20) comprising:
- receiving a user input (28, 34),
- generating a first key (40) from the user input (28, 34),
- performing a physical measurement (36) of the device (10),
- obtaining helper data (42) for the device (10),
- computing a second key (44) from the physical measurement (36) and the helper data (44), and
- performing an operation (46) using the first and second keys (40, 44).

2. A method according to claim 1, wherein the step of performing an operation (46) using the first and second keys (40, 44) comprises performing a defined function on the first and second keys (40, 44) to obtain a third key.

3. A method according to claim 1 or 2, wherein the step of receiving a user input (28) comprises receiving a password (28) and the step of generating a first key (40) from the user input (28) comprises computing the first key (40) from the password (28).

4. A method according to claim 1 or 2, wherein the step of receiving a user input (34) comprises performing a biometric measurement (34) of the user (20) and the step of generating a first key (40) from the user input (34) comprises obtaining helper data (38) for the user (20) and computing the first key (40) from the biometric measurement (34) and the user helper data (38).

5. A method according to claim 4, wherein the step of obtaining helper data (42) for the device (10) comprises computing the helper data (42) from the first key (40) and a stored component.

6. A method according to any preceding claim, and further comprising obtaining a user share, obtaining a device share, and performing a defined function on the user share, device share, first and second keys (40, 44) to obtain a third key.

7. A system for authenticating a device (10) and a user (20) comprising:
- a user interface (32) arranged to receive a user input (28, 34),
- a query component arranged to perform a physical measurement (36) of the device (10), and
- a processing component (30) connected to the user interface (32) and the query component, and arranged to generate a first key (40) from the user input (28, 34), to obtain helper data (42) for the device (10), to compute a second key (44) from the physical measurement (36) and the helper data (42), and to perform an operation (46) using the first and second keys (40, 44).

8. A system according to claim 7, wherein the processing component (30) is arranged, when performing an operation (46) using the first and second keys (40, 44), to perform a defined function on the first and second keys (40, 44) to obtain a third key.

9. A system according to claim 7 or 8, wherein the user input (28) comprises a password (28) and the processing component (30) is arranged, when generating a first key (40) from the user input (28), to compute the first key (40) from the password (28).

10. A system according to claim 7 or 8, wherein the user input (34) comprises a biometric measurement (34) of the user (20) and the processing component (30) is arranged, when generating a first key (40) from the user input (34), to obtain helper data (38) for the user (20) and to compute the first key (40) from the biometric measurement (34) and the user helper data (38).

11. A system according to claim 10, wherein the processing component (30) is arranged, when obtaining helper data (42) for the device (10), to compute the helper data (42) from the first key (40) and a stored component.

12. A system according to any one of claims 7 to 11, wherein the processing component (30) is further arranged to obtain a user share, obtain a device share, and to

perform a defined function on the user share, device share, first and second keys (40, 44) to obtain a third key

13. A system according to any one of claims 7 to 12, wherein the user interface, the query component and the processing component are contained within a single device.

14. A system according to any one of claims 7 to 12, wherein the user interface (32), the query component (10) and the processing component (30) are distributed across a plurality of devices.

15. A method of registering a device (10) and a user (20) comprising:

- receiving a user input (28, 34),
- generating a first key (40) from the user input (28, 34),
- performing a physical measurement (36) of the device (10),
- generating a second key (44) and helper data (42) for the device (10) from the physical measurement (36),
- performing an operation (46) using the first and second keys (42, 44), and transmitting an output of the operation (46) to a remote data store.

16. A method according to claim 15, wherein the step of receiving a user input (34) comprises performing a biometric measurement (34) of the user (20) and the step of generating a first key (40) from the user input (34) includes generating helper data (38) for the user (20).

17. A system for registering a device (10) and a user (20) comprising:

- a user interface (32) arranged to receive a user input (28, 34),
- a query component arranged to perform a physical measurement (36) of the device (10), and
- a processing component (30) arranged to generate a first key (40) from the user input (28, 34), to generate a second key (44) and helper data (42) for the device (10) from the physical measurement (36), to perform an operation (46) using the first and second keys (40, 44), and to transmit an output of the operation (46) to a remote data store.

18. A system according to claim 17, wherein the user input (34) comprises a biometric measurement (34) of the user (20) and the processing component (30) is further arranged, when generating a first key (40) from the user input (34), to generate helper data (38) for the user (20).

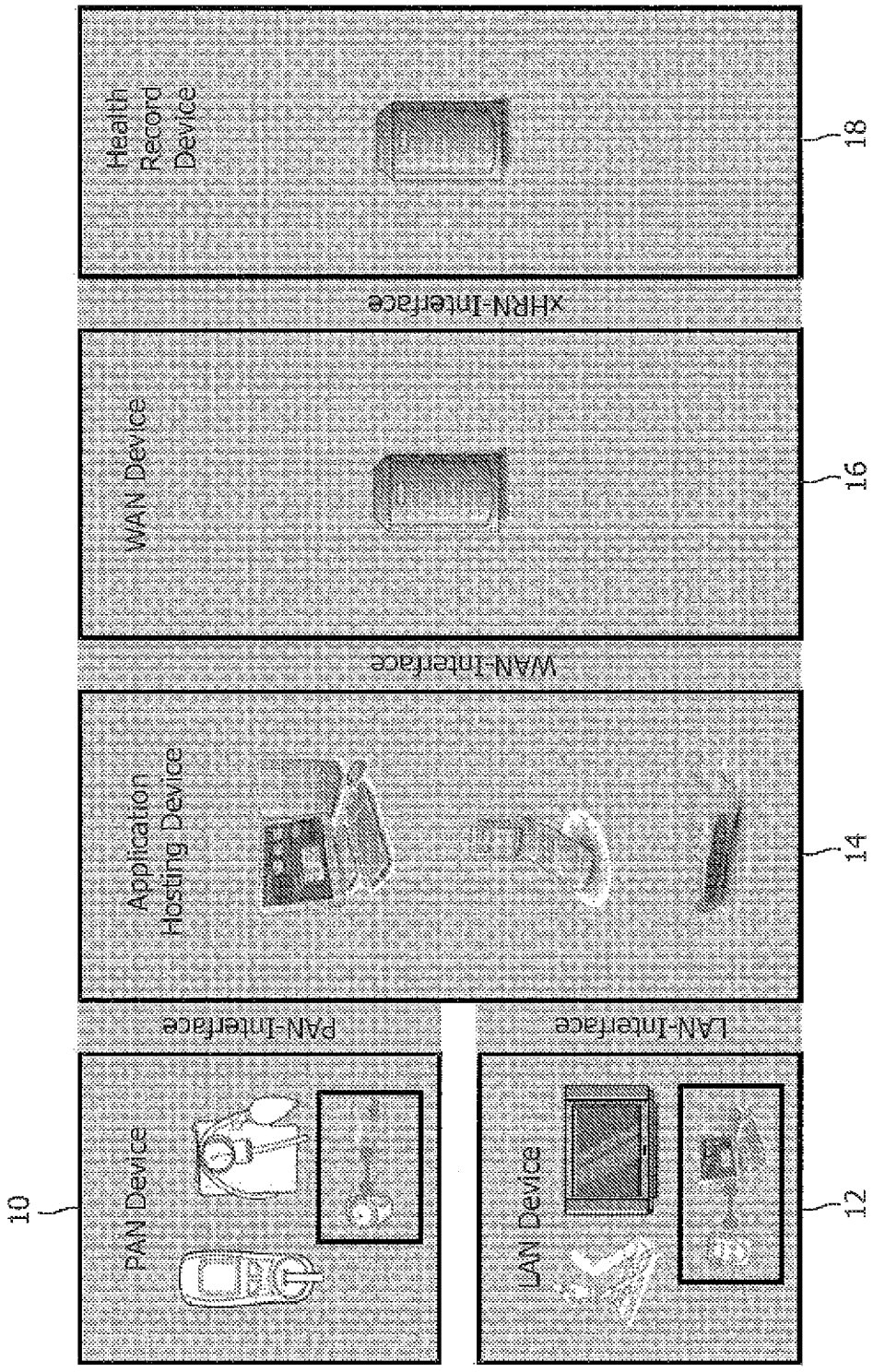
Health Record Device
18
xHRN-Interface
WAN Device
16
WAN-Interface
Application Hosting Device
14
PAN-Interface
LAN-Interface
PAN Device
LAN Device
10
12

FIG. 1

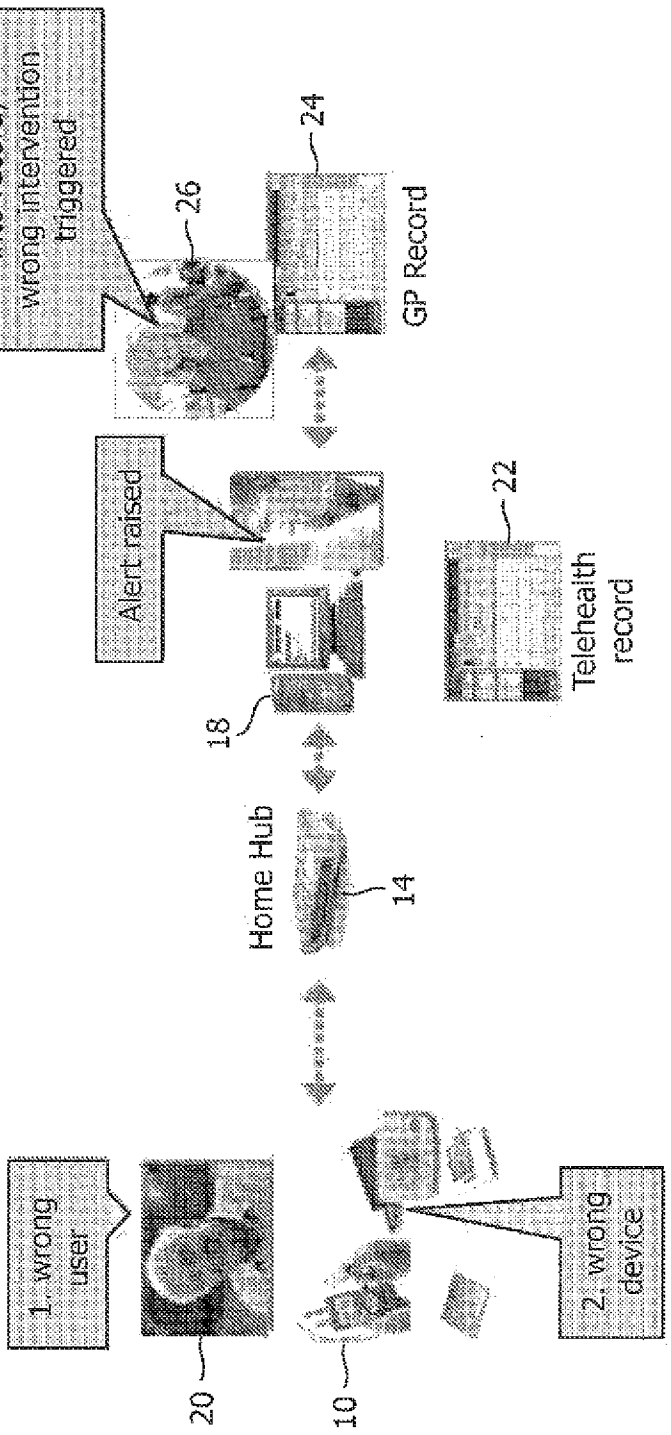
1. wrong user
2. wrong device
Home Hub
14
18
Alert raised
Reading entered into record; wrong intervention triggered
26
24
GP Record
22
Telehealth record
20
10

FIG. 2

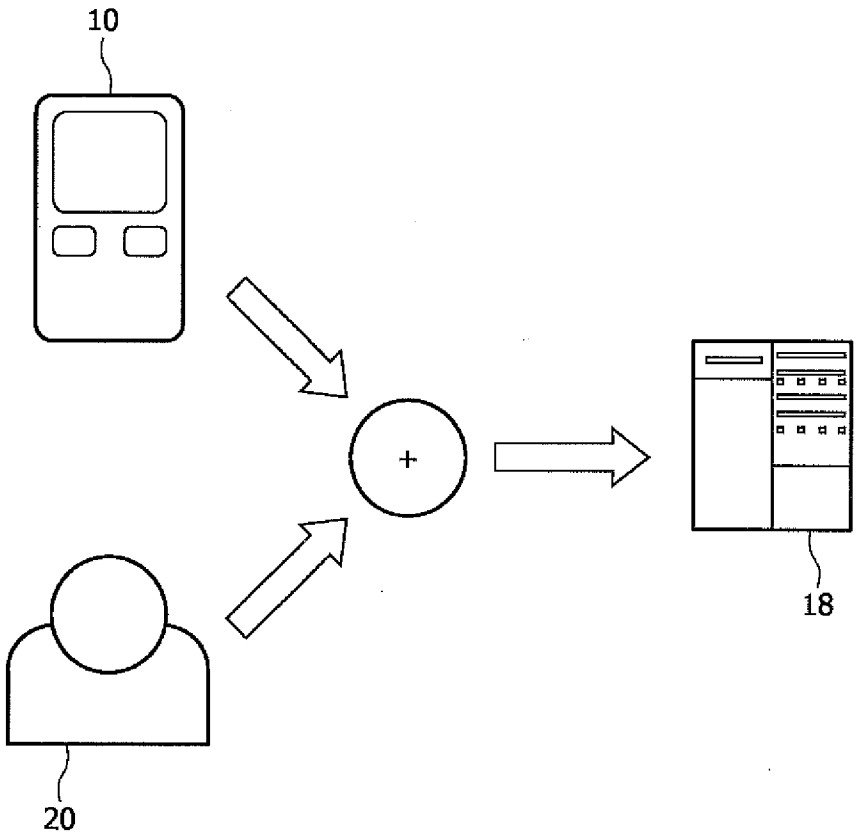

FIG. 3

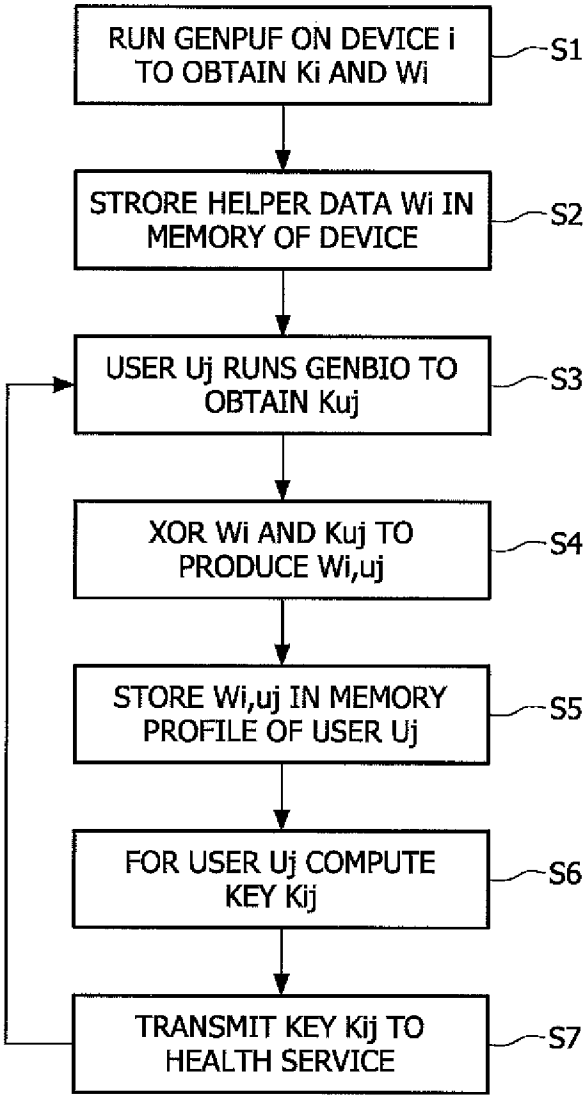
RUN GENPUF ON DEVICE i TO OBTAIN Ki AND Wi
S1
STRORE HELPER DATA Wi IN MEMORY OF DEVICE
S2
USER Uj RUNS GENBIO TO OBTAIN Kuj
S3
XOR Wi AND Kuj TO PRODUCE Wi,uj
S4
STORE Wi,uj IN MEMORY PROFILE OF USER Uj
S5
FOR USER Uj COMPUTE KEY Kij
S6
TRANSMIT KEY Kij TO HEALTH SERVICE
S7

FIG. 4

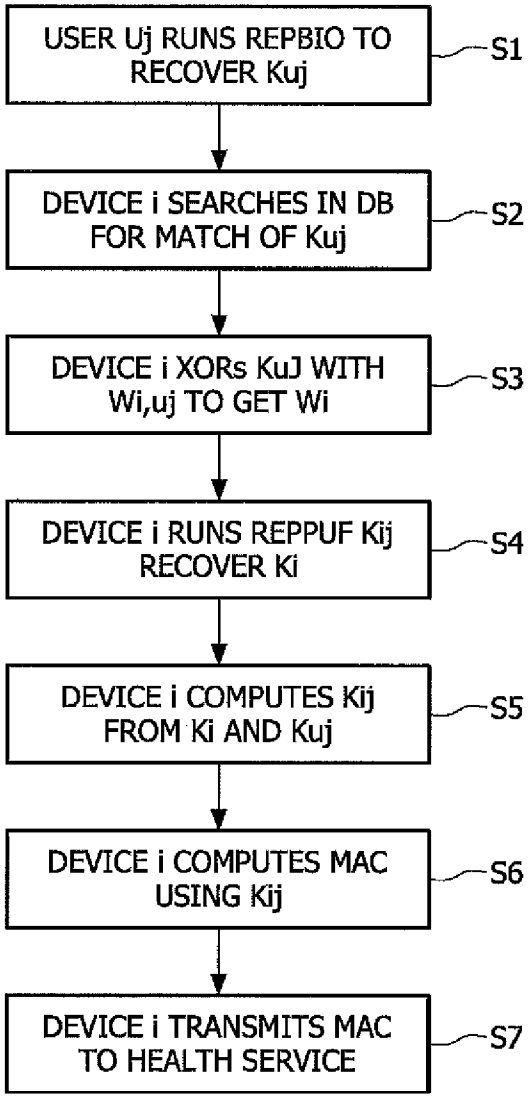
USER Uj RUNS REPBIO TO RECOVER Kuj
S1
DEVICE i SEARCHES IN DB FOR MATCH OF Kuj
S2
DEVICE i XORs KuJ WITH Wi,uj TO GET Wi
S3
DEVICE i RUNS REPPUF Kij RECOVER Ki
S4
DEVICE i COMPUTES Kij FROM Ki AND Kuj
S5
DEVICE i COMPUTES MAC USING Kij
S6
DEVICE i TRANSMITS MAC TO HEALTH SERVICE
S7

FIG. 5

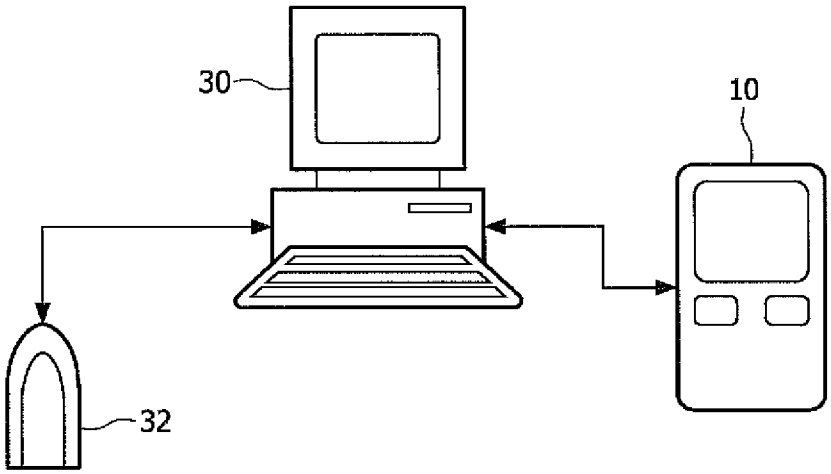
30
10
32

FIG. 6a

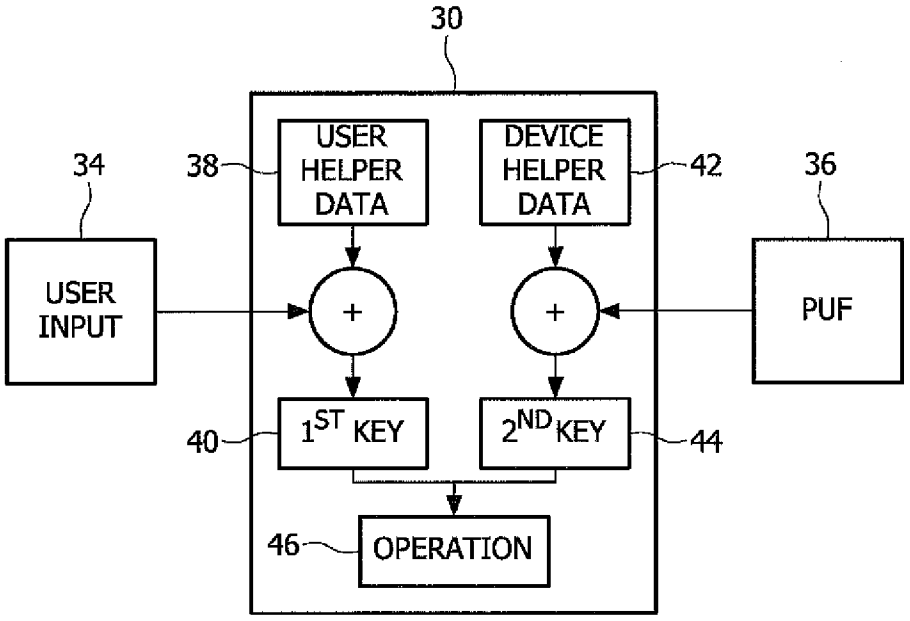
30
34
38
USER HELPER DATA
DEVICE HELPER DATA
42
36
USER INPUT
+
+
PUF
40
1ST KEY
2ND KEY
44
46
OPERATION

FIG. 6b

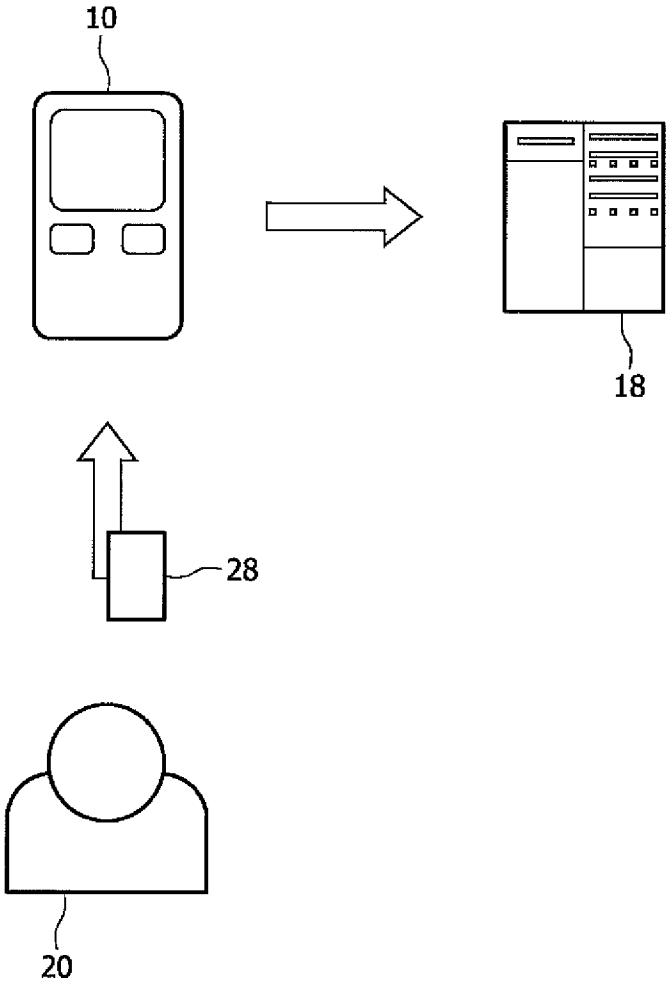

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/054120

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)
G06F

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 practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/044139 A1 (TUYLS PIM T [NL] ET AL) 22 February 2007 (2007-02-22) paragraph [0026] - paragraph [0052]; figures 1, 2A, 2B	1-18
Y	WO 2007/063475 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; SKORIC BORIS [NL]; BRUEKERS ALPHO) 7 June 2007 (2007-06-07) page 3, line 1 - page 3, line 15	1-18
A	WO 2006/067739 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; TUYLS PIM T [BE]; GOSELING JASPER) 29 June 2006 (2006-06-29) abstract	1-18

[ ] Further documents are listed in the continuation of Box C.

[X] 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 but 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	Date of mailing of the international search report
12 February 2010	19/02/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jascau, Adrian

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2009/054120

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007044139 A1	22-02-2007	CN 1792060 A	21-06-2006
		WO 2004104899 A2	02-12-2004
		JP 2007500910 T	18-01-2007
		KR 20060023533 A	14-03-2006
WO 2007063475 A2	07-06-2007	AT 426969 T	15-04-2009
		CN 101317361 A	03-12-2008
		EP 1958374 A2	20-08-2008
		JP 2009517911 T	30-04-2009
		US 2008260152 A1	23-10-2008
WO 2006067739 A2	29-06-2006	JP 2008526078 T	17-07-2008
		KR 20070095908 A	01-10-2007

Form PCT/ISA/210 (patent family annex) (April 2005)

Electronic Acknowledgement Receipt

EFS ID:	15823056
Application Number:	13366197
International Application Number:	
Confirmation Number:	5655
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul Timothy Miller
Customer Number:	27683
Filer:	David B. Bowls/Pia Kamath
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.3
Receipt Date:	20-MAY-2013
Filing Date:	03-FEB-2012
Time Stamp:	17:44:54
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		IDSTransmittalandForm.pdf	228330 66e3124fb9ed0e326611a78346e93fdeeb93bc91	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:					
Information:					
2	Non Patent Literature	ISRReference.pdf	603770 9b47e4406dbe7d05557983023777ca1c3cda5edd	no	11
Warnings:					
Information:					
3	Foreign Reference	ForeignRef.pdf	1630903 50545fc1e2f09a12a6beaecae47b89bc387995dc	no	30
Warnings:					
Information:					
		Total Files Size (in bytes):	2463003		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Paul Timothy Miller and George Allen Tuvell		
Assignee:	mSIGNIA, Inc.		
Title:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Application No.:	13/366,197	Filing Date:	February 3, 2012
Examiner:	Ho, Dao Q.	Group Art Unit:	2493
Docket No.:	47583.3	Confirmation No.:	5655

Irvine, California
May 20, 2013

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. §§1.56, 1.97, and 1.98

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97, and 1.98, the documents listed on the attached form PTO/SB/08A and/or PTO/SB/08B are called to the attention of the Examiner for the above patent application. The documents were cited in an International Search Report mailed April 23, 2013 in corresponding PCT Patent Application No. PCT/US2013/022292. A copy of the Search Report is also enclosed for the Examiner's review.

Citation of these documents shall not be construed as:

(1) an admission that the documents are necessarily prior art with respect to the instant invention;

(2) a representation that a search has been made, other than as described above; or

(3) an admission that the information cited herein is, or is considered to be material to patentability.

Haynes and Boone, LLP
18100 Von Karman
Suite 750
Irvine, CA 92612
Tele: (949) 202-3000
Fax: (949) 202-3001

Enclosed with this statement are the following:

☒ Form PTO/SB/08A and/or PTO/SB/08B. The Examiner is requested to initial the form and return it to the undersigned in accordance with M.P.E.P. §609.

☒ A copy of each cited document as required by 37 C.F.R. §1.98 (*except where otherwise indicated*).

Complete copies are not submitted of U.S. patents and U.S. patent application publications per 37 C.F.R. §1.98(a)(2)(ii), and copies are not submitted of documents already cited or submitted in a parent application from which benefit under 35 U.S.C. §120 is claimed per 37 C.F.R. §1.98(d).

This statement should be considered because:

☒ This statement qualifies under 37 C.F.R. §1.97, subsection (b) because:

- ☐ It is being filed within 3 months of the application filing date of a national application other than a continued prosecution application under §1.53(d);
  -- OR --
- ☐ It is being filed within 3 months of entry of the national stage as set forth in §1.491 in an international application;
  -- OR --
- ☒ It is being filed before the mailing date of a first Office action *on the merits*;
  -- OR --
- ☐ It is being filed before the mailing date of a first Office action *after the filing of an RCE under §1.114.*

whichever occurs last.

☒ Although it may not qualify under subsection (b), this statement qualifies under 37 C.F.R. §1.97, subsection (c) because:

(1) It is being filed before the mailing date of a FINAL Office Action and before a Notice of Allowance or another action closing prosecution (whichever occurs first);
-- AND *(check at least one of the following)* --

- ☐ (1) It is accompanied by the $180 fee set forth in 37 C.F.R. §1.17(p);
  -- OR --
- ☒ (2) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure statement was first cited in a 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.

--OR--

- ☐ (3) Pursuant to 37 C.F.R. §1.97(e), no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart

Haynes and Boone, LLP
18100 Von Karman
Suite 750
Irvine, CA 92612
Tele: (949) 202-3000
Fax: (949) 202-3001

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 § 1.56(c) more than three months prior to the filing of the information disclosure statement.

☐ Although it may not qualify under subsections (b) or (c), this statement qualifies under 37 C.F.R. §1.97, subsection (d) because:

(1) Pursuant to 37 C.F.R. §1.97(e), each item of information contained in the information disclosure Statement was first cited in a 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;

-- AND --

(2) It is accompanied by the fee set forth in 37 C.F.R. §1.17(p);

-- AND --

(3) It is filed on or before payment of the Issue Fee.

☒ ***Fee Authorization.*** The Commissioner is hereby authorized to charge any additional fee(s), charge any underpayment of fee(s), or credit any overpayment associated with this communication to Deposit Account No. 08-1394.

Certificate of Transmission

I hereby certify that this correspondence is sent electronically via EFS Web to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

May 20, 2013

Pia S. Kamath

Respectfully submitted,

David B. Bowls
Reg. No. 39,915

Haynes and Boone, LLP
18100 Von Karman
Suite 750
Irvine, CA 92612
Tele: (949) 202-3000
Fax: (949) 202-3001

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
13/366,197	02/03/2012	Paul Timothy Miller	47583.3

CONFIRMATION NO. 5655

PUBLICATION NOTICE

27683
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

OC000000055871948

Title:CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Publication No.US-2012-0201381-A1
Publication Date:08/09/2012

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.

Office of Data Managment, 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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/366,197	02/03/2012	2431	1075	47583.3	34	4

CONFIRMATION NO. 5655

27683
HAYNES AND BOONE, LLP
IP Section
2323 Victory Avenue
Suite 700
Dallas, TX 75219

FILING RECEIPT

Date Mailed: 02/22/2012

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 submit a written request for a Filing Receipt Correction. 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)

Paul Timothy Miller, Irvine, CA;
George Allen Tuvell, Thompson's Station, TN;

Assignment For Published Patent Application

mSignia, Inc., Irvine, CA

Power of Attorney: The patent practitioners associated with Customer Number 27683

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/462,474 02/03/2011

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 02/16/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/366,197**

Projected Publication Date: 08/09/2012

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Preliminary Class

380

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).

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/366,197

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	34 minus 20 =	* 14	x 30 =	420	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x 125 =	125			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 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).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1075		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	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	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	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 found in the appropriate box in column 1.

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	Herewith
				Filing Date	Herewith
				Applicant(s)	Paul Miller
				Art Unit	Not yet assigned
				Examiner Name	Not yet assigned
SHEET	1	OF	1	Attorney Docket Number	47583.3

U. S. PATENT DOCUMENTS				
Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	1	2011/0082768 A1	04-07-2011	Ori Eisen
	2	7,373,669 B2	05-13-2008	Ori Eisen
	3	2011/0113388 A1	05-12-2011	Eisen, et al.
	4	2008/0244744 A1	10-02-2008	Thomas, et al.
	5	2007/0214151 A1	09-13-2007	Thomas, et al.
	6	2007/024801 A1	05-31-2007	Thomas, et al.
	7	7,908,662 B2	03-15-2011	Ric B. Richardson
	8	2010/0229224 A1	09-10-2010	Craig S. Etchegoyen
	9	2009/0138975 A1	05-28-2009	Ric B. Richardson
	10	7,937,467 B2	05-03-2011	Timothy P. Barber
	11	7,330,871 B2	02-12-2008	Timothy P. Barber

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published

Examiner Signature		Date Considered	

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul T. Miller
Filer:	David B. Bowls/Pia Kamath
Attorney Docket Number:	47583.3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
Pages:				
Claims:				
Claims in excess of 20	2202	14	30	420
Independent claims in excess of 3	2201	1	125	125
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1075**

Electronic Acknowledgement Receipt

EFS ID:	12000582
Application Number:	13366197
International Application Number:	
Confirmation Number:	5655
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul T. Miller
Customer Number:	27683
Filer:	David B. Bowls/Pia Kamath
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.3
Receipt Date:	03-FEB-2012
Filing Date:	
Time Stamp:	20:06:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1075
RAM confirmation Number	6249
Deposit Account	081394
Authorized User	BOWLS,DAVID B.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	UtilityPatentTransmittal.pdf	83093 f7ad9b48fc399794765dd2dde9111fb8a7ce4a70	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	FeeTransmittal.pdf	83348 8d03a894b3dfd458ed883062d3c528fe87e6a58e	no	1
Warnings:					
Information:					
3	Application Data Sheet	ApplicationDataSheet.pdf	283138 dedb75f41b9d2f8a72a7b465eb2a569985e20a72	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
4		Application.pdf	3518483 affa766187d40fea5f5e6b1f18f64657c9580b67	yes	57

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	48
Claims	49	56
Abstract	57	57

Warnings:					
Information:					
5	Drawings-only black and white line drawings	FormalDrawings.pdf	458282 0532d5439a51dd6379fe4fe8c5dc08ff6a567036	no	11
Warnings:					
Information:					
6	Oath or Declaration filed	DeclarationandPOA.pdf	157431 f9d1ce93b4b22add2599402ba47d87fe97993e3a	no	2
Warnings:					
Information:					

7	Information Disclosure Statement (IDS) Form (SB08)	InformationDisclosureStatement.pdf	63054 bf5b19763ad1b402823947ccdc53b26ee6fa3bee	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Fee Worksheet (SB06)	fee-info.pdf	38139 603b04100c3b679041e40789641ae8ab85249fdb	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	4684968	

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:	12000582
Application Number:	13366197
International Application Number:	
Confirmation Number:	5655
Title of Invention:	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE
First Named Inventor/Applicant Name:	Paul T. Miller
Customer Number:	27683
Filer:	David B. Bowls/Pia Kamath
Filer Authorized By:	David B. Bowls
Attorney Docket Number:	47583.3
Receipt Date:	03-FEB-2012
Filing Date:	
Time Stamp:	20:06:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1075
RAM confirmation Number	6249
Deposit Account	081394
Authorized User	BOWLS,DAVID B.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	UtilityPatentTransmittal.pdf	83093 f7ad9b48fc399794765dd2dde9111fb8a7ce4a70	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	FeeTransmittal.pdf	83348 8d03a894b3dfd458ed883062d3c528fe87e6a58e	no	1
Warnings:					
Information:					
3	Application Data Sheet	ApplicationDataSheet.pdf	283138 dedb75f41b9d2f8a72a7b465eb2a569985e20a72	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
4		Application.pdf	3518483 affa766187d40fea5f5e6b1f18f64657c9580b67	yes	57

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	48
Claims	49	56
Abstract	57	57

Warnings:					
Information:					
5	Drawings-only black and white line drawings	FormalDrawings.pdf	458282 0532d5439a51dd6379fe4fe8c5dc08ff6a567036	no	11
Warnings:					
Information:					
6	Oath or Declaration filed	DeclarationandPOA.pdf	157431 f9d1ce93b4b22add2599402ba47d87fe97993e3a	no	2
Warnings:					
Information:					

7	Information Disclosure Statement (IDS) Form (SB08)	InformationDisclosureStatement.pdf	63054 bf5b19763ad1b402823947ccdc53b26ee6fa3bee	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Fee Worksheet (SB06)	fee-info.pdf	38139 603b04100c3b679041e40789641ae8ab85249fdb	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	4684968	

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/05 (08-08)
Approved for use through 01/31/2014. 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.	47583.3
First Inventor	Paul T. Miller
Title	Cryptographic Security Functions...
Express Mail Label No.	Electronically Filed

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☑ **Fee Transmittal Form** (e.g., PTO/SB/17)
2. ☑ **Applicant claims small entity status.** See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages* 57]
   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* 11]
5. **Oath or Declaration** [*Total Sheets* 2]
   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

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

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.: .....

Prior application information: *Examiner* _____ *Art Unit:* _____

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 27683 ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	David Bowls	Date	Feb 3, 2012
Name (Print/Type)	David Bowls	Registration No. (Attorney/Agent)	39,915

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.

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 1075.00

Complete if Known	
Application Number	Herewith
Filing Date	Herewith
First Named Inventor	Paul T. Miller
Examiner Name	Not yet assigned
Art Unit	Not yet assigned
Attorney Docket No.	47583.3

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☐ Deposit Account Deposit Account Number: _____ Deposit Account Name: _____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

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.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	530.00
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
34 - 20 or HP =	14	x 30.00	= 420.00

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
4 - 3 or HP =	1	x 125.00	= 125.00

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Fee Paid ($)

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 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).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
- 100 =	/ 50 =	(round **up** to a whole number)	x	=

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge):	

SUBMITTED BY

Signature	David Bowls	Registration No. (Attorney/Agent) 39,915	Telephone (949) 202-3000
Name (Print/Type)	David Bowls		Date February 3, 2012

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.3
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

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
	Paul	Timothy	Miller	

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

City	Irvine	State/Province	CA	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i] US

Mailing Address of Applicant:

Address 1	10 Wandering Rill		
Address 2			
City	Irvine	State/Province	CA
Postal Code	92603	Country[i]	US

Applicant 2

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
	George	Allen	Tuvell	

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

City	Thompson's Station	State/Province	TN	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i] US

Mailing Address of Applicant:

Address 1	2617 Clayton Arnold Road		
Address 2			
City	Thompson's Station	State/Province	TN
Postal Code	37179	Country[i]	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.**

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.3
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

Customer Number	27683		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE		
Attorney Docket Number	47583.3	**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)	11	**Suggested Figure for Publication (if any)**	

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 and will not** be the subject of an application filed in another country, or under a multilateral international 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	○ Limited Recognition (37 CFR 11.9)
Customer Number	27683		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. 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)
instant	non provisional of	61/462474	2011-02-03

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	47583.3
	Application Number	
Title of Invention	CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE	

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.

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	mSignia, Inc.		
Mailing Address Information:			
Address 1	10 Wandering Rill		
Address 2			
City	Irvine	**State/Province**	CA
Country [i]	US	Postal Code	
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	/David Bowls/			Date (YYYY-MM-DD)	2012-02-03
First Name	David	Last Name	Bowls	Registration Number	39915

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.**

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 the Freedom of Information Act requires disclosure of these records.

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 inspections 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.

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

Paul T. Miller, George A. Tuvell

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application No. 61/462,474 filed February 3, 2011, which is incorporated by reference.

BACKGROUND

Technical Field

The present disclosure generally relates to dynamic key cryptography used, for example, for authentication between a client electronic device and a service provider, encryption of data communications, and digital signatures and, more particularly, to cryptography using dynamic keys derived from dynamically changing key material.

Related Art

Use of computers for connecting to a network (such as the Internet) and communicating with a variety of services risks the privacy of many types of information belonging to a user including, for example, the user's relationships (e.g., social connections), business secrets, banking details, payment options, and health records. The use of cryptography is common to authenticate identities, protect data, and digitally sign the summary (i.e. digest) of an action.

Cryptography generally uses an algorithm (e.g., Advanced Encryption Standard (AES), Rivest Shamir Adelman (RSA)) to combine cryptographic keys (which may be symmetric, public, or private, for example) with plain text to form cipher text. Cryptography keys are typically random numbers without any special meaning. The process of distributing cryptographic keys and storing them on a client computer (referred to as "key management") is difficult to perform securely and is often the point-of-attack for breaking the security of a cryptographic system. The key represents a single sequence of data and thus a single point-of-failure for the cryptographic system. Since the key normally must be present at the client

computer, finding the key and then copying it to another computer can allow an imposter entity to masquerade as a valid entity.

Secure elements (e.g., smartcards) can securely store the cryptographic key and, in some instances, generate the key in a secure environment. Access to the key was typically controlled by requiring the user to enter a personal identification number (PIN); this ensured that the user had to provide a secret before the secure element would allow use of the key. Such access to a key is commonly known as two-factor authentication, and the two factors are generally referred to as: "Something You Know" and "Something You Have". A third factor, "Something You Are", can include, for example, biometric information. The factors themselves are related in use but entirely separate in material. Possession of the physical secure element ("Something You Have") may be via validation of cryptographic functions using the random number cryptographic key provisioned to a particular secure element whose use may be protected by a secret PIN ("Something You Know"). There is no implicit binding between the key and the user.

The use of certificates in cryptography enabled the binding of a distinguished name (e.g., a unique user) with a cryptographic key. Yet, still the cryptographic key is a random number, and when the key is validated, the cryptographic system attributes the user in the certificate to the usage of the key; the key matter itself has no relation to the user.

On the Internet, ensuring a real-world identity for the user is critical for protecting data and privacy. Mobile users especially are at risk because they often do not use anti-virus applications and many of the service providers use applications (apps) optimized for simplicity, not security. This leaves much of the private data meaningful to both a user's identity and a service's value inadequately protected. Since online service providers (OSP) incur much of the risk, safety has become their responsibility.

The standard method for identifying a user to an online service is by entering a username and password. The username is a known service index and, as such, can be stored on the computer for convenience. The password is a user secret verifiable by the OSP; it should not be stored at the computer, where it can be compromised. However, because a quality password has many characters which should be a mix of upper, lower, punctuation and special characters, the password is often difficult and time-consuming to type. This is especially true on a mobile computer using touch keypads that have various 'levels' of

keypads for characters beyond simple alpha-numeric. Thus, many mobile apps store the password on the computer. Because mobile operating systems require mobile apps to be signed in order to run, the apps themselves cannot be altered after installation. So, any data stored by the mobile app is separate from the mobile app and often can be vulnerable to attack. Furthermore, because the app cannot change, if encryption was used to protect the cached password, there could only be one encryption key for all instances of the application. This commonality made harvesting and cracking stored passwords on a mobile computer relatively simple, even if the passwords were encrypted, since they all used the same key for decryption.

Computer and computer identification has been attempted by calculating a hash of the minutia found on a computer to uniquely identify the computer, often referred to as a computer fingerprint. Computer fingerprints typically are used, among other things, to 'lock' software to a particular computer fingerprint and identify computers used in online actions to profile the history and potential risk of particular actions. A typical computer identifier is computed and remains static; to ensure reliability the computer fingerprint typically uses computer minutiae (e.g., serial numbers) that normally do not change . Thus, current computer fingerprints typically use a relatively small set of static minutia which may be prone to spoofing. Some approaches to improving computer identification have sought to increase the number of minutiae used in identifying the computer through the analysis of time (both in clock and network latency) and bits of information left on the computer (i.e. 'cookies'). However, as more minutiae are included in the computation, the probability that changes occurred naturally to the minutia can result in a new computer fingerprint. This falsely identifies a computer as 'different' when it is actually the same computer (often referred to as 'false negatives'). These changes to the minutia on a unique computer occur naturally during normal use and can invalidate the computer fingerprint process or inconvenience the user or service by forcing a re-initialization of the computer fingerprint.

SUMMARY

According to one or more embodiments of the present invention, methods and systems for dynamic key cryptography use a wide range of minutiae as key material including computer hardware, firmware, software, user secrets, and user biometrics rather

than store a random number as a cryptographic key on the computer. Methods and systems for using dynamic key cryptography, according to one or more embodiments, can be used for authenticating users to services, ciphering data for protection, and digitally signing message digests. In one embodiment, dynamic key cryptography anticipates changes to computers caused by industry updates to hardware, firmware, and software of computers.

In one embodiment, a method of dynamic key cryptography includes: selecting a subset from a set of minutia types; for a particular device, sending a challenge to the device, in which: the challenge includes information from which the device can collect actual values of minutia corresponding to the selected subset of minutia types in order to form a cryptographic key, the cryptographic key is never transmitted from the device across any communication channel, and the cryptographic key is used to encrypt an actual response to the challenge; pre-processing a set of responses to the challenge based on tracking updates of minutia from which the selected subset of minutia types is selected, in which: the set of pre-processed responses covers a range of all actual responses possible to be received from the particular device if the combination of the particular device with collected actual values of minutia is valid; comparing the actual response from the particular device to the set of pre-processed responses; and validating the combination of the particular device with the collected actual values if the actual response is included in the set of pre-processed responses for the particular device.

In another embodiment, a method includes: selecting at least one type of minutia from a plurality of minutia types; forming a challenge that conveys the selection of minutia types; computing a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key, each key is computed using values that are possible for the selection of minutia types; sending the challenge to the device; receiving an actual response to the challenge from the device, in which: the actual response is computed using an actual key, the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; comparing the actual response to the pre-processed responses for a match; and based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

In still another embodiment, a system includes a server configured to communicate with a device, in which the server selects at least one type of minutia from a plurality of minutia types; the server forms a challenge that conveys the selection of minutia types; the server computes a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key, each key is computed using values that are possible for the selection of minutia types; the server sends the challenge to the device; the server receives an actual response to the challenge from the device, in which: the actual response is computed using an actual key; the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; the server compares the actual response to the pre-processed responses for a match; and based on whether or not a match was found, the server validates the combination of the device with the actual values of the selection of minutia types.

In yet another embodiment, a computer program product includes a non-transitory computer readable medium having computer readable and executable code for instructing a processor to perform a method, the method including: selecting at least one type of minutia from a plurality of minutia types; forming a challenge that conveys the selection of minutia types; computing a plurality of pre-processed responses possible to receive from a valid device, in which: each pre-processed response is computed using a key and each key is computed using values that are possible for the selection of minutia types; sending the challenge to the device; receiving an actual response to the challenge from the device, in which: the actual response is computed using an actual key, the actual key is computed using: a deduction of the selection of minutia types from the challenge and actual values of the selection of minutia types; comparing the actual response to the pre-processed responses for a match; and based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a system diagram illustrating communication and security between a client, a client device and a service provider facilitated by a dynamic key cryptography provider in accordance with one or more embodiments;

Figure 2 is a system diagram illustrating a challenge, response and validation process performed by the system of Figure 1 in accordance with an embodiment;

Figure 3 is a system diagram illustrating a service provider application (app) delivery system in accordance with an embodiment;

Figure 4 is a system process flow diagram illustrating a system for registration of computer system and user minutiae and services in accordance with an embodiment;

Figure 5 is a system diagram illustrating a system to catalogue and model industry minutia and user heuristics to create and update anticipated minutia databases in accordance with an embodiment;

Figure 6 is a system process flow diagram illustrating a system for validation scoring, confidence rating and step-up authentication processing in accordance with an embodiment;

Figure 7 is a system process flow diagram for an authentication and digital signature system capable of incorporating three identity factors in accordance with an embodiment;

Figure 8 is a system process flow diagram illustrating a system for application processing for local and update data security functions in accordance with an embodiment; and

Figure 9 is a system diagram illustrating computer identity provider lifecycle functionality and services to service providers in accordance with an embodiment.

DETAILED DESCRIPTION

In accordance with embodiments of the present invention, methods and systems of dynamic key cryptography using dynamically changing keys composed of or derived from dynamically changing key material provide cryptographic services such as authentication, data protection, and digital signature by uniquely identifying a user's computer or other electronic device based on (1) the electronic device itself, e.g., a mobile phone or personal computing device, and using a very wide range of hardware, firmware, and software minutia found on the computer; (2) secrets a user of the computer knows; and (3) biometric information the computer might collect from the user. Dynamic key cryptography in accordance with one or more embodiments enables secured actions for users of electronic computers and, more particularly, provides authentication between a client electronic computer and a service provider, encryption of data electronically stored or sent on a

communication channel, and digital signature for electronic digests of actions performed by the user on an electronic computer.

The dynamic key cryptography system according to one embodiment anticipates changes to the minutia caused by updates and natural usage of the computer and practically eliminates false negatives that block valid users from a network service. Dynamic key cryptography may provide a safe, reliable method to users of network services for authenticating the user to network services that protects both the user and the network services, protects the integrity and privacy of data, and provides for digitally signing the digest of an action performed by the user on the electronic computer.

One or more embodiments may provide features such as: 1) simple user experience – no difficult passwords to remember or type, the user device or computer is invisibly authenticated and the user can be asked to enter a second identity factor such as a secret PIN or biometric (e.g., voiceprint) into the computer only if required by the service and protected services can be automatically reconnected to a new device or computer when it is registered by the user; 2) unprecedented security – using a wider range of hardware, firmware, software, secret and biometric minutia to deliver a very accurate device or computer and user identity that is more difficult to spoof, especially as some computer identifier values are not static but are expected to change; 3) reliability – anticipating changes to the user device or computer delivers a tolerant, yet secure authentication with fewer false negatives that anger users and clog customer support services; and 4) service and data separation – delivered as an integrated part of a mobile application (app), a "foundation" (e.g., dynamic key cryptographic service) helps protect the app, encrypt service data stored on the user device or computer, digitally sign actions and allows the service to react without affecting other services, e.g., should data need to be wiped, only the app's data is affected, not the user's other information such as the user's pictures or messages.

One or more embodiments may enable a more convenient method for connecting the user and service. For example, instead of subscribers typing in cumbersome passwords (or worse yet, storing them unencrypted on the computer), the dynamic key cryptographic (dynamic key crypto) service and related client software can compute and manage the unique properties of the user device or computer. The resultant identified computer can be used in place of passwords to simplify the customer connection experience. Since the computer

itself is uniquely identified, it represents a safer method of identifying customers (e.g., users or subscribers). By forming cryptographic keys which use minutia found on the computer, the computer itself (as defined by its minutia) is validated, not a static key stored or intended to be stored only on the computer. The discovery and copying of a single value (the secret key) is significantly easier than the discovery and copying of a very large range of computer minutia values. In addition, the writing of a single key in a computer's memory effectively counterfeits the uniqueness of a computer identified by a single, static stored value. To counterfeit a dynamic key crypto-identified computer, it would be necessary to intercept various methods to learn the minutiae values of the computer. Several direct and related methods may exist for learning the value of a particular computer minutia; to effectively counterfeit the computer, it may be that all methods for accessing all computer minutia values would need to be intercepted and the fraudulent response returned. Furthermore, since the dynamic key crypto system expects certain computer minutia values to change, a successfully counterfeited computer would also need to ensure the fraudulent computer minutia values change in an expected manner. Should a user's online activities require an even higher level of trust, the platform (e.g., dynamic key crypto service and related client software) can force the user to enter the user's standard PIN into the computer to ensure a valid user is the person using the computer.

Several technologies exist for processing security and assurance claims using static values. These include passwords themselves and static 'seed keys' for functions like one-time-password and challenge-respond security mechanisms. Even public key cryptography is based off a static key pair (public and private). One or more embodiments of the dynamic key crypto system may use a very large numeric representation (e.g., 100,000's of bits) of computer and user minutia (e.g., any piece of information that can be definitively associated with the computer and its user, including information from the general categories of what the user or computing device has, what the user knows, and what the user is) to form cryptographic keys that support a range of security functions in a verifiable manner (a cornerstone of security). In one or more embodiments methods based on the predictable dynamic nature of the minutia may allow for verification of the minutia (as if they were a single static value) but not all of the minutia is required to be static; most values of the minutia can (and are expected to) change and evolve over time and the change of the minutia

values themselves increases the perceived randomness of the resultant dynamic crypto keys. The validation of dynamic key cryptography based on changing minutia uses a complex confidence scoring which isolates and evaluates the minutiae that have changed and uses confidence weightings against the predictability of such changes. Changing minutia when used as dynamic key material for dynamic key cryptography adds complexity to the cryptographic system which can improve security as a one-time copy of the minutia values or resultant key will likely fail later in time as the minutia values are expected to change.

Layering static minutia (e.g., hardware minutia, user secrets, some user biometrics), slow-changing minutia (e.g., firmware minutia, some user biometrics), and predictably changing minutia (e.g., software minutia) can create a very large set of key material (or keyspace) which can be processed as subsets of minutia. These subsets of minutia function as static keys over a particular time interval and provide increased security while being fault-tolerant to normal and natural anomalies. Examples of categories of minutia include various hardware, firmware, software, user secrets, and user biometric values. For example, hardware minutia may include the make and model of the computing device (e.g., smart phone or pad), an international mobile equipment identification (IMEI) number of the computing device, or a circuit manufacturer's ID number which may be readable from a circuit chip element of the computing device. Similarly, examples of firmware and software minutia may include which firmware and software codes are installed on the computing device and characteristics such as what particular version or release date of firmware or software are installed on the computing device. Other minutia may include such information as geo-location from GPS (global positioning system) capability of the computing device. In some embodiments, minutia may also include secrets a user of the computing device knows (e.g., a PIN number or password) or biometric information the computing device might collect from the user (e.g., a fingerprint, voiceprint, or retinal scan). In this manner, dynamic key cryptography can utilize minutia values from the three identity factors ("have", "know", and "are") to form a dynamic key so that dynamic key crypto purposes such as authentication, data protection, and digital signature can benefit from the three identity factors simultaneously.

Dynamic key cryptography key matter is a significant improvement over static cryptographic keys of simply random numbers (as nearly all prior art cryptography uses).

Dynamic key crypto keys are permutations of a very large collection of minutia values, many of which change over time; the result is a seemingly random number comprised of independently meaningful minutia values.

To achieve fault tolerance over a possibly changing set of minutia, anticipated changes to minutia and multiple subsets of minutia that provide back-up to any single subset can be used. By using mass produced electronic devices (e.g., mobile units and computers) which contain both a vast array of minutia and predictable evolution paths of minutia, a dynamic encryption system of methods based on evolving minutia can be maintained for the benefit of nearly any security function. In addition, since the range of minutia is so large, certain cryptographic functions can be performed several times using different subsets of minutia. In this manner, should one subset of minutia change, cryptographic checks using other minutia subsets and the anticipated changes to the minutia can improve fault tolerance and detection of spoofed minutia values.

Assertions regarding a computer's uniqueness, confidence in the computer's uniqueness, and service-orientated directives (e.g., provision, lock-hold, erase, transfer, blacklist) are formulated, controlled, and directed by the dynamic key crypto service. For example, computer dynamic key crypto libraries (installed on various user devices) gather the computer minutia values (e.g., from various user devices) and act on the computer (selected one of the various user devices) in response to dynamic key crypto service directives. The heuristics for the predictive and constantly changing minutia values are performed in the dynamic key crypto service using data forwarded by the dynamic key crypto libraries (from the various user devices) in addition to data gleaned from industry sources. Industry data includes cataloguing publically available data (such as over-the-air upgrades – including operating system (OS), firmware, and applications – and network updates) over the range of possible computers. While nearly infinitely larger than the changes that can occur to a single computer (lending security via a broader search space) the industry data is still finite and, therefore, useful in predictive heuristics regarding computers in use.

Various embodiments may provide systems and methods for secure dynamic key cryptography services including:

1) Registering online service providers (OSP) with the dynamic key crypto service to create custom (for each OSP) computer dynamic key crypto libraries that conduct security functions but are resistant to successful attacks by other services and prohibit collaborating online service providers from profiling users.

2) Collecting and registering the minutia values with the dynamic key crypto system, tying the minutiae to an online service provider account identifier.

3) Gathering industry information regarding updates to computer hardware, firmware and software to create a catalogue of industry minutia values which may possibly appear on registered computers when they are updated. The catalogued industry minutia values are indexed and the possible minutia and current minutia are combined and permutations intelligently stored to anticipate future minutia possibilities.

4) Identification based on a hash from a subset of minutia taken from a very wide range of minutia found or collected by the computer including hardware, firmware, software, user secrets, and user biometrics. The authentication can be performed as an intelligent challenge and response which indexes minutiae and, when compared to possible responses from anticipated minutiae, can ascertain minutia changes without having to actually exchange the minutiae between the computer and dynamic key crypto services.

5) Scoring the confidence of a valid response based on the minutia used, the anticipated and expected changes to the minutia used including non-computer factors such as user PIN entry, geo-location, and biometrics. Different minutia can be intelligently chosen for the challenge to achieve a response that yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation.

6) Protecting the application and data running on a computer by using the minutia in cryptographic functions such as encrypted memory, local identification, and heartbeat to prohibit application self-destruction. Some cryptographic functions are computed using more than one subset of minutia to allow back-up functionality should minutia used in the cryptographic function change. The high number of meaningful minutia enables a more complex interaction between the user the computer, and the software computing the identifier. The increased "chatter", a mix of meaningful and decoy reads of minutia, obscure which minutia is meaningful, and thereby increases the difficulty of spoofing minutia values and intercepting calls intended to counterfeit the original computer.

7) Digitally signing a digest of an action performed by the user on the computer by ciphering the message digest with a key formed by minutia values which can include the three factors of identity ("have", "know", and "are", e.g., respectively, computer or device, user secret, user biometric information).

8) Notifying a wide range of online service providers should a computer status change. This enables a single event to trigger responses from a wide range of registered online service providers so that security and service continuity are maintained.

9) Forcing a user to enter a service PIN, computer PIN or biometric on a registered computer to include user minutia in the dynamic key cryptography function and ensure that a valid user is controlling an identified computer.

Some embodiments of systems and methods allow the calculation of one or more minutia value subsets to be based on a very wide possible range of minutia from various categories including hardware, firmware, software, user secrets, and user biometrics. One embodiment models predictive and anticipated changes that occur naturally and during the use of a computer or device. The larger considered ranges of minutia found on a computer or collected by a computer and the modeled dynamic nature of some minutiae enable a more robust and secure authentication system which is less prone to spoofing.

One embodiment uses a computer identity provider service to collect computer minutia information from the industry and uses this data to anticipate possible changes and permutations to minutiae on registered computers. By anticipating changes in minutiae found on the hardware, firmware, and software elements of a computer, embodiments are more fault-tolerant to natural changes in the computer. In this manner, embodiments can anticipate changes to minutiae and, through a challenge and response exchange between a computer and dynamic key crypto service, synchronize changes to minutiae without actually exchanging the minutiae between the computer and dynamic key crypto service.

Since nearly all security functions such as authentication, encryption, and digital signature are based on static keys and identifiers, embodiments of the present systems and methods also allow for the in-system back up of some cryptographic functions and secure transmission, synchronization, and updating of dynamically changing minutiae between the computer and the dynamic key crypto service. The dynamic key crypto service and computer enable the dynamically changing minutiae to be used in or used in place of

traditionally static security functions including authentication, encryption, digital rights management, and data protection.

Figure 1 illustrates a system 100 in which a service user 20 may communicate through a network 16 (e.g., the Internet, local area networks (wired and wireless), and personal networks (e.g., P2P, Bluetooth, near field communications (NFC)) using a computer 18 (e.g., a mobile phone, computer system, smart phones, laptops, tablets, sensors, payment terminals, and meters or any other communication capable electronic computer). The computer 18 (also referred to as "electronic device", "user device", or simply "device") may operate by executing an operating system (OS) that may enable execution on computer 18 of a dynamic key crypto library 56 and a service provider app 44. Service provider app 44 may be provided by one or more of a number of various OSPs and may provide features specific to a particular service provider 14 that provides the service provider app 44 to the service user 20 and user computer 18. As shown in Figure 1, service provider app 44 may interface with dynamic key crypto library 56, and both service provider app 44 and dynamic key crypto library 56 may interface with computer 18 and its operating system. Service user 20 may communicate with service provider 14 over the network 16 using computer 18, for example, using service provider app 44. A service user 20 may be a person that can have several different types of computer 18 and may be a user of any number of service provider systems 14. Likewise, a computer 18 may be used by more than one service user 20, for example, family members sharing a smartphone or pad.

A dynamic key crypto provider 10 may provide various services and functions related to minutiae found on the computer 18 or minutiae collected by the computer 18 from the service user 20. The dynamic key crypto provider 10 may be a web service capable of securely manipulating and analyzing large amounts of data such as performing calculations, data modeling, permutation processing, interpolation, internet searches and complex database functions. The dynamic key crypto provider 10 may be cloud-based so it can have sufficient computational speed and power to off-load intensive computational efforts from a sometimes resource-constrained computer 18. The dynamic key crypto provider 10 may provide a secured processing environment for the processing in some embodiments including managing an enormous data-intensive query engine for complex data pattern matching, modeling and processing of complex and numerous permutations. As shown in Figure 1,

dynamic key crypto library 56 may communicate with dynamic key crypto provider 10 and may also communicate with the service provider 14 through Network 16. Dynamic key crypto provider 10 also may communicate with online service providers via network 16 and may communicate with the particular service provider 14 that provides the service provider app 44 to the service user 20 and user computer 18. Service provider 14 may have a customer-vendor relationship, for example, with dynamic key crypto provider 10 in which service provider 14 is a customer receiving services from dynamic key crypto provider 10. There can be any number of service provider systems 14 connected to the dynamic key crypto provider 10. The service provider 14 may be an industry typical website usually requiring a username and password. Examples of a service provider 14 include but are not limited to social networking websites, corporate IT services, and online banking, healthcare, and travel services.

Figure 2 shows an illustrative example for providing and using dynamic key cryptography to ensure a valid service user 20 is using an authenticated computer 18 in a system such as system 200 shown in Figure 2. As described in more detail below, system 200 may collect and catalog a number of minutiae values of computer 18 and service user 20 that may be useful for identifying the computer 18 and service user 20 in the sense that computer minutia 64 and secrets and biometric minutia 26 can be used by the dynamic key crypto provider 10 to form dynamic keys unique to each and every distinct computer 18 and service user 20. In other words, each distinct computer 18 may have a method for using unique computer minutia 64 and secrets and biometric minutia 26 in system 200 that corresponds to that distinct computer 18 and service user 20, and each uniquely identified computer 18 corresponds to one and only one distinct computer 18 and each uniquely identified service user 20 may correspond to one and only one distinct service user 20. The unique identification of a computer 18 may be processed by system 100, for example, by a service provider 14 or by the dynamic key crypto provider 10, and there be no meaningful single identifier or identity key itself stored on the computer 18. System 200 shown in Figure 2, illustrates an example of identifying and authenticating a specific computer 18 and service user 20 via challenge, response and validation sequences performed by dynamic key crypto provider 10. Each distinct computer 18 and service user 20 may be recognized, for example, by specific computer minutia 64, specific secrets and biometric minutia 26,

combinations of computer minutia 64, combinations of specific secrets and biometric minutia 26 or combinations of both specific computer minutia 64 and combinations of specific secrets and biometric minutia 26 found on the computer 18 or collected by the computer 18 from the service user 20 as cataloged by the dynamic key crypto provider 10.

Collection of minutia can include methods such as fuzzing and hashing that obfuscate the actual values of minutiae that represents personal identifiable information before the minutiae values are sent from the computer 18 to the dynamic key crypto provider 10 such that the anonymity of a service user 20 is maintained. For example, phone numbers can be hashed so that the actual phone number is not known. In another example, the geo-location home of a service user 20 can be fuzzed by truncating the GPS coordinates so that the value processed by the dynamic key crypto library 56 represents, for example, a multiple mile radius, not multiple feet. In this manner, it would be difficult to determine the exact address a computer 18 resides nearly every night that could be interpolated to be the home of the service user 20. The fuzzy geo-location can be beneficial because the location of the computer 18 can be tracked without invading the privacy of the service user 20 because, to the dynamic key crypto provider, the service user 20 can be anonymous. If a service provider that knows the true identity of a service user 20 were to also know the geo-location of the device, the privacy of the service user 20 could be abused. Thus, a separation of device and user knowledge can exist so that the device (i.e. computer 18) of an anonymous service user 20 can be tracked 24x7 and service providers (who do know the identity of service user 20) can ask for geo-location information from dynamic key crypto provider 10 only when they require it so as to gain benefit of geolocation without a privacy invasion of the service user 20.

As shown in Figure 2 at step 2001, in one example, computer minutia 64 can represent a set of 390 distinct minutiae values that may be chosen for collecting and cataloging from the computer 18. In the particular example, there are 40 categories or types of the minutia that are hardware minutia; 70 categories or types of the minutia are firmware minutia; and 280 categories or types of the minutia are software minutia. Hardware minutia may include such items as the device manufacturer, model number, serial number, and international mobile equipment identification (IMEI) number, for example. Firmware minutiae may include, for example, the name of the firmware vendor, version number,

revision number, revision date, communication and telephony services, location and GPS data, and operating system. Software minutia, similarly for example, may include application name, supplier identification, software release number, memory reads, software cataloguing, clock and other counters, and date. Hardware minutia values typically cannot change without changing a physical component of the computer 18. Firmware minutia can be updated but usually their update is controlled by someone other than the service user 20. Software minutia changes dynamically via various individual instantiations of service user 20 and includes elements that may require predictable, constant change in normal situations (i.e.frequently called contact phone numbers).

It is important to note that software minutiae values can often reflect customizations performed by the service user 20. In this manner, software minutiae values can accurately identify computer 18 devices that are otherwise extremely similar in hardware and firmware. When the computer 18 is manufactured, devices are very similar, hence the need for serial numbers, but, under security considerations, these hardware minutia identifiers are few in number and can be easily spoofed. Significant customization affecting software minutiae values is typically done within days, even hours, of ownership of a computer 18 by the service user 20. Thus the software minutiae values diverge significantly at device personalization and the addressable space continues to expand throughout the use of the computer 18 by the service user 20. Therefore, the uniqueness of a computer 18 increases with time after manufacturing, this is often referred to as entropy, or the natural tendency towards chaos, and, thus, software minutiae are valuable in the security of dynamic key cryptography functions. To illustrate the potential range represented by the values of minutia if, for example, there were 300 minutia values each averaging four bytes in length, by interleaving and mixing the minutia values to form dynamic crypto keys, the keys could represent a space defined by as 2 raised to the 9600^{th} power (cryptographic keys of 2 raised to the 1024 power are considered secure by the industry).

Nearly any data can be introduced into the system 200 by the definition and addition of minutia classes. For example, PIN, password, service history and other service user 20 secrets can be entered and processed as if they were a class of minutia. For example, a minutia index might refer to memory location where the minutia value could be read and processed. If the minutia index for the PIN is sent to the device, instead of, for example,

reading a memory location, a PIN screen can be displayed on the computer 18, the service user 20 can enter their PIN (or other secret value) and the information entered can be processed as the minutia value in the method here described by system 200. A similar process can be performed for biometric values, for example, facial geometry, voice patterns, fingerprinting. In another example, the service provider app 44 might be analyzed and the software structure itself provide minutiae values that can be challenged and validated to ensure the run-time integrity of the calling application service provider app 44. Thus by adding minutia classes, any information can be processed to get the benefits of system 200 (e.g., secure input for crypto key material, fuzzy validation matching, inferred minutia value learning, confidence rating).

Step 2003 shows an example of specific values of the minutia 70 database for a specific computer 18. The minutiae can be obtained via the dynamic key crypto library 56. Various instances of the dynamic key crypto library can exist on a single computer 18 and can be related to one or more instances and providers of a service provider app 44. In this example, the first hardware minutia (H1) may be the IMEI number of computer 18, and for the specific computer 18 of the example, the IMEI number may be encoded as "1234". The computer 18 may have specific values for the 40 different hardware minutia, H1 to H40; specific values for 70 different firmware minutia, F1 to F70; 280 specific values for different software minutia, S1 to S280, 2 specific values for service user 20 secrets, ?1 and ?2; and 5 specific values for service user 20 biometric minutia, B1 to B5, from which it may be possible to accurately and uniquely identify the specific computer 18 and associated service user 20 for computer 18. The actual minutia used and their index ordering as H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5 provide a particular cataloging scheme or a cataloging of minutia DB 70 for the specific example illustrated in Figure 2. The combination of specific hardware, firmware, software, secret and biometric values found on the computer 18 and collected from the service user 20 at a particular time or within some pre-defined time frame may be referred to as the "current device image" as indicated at step 2003.

For a particular computer 18 and a particular scheme (e.g., H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5 of Figure 2) a number of possibilities for specific values of the minutia can actually occur on the computer 18, be known by the service user 20 or

represent the biometrics of service user 20. For example, as indicated at step 2005, the specific minutia value for index F1 may be either of F1A, F1B, or possibly others, referred to as the anticipated minutia DB 98. All other computer minutia values remaining the same, a change at the F1 index from a value of F1A to F1B, for example, represents one permutation of computer minutia possible for a specific type of computer 18 (e.g., for computers running the Android operating system). It can be seen that if five different values were possible at index F1, then 5 permutations that change only F1 may be possible for each different combination of the remaining computer minutia. Although all 5 values of F1 may not be possible for every combination, the number of permutations is generally multiplicative so that an estimate of the number of possible permutations can be made by multiplying together the number of possible values at each index, for all the indexes H1 to H40, F1 to F70, S1 to S280, ?1 to ?2, and B1 to B5. For the example shown in Figure 2, it can be seen that even with only 2 or 3 values of possibility for each index, the number of permutations, or different possible combinations of minutia, for all types of computer 18 can easily be practically infinite. Thus, even for large numbers of computer 18 that appear otherwise identical, within the millions of different possible combinations of minutia DB 70 and the related practically infinite range of minutia values in the anticipated minutia DB 98, each single computer 18 can be uniquely identified by matching its unique computer minutia 64 and secrets and biometric minutia 26 collected by computer 18. As an example, when a service user 20 receives a newly manufactured mobile device (i.e. computer 18), typically part of the out-of-the-box initialization routine is to customize the computer 18 with service user 20 specific information such as, for example, contacts, email and network connections. The customizations these additions represent (i.e. minutia) can immediately differentiate two examples of computer 18 that were manufactured one immediately after the other. As the service user 20 uses their computer 18, the usage continues to affect and differentiate the minutiae that can be collected from the computer 18 (e.g., frequently called phone numbers). By maintaining a database of all industry updates related to the collective industry of instances of computer 18 – e.g., by collecting and cataloging all industry updates to hardware, firmware, and software minutia –dynamic key crypto provider 10, for example, may be able to know what all the possibilities are for the computer minutia 64 of a given computer 18 so that method 2000 may be able to recognize a computer 18 in spite of changes

not reflected or known by the current minutia DB 70. In fact method 2000 may improve the accuracy and fault tolerance of its recognition of devices (i.e. computer 18, computer minutia 64, service user 20 and secrets and biometric minutia 26) by exploiting knowledge of changes (i.e. anticipated minutia DB 98) to the current device image (i.e. minutia DB 78).

When using combinations of computer minutia 64 for identifying a specific computer 18, method 2000 may use intelligent minutia selection 114 to select a combination of minutia from the total set of minutia (i.e. computer minutia 64 and secrets and biometric minutia 26). In the specific method 2010 example illustrated in Figure 2, the combination of minutia chosen is one hardware minutia, Hx, one firmware minutia, Fy, and one software minutia Sz. Such a combination may be referred to as a "triplet". Although a triplet Hx-Fy-Sz may include one hardware, one firmware, and one software minutia as in the example illustrated in Figure 2, a triplet could also include, for example, two hardware minutiae and one software minutia, e.g., Hx-Hy-Sz. Also, for example, more or less than three minutiae could be used at a time, e.g., a "quadruplet" such as Hx-Fy-Sz-Bb. Any combination of minutia from the total set of minutia DB 70 may be used. Smaller subets of minutia values constrain the scope of change within the minutia values so the results can be rapidly validated. Longer subsets of minutia values increase the potential change (and therefore security) and can be useful in infrequent, but high security crypto actions like digital signature.

The particular values for x, y, and z are not specified for this example so that Hx could be any one of the 40 hardware minutia H1-H40 shown in step 2003, e.g., IMEI number. Similarly, Fy could be any one of the 70 firmware minutia, and Sz could be any one of the 280 software minutia shown, for example, in step 2003. A hardware minutia of a particular computer 18 generally will not change without changing the entire computer 18 (and identity) itself, so whatever hardware minutia, Hx, is used, it may not be expected to change for the particular computer 18 being challenged, as indicated by "(no changes)" next to H1-H40 in step 2005, so that the number of possibilities for each individual Hx is limited to one. In the particular example illustrated in method 2030 of Figure 2, the firmware minutia, Fy, is assumed to have nine different acceptable values for illustration, and the software minutia, Sz, is assumed to have twenty different acceptable values for illustration. Method 2030 can vary the fault tolerance of the invention by varying the allowable range of

acceptable minutia values with respect to the range of possible minutia values for each minutia value.

Although it may be the case that certain combinations of hardware, firmware, and software values may be incompatible (e.g., a particular software update might require a particular firmware update) the example of Figure 2 assumes that all updates are independent so that the total number of permutations of acceptable device characteristic values for the particular computer 18 being challenged is the product of the number of acceptable possibilities for each component, Hx, Fy, Sz, of the triplet Hx-Fy-Sz, or 1*9*20 = 180, as indicated at step 2007. The number of acceptable permutations for a selected combination of minutia, then, can be smaller than the number of possible permutation for the same triplet and significantly smaller than the total number of permutations for all minutiae, as shown by this example, e.g., 180 out of potentially millions of possible minutia values and 180 out of the potentially infinite number of permutations as indicated at step 2005.

Selection of the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging a particular device may vary, not only from computer 18 to computer 18 and service provider 14 to service provider 14, but, for example, each time the same computer 18 is challenged on behalf of the same service provider 14. The intelligent minutia selection 114 may employ a number of considerations in selecting the combination of minutia to be used for a particular challenge of a particular computer 18 and service user 20. As shown step 2010, intelligent selection of the combination of minutia (e.g., Hx, Fy, Sz for the example) may be based on need for uniqueness, predictability and scope of possible changes. For example, selection of minutia may use expectations for changes to the current minutia DB 70 database based on knowledge of the current computer minutia 64, current secrets and biometric minutia 26 and knowledge of all minutia value updates that can occur (i.e. anticipated minutia DB). Knowledge of all minutia value updates that can occur, whether or not the updates actually have occurred, can be gained from the previously mentioned collecting and cataloging industry-wide of all computer minutia updates and the heuristically determined trends caused by the use of computer 18 by a particular service user 20 . Also, for example, if uniqueness and predictability are of concern, minutiae may be chosen for which the values are known and are not expected to change. If scope of possible changes is of concern, minutiae with a reduced capacity for

change or a tighter tolerance of acceptable change may be selected. Combinations of minutiae can be selected to isolate a particular minutia by combining it with static minutiae. Likewise, a static minutia can be grouped with minutia that changes rapidly to form a set that changes in some manner to protect static minutia members. Minutia sets can be selected to address specific purposes such as geo-location or user secrets. Minutia sets can combine minutia from the various identity factors of something you have, something you know and something you are. Minutia values can be selected to periodically 'refresh' validations of specific minutiae.

The intelligent minutia selection 114 process can select minutiae from the different minutia sources of hardware, firmware, software, user secrets and user biometrics. The intelligent minutia selection 114 process chooses the minutia nearly randomly to widely and unpredictably sample various computer minutia 64 and secrets and biometric minutia 26 such that deducing a pattern for minutia sampling is difficult to infer. However, there may be certain minutia pairings and groupings that readily show and determine changes to computer minutia 64. In such cases, a 'selected' (versus 'random') subset of minutiae may be selected by the intelligent minutia selection 114 process.

After the intelligent minutia selection 114 process determines the minutiae to be used, the formulate challenge 116 process looks up the minutia index for that minutia from the SP info and IDs 32 database; this allows the minutia index for one service provider 14 to be different from another service provider 14. The indexes are then combined with a random number using an algorithm defined for each service provider (as described in Figure 3, specifically the SP info and IDs 32 database); again to provide differentiation and security between service provider 14 instances. The challenge result from the formulate challenge 116 process can then be processes and step 2020 and given to the send challenge and await response 118 process. Since the challenge contains nearly random information which serves as the actual challenge value, the transmission of the challenge need not be done via an encrypted tunnel but it can be sent securely by send challenge and await response 118 if desired.

As shown at step 2020, the formulate challenge 116 process can compute a cryptographic key based on the selected combination of minutia (e.g., Hx-Fy-Sz for the illustrated example). For example, each of x, y, and z may be a table index value (e.g., an

integer) to the corresponding hardware (H), Firmware (F) and Software (S) information in a database of the particular service provider 14. The specific x, y and z table ordering and properties for a particular service provider 14 is found both in the dynamic key crypto library 56 created specifically for the service provider 14 and in a database of information specific to the service provider 14 maintained by the dynamic key crypto provider 10. The key may be computed as shown at step 2020, for example, by applying a mathematical or cryptographic function "Fn" to the combination of minutia values Hx+Fy+Sz. Thus, the cryptographic key may cryptographically encode information from the selected combination of minutia, e.g., triplet Hx-Fy-Sz. The same minutiae references, for example the x, y and z table indexes, can be computed by applying a mathematical or cryptographic function "Fn", which may be the same or a different function from that used earlier, to form a challenge value combining the indexes with other information such a random number, as used in the example. Thus, the challenge cryptographically encodes enough information for the computer 18 being challenged to determine which minutia should be used in computing its actual response. It is important to note, however, that even though the computer 18 may use the minutiae Hx-Fy-Sz and its own actual values for those minutiae in computing its response, no information as to what are the actual values of the minutiae is included in the challenge or response nor is directly gleanable from the response.

At step 2030, the dynamic key crypto provider 10 computes all responses that are acceptable for the computer 10 to make. The acceptable response computations can be based on the allowable range of possible changes to the defined subset of minutiae selected for the challenge. These computations can be performed beforehand (e.g., independently – whether prior, concurrently, or after – receiving the actual response from the computer 18) and stored in valid responses DB 130 for comparison to the actual response from computer 18. The challenge may be sent by dynamic key crypto provider 10 or by the service provider 14 to the particular computer 18 being challenged. The range of possible changes may be processed because of the constant and continuous collecting and cataloging of industry updates for the total set of minutia from which the particular combination of minutia (e.g., Hx, Fy, Sz for the example of Figure 2) to be used for challenging the particular device is selected. Because every allowable response to a challenge is therefore known (e.g., computed at step 2030) before the challenge is sent to the computer 18, the actual response that will be received from

the computer 18 to the challenge may be among the range of pre-processed acceptable responses (and therefore among the acceptable changes) computed by the dynamic key crypto provider 10 that is challenging the computer 18. As illustrated at step 2030, in this particular example having no possible changes for hardware (e.g., one possible value), nine possible changes or values for firmware and twenty possible changes for software, there are 180 allowable responses for the computer 18 to return to the challenge. Each of the 180 allowable responses may be calculated by the dynamic key crypto provider 10 in a similar manner that the computer 18 will compute its actual response in response process 112, as illustrated in step 2040.

At step 2040, the particular computer 18 being challenged may receive the challenge and unpack the challenge to determine which minutia it should collect and use the values of to form its response to the challenge. Having unpacked the challenge using information and algorithms stored in the dynamic key crypto library 56, the response process 112 can use the computer 18 to fetch the values of the selected computer minutia 64 or collect the values of selected service and biometrics minutia 26 and build a key that may be identical to the key computed by the dynamic key crypto provider 10 at step 2020. The particular computer 18 being challenged may form a response to the challenge by applying a mathematical or cryptographic function "Fn", which should be the same as that used at step 2020 or step 2030, to the key + challenge as shown in Figure 2. The computer 18 being challenged may then communicate the response to return it directly to the dynamic key crypto provider 10 or indirectly via the service provider 14. Again, since the challenge and response exchange may contain a random number element, it can change every time, even if the same minutiae were selected. As such, it does not need to be securely transmitted between computer 18 and dynamic key crypto provider 10 over network 16, but it can be if desired. The dynamic key crypto provider 10 sends the computer 18 response to the validate response from computer 120 process for processing in step 2050.

As illustrated at step 2050, the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match. Decrypting or decoding of a response is not necessary so the validation can occur very quickly. On a match between the actual response and one of the

pre-processed responses, the validate response from computer 120 process may then know what the particular actual minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values. If a match is found, the subset of minutiae used in the challenge may be regarded as being known or authenticated. For example, as seen at step 2007, if the actual response matches the 172nd possible response "Resp172" or permutation, then the actual device values must match those of Hx, the first possibility for Fy (e.g., Fy0), and the twentieth possibility for Sz (e.g., Sz19) even though "Resp172" itself contains no direct information regarding the actual minutia values being challenged.

The validate response from computer 120 process can use logical groupings of minutia values to increase the confidence of a matched response. Groupings of related minutia may be gleaned, for example, from the anticipated minutia DB 98 or discovered heuristically. For example, if a set of minutiae is only changed via an industry update and all minutiae within the set change to unique values in unison with the particular update, then should a particular minutia value or values within the set of update related minutia not share the expected values of other minutiae with regard to a single update set, then the validate response from computer 120 could deduce the response related to the minutiae values within the update logical grouping may be in error or fraudulent. As an example, should a fraudulent entity alter the computer 18 to return falsified information when the minutia value is collected by the response process 112 via the operating system on computer 18, the actual minutia value would not be returned. In this manner, a fraudulent entity could make one computer 18 look like another computer 18 or make one service user 20 appear as another service user 20. The validate response from computer 120 can use logical groupings of minutiae and, for example, employ multiple methods for collecting what should be the same value (i.e. a smartphone's phone number can be learned through several methods) (1) Often, multiple methods exist for reading a particular value such as phone number. The various methods can be used and the returned minutia value compared for consistency. (2) Often groups of minutia values are related such that a change in one should create changes elsewhere (for example time and time zone.) In the validate response from computer 120

process, the minutia values related to one another can be verified to ensure changes are found to be consistent throughout the related 'group' of minutia values.

Even if an exact match is not found, the allowable ranges from the set of possible minutiae may be expanded or additional challenges using other, possibly related minutiae, may be sent to the device in an effort to validate the device. If necessary, changes in the computer minutia 64 of a computer 18 can be sent from the computer 18 to the dynamic key crypto provider 10 using the registration subsystem 400 described in Figure 4.

If the response is not an expected response, then a validation failure process as described in Figure 6B can alert the service provider 14 that the validation has failed.

At step 2060, on a match between the actual response and one of the pre-processed responses, the update computer minutia 128 process may then know what the particular actual minutia values from computer 18 are for the combination selected (e.g., triplet Hx-Fy-Sz) by knowing which possible response has matched the actual response even though neither response contains any direct or decipherable information about the actual minutia values. The values from the valid responses DB 130 used in the response calculation can then be used to update the values stored in the minutia DB 70 database.

Figure 3 illustrates a service provider application (app) delivery system 300 in accordance with an embodiment. Figure 3 shows a system for delivering a service provider app 44 to a computer 18 such that the service provider app 44 has included within it a dynamic key crypto library 56 which is unique to the service provider 14 and performs computer security functions on the computer 18.

The service provider app 44 may be similar to a typical industry application except that service provider app 44 makes application programmer interface (API) calls to a dynamic key crypto library 56 that was compiled as a library with the application source code 42 to form the final executable form of the service provider app 44. The service provider app 44 can be shared with the dynamic key crypto provider 10 for analysis to generate minutia values that can validate the integrity of service provider app 44 when service provider app 44 is running on a computer 18. Service provider app 44 may contain or wish to store data that the service provider 14 requires to secure and make private.

Within the dynamic key crypto provider 10 there may be a service provider registration 30 process for registering service provider systems 14 to use system 300. The

service provider registration 30 process records and generates data specific to the service provider 14 and stores that data in the SP info and IDs 32 database. Such data can include preferences like PIN utilization (i.e. force a system PIN, use a service PIN, etc.) and minimum scores to allow connection. The SP info and IDs 32 database may be, for example, a list of customers and partners for whom a custom dynamic key crypto library 56 has been created. The SP info and IDs database 32 may include key material used to identify and encrypt data of the service provider 14 throughout the system 300 and a table for indexing minutia. Such SP info and IDs 32 database may uniquely identify the service provider 14 and ensure that features and elements of system 300 used by the service provider 14 are secure and separate from other service provider systems 14 that might use the system 300. This provides service separation of data and identifiers such that multiple, independent service provider systems 14 cannot collude, compare data and infer what might be considered private data or tendencies of a service user 20.

The SP info and IDs 32 data unique to a service provider 14 may be used in a custom library creation 34 process to make a dynamic key crypto library 56 which contains data elements of the SP info and IDs 32 database. In addition to data unique to the service provider 14, the custom library creation 34 process can create code custom to a particular service provider 14. Such custom code can include different encryption algorithms (e.g., AES, RSA, Elliptical curve), different hashing algorithms (e.g., secure hash algorithm (SHA-1), message digest (MDM)), unique system encryption keys, unique look up table routines and orderings, different hashing methods for combining minutia values into dynamic crypto keys (e.g., interleaved bit transformations, reverse-ordering, bit inverse, bit shifting), and minutia definitions and classes uniquely available to a particular service provider 14. All of the customizations when compiled form a dynamic key crypto library 56 unique to the service provider 14 such that a breach of a dynamic key crypto library 56 for one service provider 14 may not affect the dynamic key crypto library 56 of another service provider 14. In addition, even if the exact same minutia values are used to form a dynamic crypto key on the exact same computer 18, the resultant dynamic crypto key for one service provider 14 may be different than the resultant dynamic crypto key for another service provider 14; thus the responses for different instances of service provider 14 would be different even if the exact same challenge was sent.

Because of the different SP info and IDs 32 databases used in the formation of the dynamic key crypto libraries 56, two instances of service provider 14 (e.g., two different online service providers), for example, may be prevented from being able to compare information gleaned from the computer 18 and conclude their individual service provider apps 44 are residing on the same computer 18. This prohibits the profiling of a service user 20 based on multiple instances of service provider 14 connected to their computer 18.

Likewise, because of the unique computational possibilities introduced in the custom library creation 34 that formed the dynamic key crypto library 56, a successful attack against the privacy and security included within a particular dynamic key crypto library 56, may not be successful against a dynamic key crypto library 56 related to another service provider 14.

The dynamic key crypto library 56 is responsible for, among other activities:

1) reading computer minutia 64 found on the computer 18 and facilitating entry by service user 20 of secrets and biometric minutia 26 into computer 18 that can validate that an appropriate service user 20 is using an identified computer 18;

2) communicating computer minutia information across the network 16;

3) responding to dynamic key crypto provider 10 challenges to establish a computer's unique identity, protect data, and perform digital signatures using computer minutia 64 found on the computer 18 and secrets and biometric minutia 26 input by service user 20 into computer 18;

4) processing requests from the dynamic key crypto provider 10 to possibly hold, transfer, or a delete service provider app 44 and itself (dynamic key crypto library 56); and

5) randomizing or obfuscating dynamic key crypto library 56 activity through various mechanisms that make it difficult to intercept sensitive actions.

The dynamic key crypto library 56 created uniquely for the service provider 14 may be sent to the service provider 14 securely over a network 16 in the send custom library to service 38 process using any of several methods. The dynamic key crypto library 56 may include program logic designed to perform security functions both directed by and on behalf of the service provider app 44 by interacting with the computer 18. With newer forms of computer 18 (e.g., smartphones and tablets), a dynamic key crypto library 56 that functions as part of the service provider app 44 when it is running is a more reliable method then independently running applications to access the required services for computer 18.

Furthermore, the larger combined code size of the dynamic key crypto library 56 and the service provider app 44 can impose a more tedious and difficult effort to isolate the security functions in an effort to defeat the security.

The service provider 14 may perform an industry typical build application 40 process by combining the dynamic key crypto library 56 with application source code 42 of the service provider 14 to create a service provider app 44. The service provider app 44 can be distributed any number of ways including directly over a network 16 and through a third party software distributor 22 either over the network 16 or directly to the service user 20 for loading on the computer 18 via the distribute application 46 process. The third party software distribution system 22 may be an optional system or systems for distributing software from the service provider 14 to computer 18. Apple's AppStore® is an example of such a software distribution system.

Figure 4 illustrates a system 400 for registration of computer and user minutiae in accordance with an embodiment. Figure 4 shows a system for registering a computer 18 with a dynamic key crypto provider 10 and a service provider 14 over a network 16.

The computer 18 may have on it a service provider app 44. When the service provider app 44 is installed, the dynamic key crypto library 56 within the service provider app 44 may run tests to proof the install 76. Proof the install 76 can be part of the dynamic key crypto library 56 and can use a shared secret supplied by service provider 14 through a user authentication 50 process. In this case the service user 20 might answer previously defined questions, recognize historical service usage, and recognize past instances of computer 18 used by service user 20 or other identity proofing methods.

Additionally, the proof the install 76 process can look for other instances of service provider app 44 from other service provider systems 14 and report any found instances back to the dynamic key crypto provider 10 for additional assurances on the history of the computer 18.

After the user authentication 50 is performed, the service provider 14 may send to the dynamic key crypto provider 10 an account identifier that the service provider 14 uses to identify the service user 20. The register computer 68 process binds the account identifier with the computer minutia database (DB) 70 to link the service user 20 to a particular computer 18.

The dynamic key crypto library 56 can sample a wide range of computer minutia 64 and secrets and biometric minutia 26 using the fetch key minutia 58 process including minutiae from the computer 18 (hardware, firmware, and software) and minutiae from the service user 20 (secrets and biometrics). Secrets and biometric minutia 26 may be collected from the service user 20 by the computer 18 or via other conveyance methods. Not all possible minutia values are required to be read at installation; some may be read at a later time.

A process to select minutia for service keys 60 uses some or all of the computer minutia 64 to create encryption and identifier keys that can be used by the dynamic key crypto library 56 and other parts of the systems 100, 200, 300, 400, 500, 600, 700, 800, and 900 for things like encrypted service data 196 stored locally on the computer 18. These selections may be predefined in a dynamic key crypto library 56 or stored in a service key minutia selections 66 database that is managed and secured by the dynamic key crypto library 56. The service key minutia selections 66 database may reside within a secure element on the computer 18 and can be used for offline processing. The minutia selected by the select minutia for service keys 60 process may be used by the dynamic key crypto library 56 to dynamically build the service keys required by the dynamic key crypto library 56; the keys that result from reading the computer minutia 64 are not stored within the dynamic key crypto library 56 or system 400; they may be computed as they are needed by consulting the service key minutia selections 66 database and using the fetch key minutia 58 process to obtain the resulting computer minutia 64 or secrets and biometric minutia 26. Thus if a service provider app 44 was copied from one computer 18 to another computer 18, when the service keys were built from computer minutia 64, the resulting service key would not be able, for example, to properly decrypt data stored locally on the computer 18.

Some of the computer minutia 64 and secrets and biometric minutia 26 are sent to the dynamic key crypto provider 10 via the transmit minutia to dynamic key crypto provider (DKCP) 62 process. A relatively small amount of computer minutia 64 and secrets and biometric minutia 26 can be sent to the dynamic key crypto provider 10 so the dynamic key crypto provider 10 can look for existing matches to the computer minutia 64 in its minutia DB 70 database. If the dynamic key crypto provider 10 finds matching minutia 64, then the dynamic key crypto provider 10 can send challenge, response, and validation exchanges

described in Figure 2 to verify a wider set of computer minutia 64. If a wider sampling of computer minutia 64 are properly verified by the dynamic key crypto provider 10, then it can possibly deduce that this is another service provider app 44 being added to a computer 18. If the dynamic key crypto provider 10 does not finding matching computer minutia 64 in its minutia DB 70 database, then a subset of computer minutia 64 and secrets and biometric minutia 26 can use the process "transmit minutia to DKCP 62" such that the computer 18 can be properly and uniquely identified and the remainder of computer minutia 64 and secrets and biometric minutia 26 can be learned by the dynamic key crypto provider 10 using the update computer minutia 128 process described in Figure 2. In this manner, it may be possible to transfer some of the minutia via challenge, response, and validation as described in Figure 2, and not all of the minutia may need to be transferred via the transmit minutia to DKCP 62 process, which can use several secure transmission methods that may vary by service provider 14 through the customization of the dynamic key crypto library 56.

By performing a transmit minutia to DKCP 62 process, various values of computer minutia 64 and secrets and biometric minutia 26 may be sent along with their minutia descriptor to the dynamic key crypto provider 10 which may perform a register computer 68 process. The register computer 68 process may record the computer minutia 64 and secrets and biometric minutia 26 into a minutia DB 70 along with a reference to the service provider 14 account identifier for the service user 20. The minutia DB 70 can store the type (or category) of minutia, its value and the service identifier for later processing.

The dynamic key crypto provider 10 is able to store the computer minutia 64 and secrets and biometric minutia 26 which have been randomized by the unique dynamic key crypto library 56. The dynamic key crypto provider 10 is also able to decrypt service provider (SP) minutia 74 using SP info and IDs 32 data to learn the actual computer minutia 64. Many of these actual minutia values are known only by the dynamic key crypto provider 10 and may be used later for services to multiple service provider systems 14.

Some of the actual computer minutia 64 and secrets and biometric minutia 26 may be sent to the service provider 14 via a send computer profile to SP 72 process. To protect a service user 20 from being profiled by various instances of service provider 14 that might collude and interpolate minutia values, the descriptive names of the minutia values can be abstracted so their actual meaning is unknown (e.g., counter-1, counter-2, entertainment-1).

In addition, where possible, the values of the minutia can be hashed to hide the actual minutia value. The service provider 14 can store computer info 52 into SP computer info DB 54 or store data in the service and user data 24 database (or both). The SP computer info DB 54 information can be useful to the service provider 14 for understanding the types and minutia of computer systems 18 running their service provider app 44 software. Such information might include OS type and version, computer make and model, for example. The service and user data 24 database might contain secrets such as PINs and passwords meaningful to the service provider 14.

Figure 5 illustrates a system 500 that may be used to catalogue and model industry minutia to create and update anticipated minutia databases in accordance with an embodiment. Figure 5 shows a system 500 for creating an industry update catalogue DB 96 from a wide range of industry sources and using that information to form an anticipated minutia DB 98.

The dynamic key crypto provider 10 routinely performs industry minutia cataloguing 86 processes for ultimately amassing an industry update catalogue DB 96. This database is for managing a vast but finite collection of industry minutia. Large scale searches, interpolation, multi-upgrade permutation modeling and probability calculations are performed against the data found in the industry update catalogue DB 96.

The industry minutia cataloguing 86 process uses computer industry research 90 to heuristically and empirically perform a minutia update collection 88 process. The minutia update collection 88 process scours a network 16 (for example, the Internet) seeking out information from software manufacturers 80, computer hardware manufacturers 82 and firmware manufacturers 84. Software manufacturers 80 may include, among other entities, software manufacturers, online software storefronts, support services for software, and some operating systems. Computer hardware manufacturers 82 may include, among other entities, manufacturers of PCs, laptops, tablets, smart phones, purpose-built computers, and other hardware often capable of connecting to a network 16. Firmware manufacturers 84 may include, among other entities, software related to hardware (commonly called drivers), some operating system software, software for configuring and controlling access to a network 16 such as a mobile operator network, or public and private cloud networks.

The minutia update collection 88 process collects such information as the computer industry research 90 process may deem beneficial to system 500. The collected data is then given to a data modeling, heuristics and permutations 92 process for analysis with regard, for example, to computer or user device identification. The data modeling, heuristics and permutations 92 process considers historical minutia trends and data mining 94 as well as the current minutia DB 70, the current anticipated minutia DB 98 and the event log 12 which may log actions and exchanges performed by the dynamic key crypto provider 10 for auditing and heuristic analysis at later times. The industry updates themselves can be grouped and related such that one minutia update in the industry update catalogue DB 96 can trigger expected changes in other related minutia values. For example, if an operating system industry update is shown to change fifteen minutia values and the minutia values are not affected by service user 20 usage (including, e.g., build number, build name, subsystem versions, system sizes), then these minutia values can be grouped and inferred or validated collectively in the data modeling, heuristics and permutations 92 process.

Other related minutia values may change as a result of service user 20 usages. This is related but different to service user 20 behavior patterns; minutia values in minutia DB 70 (such as minutia values related to the computer 18) establish the behavior of the minutiae (such as computer 18) and, therefore, behavioral algorithms can be applied to the minutia DB 70 values. For example, if the computer 18 repeatedly connects to a secured wireless LAN (such as one provided by an employer) when the computer 18 is in its 'work' environment during business hours, this could imply a third-party trust of the computer 18 (via, e.g., MAC address validation, WEP key authentication) by the secured wireless LAN; failure to connect under 'normal' working conditions could signal a change such as a lost device or new job. As another example, if values in the minutia DB 70 show that an address book has consistently added addresses over a time period reaching hundreds of names and suddenly the address name count goes to eighty, that could signal ownership by a new service user 20.

From data collected and modeled, the data modeling, heuristics and permutations 92 process records possible minutia values in the anticipated minutia DB 98. The data stored in the anticipated minutia DB 98 is pre-calculated combinations of industry update catalogue DB 96 and minutia DB 70 which are managed and ordered according to probability within

the database so that rapid derivative comparisons can be verified and scored against a confidence scale.

For example, when computer industry research 90 discovers a pending operating system release, the minutia update collection 88 process can gather a copy of the newly released operating system from, again for example, the appropriate firmware manufacturers 84. The new operating system is processed by the data modeling, heuristics and permutations 92 function and the resultant minutia stored in the anticipated minutia DB 98 for later use by system 500.

As another example of anticipated minutia, for minutia that represents system counters, the counter information collected from the minutia DB 70 can be increased an allowable range as determined by the data modeling, heuristics and permutations 92 process. All counter values within the allowable range would then be stored in the anticipated minutia DB 98.

In most cases, the data modeling, heuristics and permutations 92 process and the historical minutia trends and data mining 94 process calculate a probability and confidence scoring related to the values stored in the anticipated minutia DB 98. These probability and confidence scoring values are a determinative factor in the confidence scoring system for computer authentication.

Figure 6 illustrates a system 600 for scoring, confidence rating and step-up processing in accordance with an embodiment. Figure 6 shows a system 600 for computing a minutia validation scoring 140, comparing the scoring against a threshold defined by the service provider 14 and taking additional actions to process SP step-up request 150 in an effort to increase the scoring over the desired threshold.

The dynamic key crypto provider 10 contains a subsystem for the minutia validation scoring 140. The minutia validation scoring 140 subsystem receives a response validated using the subsystem 200 defined in Figure 2. The compute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98. Information in the valid responses 130 database includes both information representative of the current state of computer minutia on the computer 18 and anticipated minutia from industry sources and service user 20 norms, both

of which are described in previous figures and in Figure 9 with regard to the service provider app 44 subsystem 900.

For example, the scoring for hardware minutiae might be typically higher than the scoring for software minutiae. Firmware minutia values that change as expected may also have a higher confidence scoring. Likewise, software minutiae (such as date) that change as expected may positively affect the overall scoring of the response.

Some minutiae value changes, while possibly anticipated, may negatively affect the overall scoring of the response. For example, if a counter value takes an unusually large jump, it will negatively affect scoring. Also, if firmware minutiae values do not reflect routine updating as per industry norms, the scoring may be negatively affected. In addition, if a computer reset is detected that resets a wide range of minutia back to a known factory default, the resulting score may be lower.

Some minutiae themselves score differently. For example, certain software minutiae may be more predictable and useful than others. So, when a more favored minutia or minutiae are used, the resultant scoring may be higher when compared to validation done with less desirable minutiae.

Because of the vast number of minutiae to be validated, another scoring input can be the time since a particular minutia value was last validated in a challenge and response exchange with the computer 18.

Information outside the scope of a single computer 18 may also impact the scoring. If several instances of a computer 18 are registered to a single service user 20 within a particular service provider 14 as shown in the minutia DB 70, the high number of registered computer 18 may negatively impact the scoring, especially if several computer 18 computers are considered to be equivalent (for example, three smart phones instead of one smart phone, one tablet and one laptop).

After compute score 144 is performed, the resulting score is compared against the initial threshold defined by the service provider 14 and typically sent up during the initial connection to the service provider 14. If the computed score >= threshold 142 then the send score to SP 148 process is used to return the score to the service provider 14 for further consideration.

If the score >= threshold 142 is not true, then the process SP step-up request 150 is performed. Note the similar process SP step-up request 150 process can be performed if the initial threshold or subsequent thresholds are not met, as defined by the service provider 14.

The process SP step-up request 150 performs a compare valid responses and threshold 152 to determine if a possible response and corresponding score are equal to or above the threshold using information from the valid responses 130 database. The process may be governed by a user impact heuristics 154 process which determines the best response and step-up manner in which to increase the score.

If any score >= threshold 156 is true, then specific minutiae as defined in the use selected minutia elements 168 may be used to formulate challenge 116 and system 600 will continue using the system 200 shown in Figure 2. In this manner, the service users 20 may not be inconvenienced by having to take an action.

If current score + 2nd >= threshold 158 is true, then the use three identity factors 170 process may request the dynamic key crypto provider 10 to direct the dynamic key crypto library 56 to collect service user 20 secrets or biometric minutia using computer 18.

If new score + 2nd >= threshold 160 then both the new, selected minutia challenge and the use three identity factors 170 processes may be triggered.

If there is no way for a new, selected minutia challenge to achieve a score equal to or higher than the threshold requested by service provider 14, then the send validation failure to SP 162 process is performed.

When the service provider 14 receives a scoring from the Minutia validation scoring 140 from the dynamic key crypto provider 10, it first determines if a step failure 172 occurred. If this is the case, the dynamic key crypto provider 10 is unable to match the threshold desired by the service provider 14. The service provider 14 must then determine how to respond in the validation failure process 180 which, for example, can include denying the service request or conducting an out-of-band identity proofing of the service user 20 that might trigger a new computer 18 registration as shown in Figure 4.

If the score from the dynamic key crypto provider 10 is not a step-up failure as determined in step failure 172, then the SP risk process 174 compares the score against its own risk tables for the service action requested by the service user 20. If the score >= threshold 142 then the allow user action 182 may be performed; the confidence in the

computer 18 and optional service user 20 may be sufficient for the service provider 14 to allow the requested action.

If the score >= threshold 142 fails, then the request step-up authentication from dynamic key crypto 178 process requests the dynamic key crypto provider 10 to perform a process SP step-up request 150 in an effort to get a scoring above the desired threshold.

Figure 7 illustrates an authentication system 700 in accordance with an embodiment. Figure 7 shows a system 700 for dynamic key cryptography authentication possibly using minutiae from the three identity factors (have, know and are) found on computer 18 or collected from a service user 20.

When a PIN or password entry is required, for example, as a second identity factor to computer 18 identification, the dynamic key crypto provider 10 may perform a use service PIN 250 decision to determine whether a service PIN native to the computer 18 is used or a PIN specific to the service provider 14 is used according to data stored in the SP info and IDs 32 database. The service provider 14 can mandate the use of a service PIN or mandate or allow that the native computer 18 PIN (or password) be used.

The dynamic key crypto provider 10 can request a service user 10 PIN entry by the challenge process described in Figure 2. In such case, the unpack challenge 108 process can enable the fetch key minutia 58 process to determine a PIN minutia request in the challenge and query use service PIN 250 to determine true or false.

The dynamic key crypto provider 10 can request either the computer 18 (if such functionality exists) to display system PIN 256 or the dynamic key crypto library 56 running on the computer 18 to perform the display service PIN 254 entry processes.

If the service provider 14 allows a PIN native to the computer 18 and the computer 18 is capable of a process to display system PIN 256, then a computer 18 process similar to (or possibly the same as) the display system PIN 256 process is called by the computer 18.

If a use service PIN 250 is yes or a computer 18 is not capable of being remotely directed to display system PIN 256, then the dynamic key crypto library 56 performs the display service PIN 254 entry process.

If use service PIN 250 is not required, then the dynamic key crypto library 56 determines if system PIN in use 252 is yes. If system PIN in use 252 is yes, then the computer 18 native PIN (or password) screen is displayed via the display system PIN 256

process as if, for example, the computer 18 'timed out' and the service user 20 was prompted to re-enter their PIN.

If use service PIN 250 is yes or a system PIN in use 252 is no, then the dynamic key crypto library 56 performs the display service PIN 254 process and a custom PIN entry screen is shown. The valid PIN can be a pre-determined number between the service provider 14 and the service user 20 or can be set during the computer system registration system in Figure 4 as part of the proof the install 76 process or some other registration process.

Regardless of the PIN screen displayed, the service user 20 enters a PIN into the computer 18 using the secrets and biometric minutia 26 information the service user 20 possesses. When the system PIN in use 252 is true the validation of the PIN is performed by the computer 18 itself. When a correct PIN is entered, the dynamic key crypto library 56 can perform a get time since last successful PIN event 260 process and return the new time since a valid last PIN entry to the dynamic key crypto provider 10. In this manner, a service user 20 may not have to enter multiple PINs or the same PIN multiple times to show they are in possession of the device; the system PIN acts a universal PIN for all protected service provider apps 44 running on the computer 18. When use service PIN 250 is true, the dynamic key crypto library 56 uses the PIN value entered by the service user 20 into the computer 18 to calculate actual response 106 which is then returned to the dynamic key crypto provider 10 for validation as described in Figure 2.

If a valid PIN entry is not performed, the dynamic key crypto library 56 may time-out and return the failure to the dynamic key crypto provider 10.

In another example, the fetch key minutia 58 process may result in a process biometric request 262. In such case, the get biometric minutia 264 process will interact with the computer 18 to collect the secret and biometric minutia 26 data from service user 20 via entry into computer 18. The biometric minutia values can then be used to calculate actual response 106 which is then returned to the dynamic key crypto provider for validation as described in Figure 2.

In still another example, the fetch key minutia 58 process may determine a digital signature 258 is requested and perform a digital signature via a substitute message hash for random number 242 process. In this manner, the hash or digest of an action (such as a

transaction receipt or other summary) can be signed by the minutia returned by the fetch key minutia 58 process using the calculate actual response 106 process. The fetch key minutia 58 process may fetch any number of minutia values covering any or all of the three factors of identity ("have", "know", and "are", e.g., respectively, the computer 18, the secrets service user 20 knows or represents or biometric minutia (from secrets and biometric minutia 26)).

As an illustrative example, to form a digital signature, the contents of a message can be hashed so that changes to the message contents form a different hash and any changes to the message become evident. The hash can then be 'signed' (encrypted) using a dynamic crypto key that contains minutiae that represent the computer 18 on which the signature occurred including relatively stable minutia (e.g., hardware minutia), geo-location minutia, and fast changing minutia (e.g., date, counters) that establish the computer 18 on which the signature was performed, where the signature was performed and multiple minutia values that collectively could validate when the signature occurred. In addition, the minutia used to form the signing dynamic crypto key could include secrets (e.g., PIN) that only a service user 20 should know and biometric minutia (e.g., facial geometry) that only a service user 20 could produce to establish who digitally signed the digest. In this manner, the dynamic crypto key can bind the instrument, place, time and person to a particular message. Thus, a very wide range of minutia can be used in the dynamic signature key (not a single triplet, but potentially dozens or even hundreds of minutia values). Furthermore, the behavioral trajectory of the computer 18 could be considered before and after the signature to lend credibility to the digital signature performed.

Figure 8 illustrates a system 800 for application processing for data protection security functions in accordance with an embodiment. Figure 8 shows a system 800 for processing interaction between the service provider app 44 and the dynamic key crypto library 56 to improve the security of both while running on a computer 18.

On the computer 18, the service provider app 44 may have been installed which contains a dynamic key crypto library 56 which may be unique to the service provider 14. The dynamic key crypto library 56 can process responses from the dynamic key crypto provider 10 to establish a heartbeat and chatter 194, possibly triggering a delete service from computer 236 self-destruction when there is no heartbeat 210 and randomize or obfuscating

dynamic key crypto library 56 activity through heartbeat and chatter 194 system calls to make it difficult to intercept sensitive actions.

The dynamic key crypto library 56 performs some of its activities in direct response to either calls by the service provider app 44 or the dynamic key crypto provider 10. For the randomization, obfuscation and sampling of the computer minutia 64, the dynamic key crypto library 56 can perform tasks while the service provider app 44 is idle, waiting for response from either the service user 20 or other external drivers; often this is referred to as waiting in the event loop.

The service provider app 44 can encrypt and decrypt data 190 to securely and privately store service provider 14 and service user 20 data on the computer 18 in encrypted service data 196. The encrypt and decrypt data 190 process can use the service key minutia selections 66 database to determine which minutia the fetch key minutia 58 process should fetch from the computer minutia 64 found on the computer 18 or the fetch key minutia 58 can receive instructions from the dynamic key crypto provider 10.

In this manner, the encrypt and decrypt data 190 process may not actually store the keys used in encrypting and decrypting data; the keys are computed as required from the computer minutia 64. Thus, when the encrypted service provider 14 data and service user 20 data is stored in the encrypted service data 196 database, it cannot be decrypted unless the same computer minutia 64 are present on the computer 18. Copying the service provider app 44 or encrypted service data 196 (or both) will not enable the decryption of the encrypted service data 196.

Encrypted data to be processed by encrypt and decrypt data 190 can be transmitted securely from the service provider 14 over a network 16 to the computer 18, input into computer 18 by service user 20 or generated locally on the computer 18 by the service provider app 44 or dynamic key crypto library 56. In the case where the encrypted service data 196 is added or changed by the service provider app 44 or dynamic key crypto library 56, the service provider 14 can be updated with the encrypted service data 196 over a secure communication between the computer 18 and the service provider 14 using the network 16. The encrypt and decrypt data 190 process is intended to function on data at rest on the computer 18, not data typically in transit over a network 16. However, the same key creation

processes based on computer minutia 64 found on the computer 18 can be used for many types of data protection.

The dynamic key crypto library 56 can also enable a local computer check 192 which uses the encrypt and decrypt data 190 to randomly validate computer minutia 64. In this manner, random data can be encrypted and, at a later time, decrypted to verify the computer minutia 64 are still valid, and thus the service provider app 44 is running on the intended computer 18. Similar verifications can be made by the dynamic key crypto provider 10 using challenge, response, and validation system 200 described in Figure 2.

Since the computer minutia 64 may contain minutia that change with normal use and time, the encrypt and decrypt data 190 may fail after those changes. For fault tolerance of the system, the encrypt and decrypt data 190 can process the data using multiple subsets from the large range of possible computer minutia 64. In this manner, the encrypt and decrypt data 190 can compute several different copies of encrypted data based off a very wide range of computer minutia 64. The number of different instances of encryptions based off a single plain text source can be controlled by the dynamic key crypto library 56 which is customizable for each service provider 14.

When encrypting plain text data, the encrypt and decrypt data 190 process uses the fetch key minutia 58 process the required number of times as controlled by the dynamic key crypto library 56. Each time a fetch key minutia 58 is performed, the corresponding minutia indexes are read from the service key minutia selections 66 and the resultant computer minutia 64 is read. The service key minutia selections 66 can be, for example, stored locally on computer 18, stored in a secure element on computer 18, or stored in the dynamic key crypto provider 10 data and be directed using the challenge, response, and validation system 200 described in Figure 2. Each return of fetch key minutia 58 contains a set of minutia values hashed and used by the encrypt and decrypt data 190 process to encrypt the plain text data and stores the encrypted result in the encrypted service data 196. Thus, multiple encryptions of the same plain text may be stored in encrypted service data 196 database.

When attempting to decrypt data in encrypt and decrypt data 190 process, the fetch key minutia 58 process follows the same logic in determining the service key minutia selections 66 and then fetching the related minutia from the computer minutia 64. When the fetch key minutia 58 returns the minutia values to the encrypt and decrypt data 190, the

encrypt and decrypt data 190 retrieves the encrypted values from the encrypted service data 196 and uses a hash of the minutia values to decrypt the information.

If the decryption performed by the encrypt and decrypt data 190 does not properly decrypt the plain text – determined by some means of checksum, know plain text tests or other means in the valid decryption 202 determination – then the number of retries exhausted 206 is compared. If more encrypted instances of the plain text exist, then the next set of fetch key minutia 58 is performed which uses the service key minutia selections 66 to index another subset of minutia values which are then retrieved from the computer minutia 64 information.

This loop of fetch key minutia 58, valid decryption 202 and retries exhausted 206 is performed until a valid decryption of the data occurs or no more retries remain. If retries exhausted 206 returns true before a valid decryption of the data occurs, then the system faults and triggers a re-registration of the computer 18 as shown in Figure 4 or the original minutia values used when the encryption was done can be returned by the dynamic key crypto provider 10 to the dynamic key crypto library 56.

If a valid decryption 202 was found, then the encrypt and decrypt data 190 can perform a synch minutia with DKCP 201 on any minutia that failed to properly decrypt the plain text. When a synch minutia with DKCP 201 is performed, the changed minutia selections are indexed from the service key minutia selections 66, the changed minutia is read from the computer minutia 64 and given to the dynamic key crypto library 56 for secure transmission over the network 16 to the dynamic key crypto provider 10 which stores the updated minutia values in the minutia DB 70.

The synch minutia with DKCP 201 process can also perform an update library storage 208 function which calls on the encrypt and decrypt data 190 process to recalculate the failed decryptions using the new minutia found in the computer minutia 64.

When the dynamic key crypto library 56 connects to the dynamic key crypto provider 10 to update computer minutia of the computer 18, the dynamic key crypto provider 10 performs an authentication just as if the computer 18 was connecting to a service provider 14.

The dynamic key crypto library 56 can also have a heartbeat and chatter 194 process that, for example, may: 1) perform random activity on the computer 18; 2) function as a

heartbeat between the dynamic key crypto library 56 and the dynamic key crypto provider 10; and 3) obscure and obfuscate meaningful actions.

The heartbeat and chatter 194 process can periodically perform a response process 112 using a challenge sent by the dynamic key crypto provider 10. Recall that the dynamic key crypto provider 10 can send a number of challenges to the dynamic key crypto library 56 for later processing. In this manner (described in Figure 2) minutia values can be inferred and updated between the computer 18 and the dynamic key crypto provider 10.

This or a similar process can also serve as a heartbeat between the computer 18 and the dynamic key crypto provider 10. If the heartbeat and chatter 194 process does not perform a valid challenge and response cycle within a timeframe defined by service provider 14 and stored within their customized version of the dynamic key crypto library 56, as shown in the no heartbeat 210 decision, then the heartbeat and chatter 194 process can call the delete service from computer 236 process described in Figure 8.

The heartbeat and chatter 194 process may also periodically fetch random minutia 204 reads of the computer minutia 64 to utilize a wide search space for any malicious parties listening to systems calls made on the computer 18. The heartbeat and chatter 194 may also randomly call the local computer check 192 process.

The heartbeat and chatter 194 may perform all of these functions to improve security and obfuscate critical actions. The heartbeat and chatter 194 may be most often called during the event loop of a service provider app 44 so as not to impact performance. The heartbeat and chatter 194 process may also be intelligent so as not to overly use battery power, network bandwidth, or other system resources.

Figure 9 illustrates computer identity provider lifecycle functionality and services to service providers in accordance with an embodiment. Figure 9 shows a system 900 for managing the lifecycle of a service provider 14 and a computer 18 including deleting and transferring services from one computer 18 to a new computer 220 and notifying service provider systems 14 of a new computer 220.

The transfer service 226 process can be triggered by several events such as: 1) a new computer 220 being detected as a possible replacement to the computer 18; 2) a service user 20 requesting a service transfer to the service provider 14; 3) a reaction to either trigger 1 or

trigger 2, causing other service providers 230 to proactively transfer their service provider app 44.

When a new computer 220 performs the registration system 400 shown in Figure 4, if the dynamic key crypto provider 10 discovers that the account identifier supplied by the service provider 14 is already in use by a similar computer 18 (for example, a second smart phone) then a transfer service 238 message can be added as part of the registration process. If required, the service user 20 agrees to transfer service from their old computer 18, then the dynamic key crypto provider 10 can perform the transfer service 226 process.

When the service user 20 notifies the service provider 14 that their computer 18 is no longer valid due to loss, theft, replacement, or some other event, then the service provider 14 can request the dynamic key crypto provider 10 to perform a hold, delete, transfer service 232.

When a transfer service 226 process is performed, the dynamic key crypto provider 10 can perform a notify other service providers 228 process that notifies the other service providers 230 who have an account identifier registered to that particular computer 18. Upon notification, the dynamic key crypto provider 10 can share a SP confidence scoring 240 based off information in the SP info and IDs 32 database on the initiating service provider 14 to gauge the validity of the action. The other service providers 230 can, at their discretion, direct the dynamic key crypto provider 10 to perform a hold service 222, a transfer service 226, a delete service 224 or even take no action.

The notify other service providers 228 process stores only the minimal amount of service provider 14 information – such as pointer to the service provider 14 and an account identifier for the service user 20 – to link a computer 18 to a service provider 14; personal identifiable information of the service user 20 may not be stored or logged by the dynamic key crypto provider 10.

For a hold service 222, the dynamic key crypto provider 10 can update the minutia DB 70 such that it may send a send validation failure to SP 162 for the held computer 18 which will cause a validation failure process 180 to occur and, ultimately, may prompt contact of the service user 20 by the service provider 14 customer care effort.

For a delete service 224, the dynamic key crypto provider 10 can instruct the dynamic key crypto library 56 running on the target computer 18 to completely erase the encrypted

service data 196 and the service key minutia selections 66 if present, sending a confirmation erase send receipt and encrypted data 234 when the data stores are erased. After the send receipt and encrypted data 234 is sent, the dynamic key crypto library 56 can self-destruct by deleting the service provider app 44 if desired.

For a transfer service 226, the delete service 224 is called to affect the old computer 18. The service provider app delivery system 300 shown in Figure 3 is then performed. Afterward, the computer system registration system 400 in Figure 4 may then be performed to completely transfer the service from the old computer 18 to the new computer 220. The reloading of service and user data 24 may also be performed as described in Figure 8 with the data being encrypted to computer minutia 64 found on the new computer 220.

Both the delete service 224 and the transfer service 226 cause the minutia DB 70 to reflect the decommissioning of the old computer 18. The old computer 18 minutia data is not deleted from the minutia DB 70 so it can be recognized for other service providers 230 or if the computer 18 performs a new registration either maliciously or through other events such as giving or selling the computer 18 to another service user 20.

Various alternative embodiments are possible. For example, in one alternative embodiment, the dynamic key crypto provider 10 may be a multi-tier distribution model that supports tiered ecosystems of service provider systems 14. In this manner, the dynamic key crypto provider 10 presiding over an eco-system can resolve the minutia within the minutia DB 70 to determine that separate instances of a service provider 14 are referencing the same computer 18. This allows the dynamic key crypto provider 10 to perform the computer identity provider lifecycle functionality shown in Figure 9 on their own ecosystem. Only the top tier dynamic key crypto provider 10 can resolve the absolute minutia value from a computer 18. Certain data will need to be exported from the sub-tier dynamic key crypto provider 10 to the master dynamic key crypto provider 10 to facilitate the lifecycle functionality shown in Figure 9.

In various embodiments, parts of the dynamic key crypto provider 10 can be designed to run onsite for a particular service provider 14 to allow data ownership. Certain data will need to be exported from the onsite dynamic key crypto provider 10 to the master dynamic key crypto provider 10 to facilitate the lifecycle functionality shown in Figure 9.

Also, for example, the dynamic key crypto library 56 does not need to be included in a service provider app 44 in all cases. Some instances of a service provider 14 may not require additional application code at the computer 18 or may use a web browser as their service portal. In this case, the dynamic key crypto library 56 will still exist on the computer 18 but may be a stand-alone, callable routine or a shared resource for the computer 18. If the dynamic key crypto library 56 is a shared resource, certain application processing functions as shown in Figure 8 may be compartmentalized within the dynamic key crypto library 56 to achieve the same, for example, service provider 14 and encrypted service data 196 separation.

In another example, the service provider 14 may also have the ability to make system calls directly to the dynamic key crypto library 56 rather than through an interface of the service provider app 44.

In another example, service provider app 44 may not communicate directly with dynamic key crypto library 56, but communication performed via exchanges between service provider 14 and dynamic key crypto provider 10 who independently communicate with service provider app 44 and dynamic key crypto library 56, respectively.

In another example, challenges could be stored on the computer 18 to facilitate faster launch of the service provider app 44 and offline processing.

In another example, anomalies in computer 18 minutiae might also be used to detect computer malware or other abnormal processing considerations.

In another example, the challenge, response and validation described in system 200 could be originate from the computer 18 and be useful for service provider 14 authentication and protected data exchange; this enables mutual authentication and benefits for the system.

In another example, the dynamic key crypto system can facilitate digital rights management for content where the content can only be decrypted on a specific computer 18 by using computer minutiae 64 specifically from computer 18 and content can be only decrypted for viewing by a specific user when they enter secrets and biometric minutia 26.

In another example, the anticipated minutia DB 98 can be expanded to model biometric minutia from secrets and biometric minutia 26 to address maturity and aging of service user 20 for biometric minutiae such as, for example, voice and facial recognition.

In another example, some forms of a computer 18 that can connect to a network 16 may not be designed for service user 20 interaction, for example machine-to-machine systems. Embodiments may still be extremely useful in this case – for what else is there to identify than the computer 18 – but the secrets and biometric minutia functionality may not apply.

In various embodiments, the encrypt and decrypt data 190 process generally functions on service and user data 198 stored on the computer 18 locally in the encrypted service data 196 database. In another alternative embodiment, however, the same encryption key processing could be used to secure service and user data 198 as it is transferred over a network 16. In a similar manner, the minutia DB 70 maintained by the dynamic key crypto provider 10 may be used to decrypt the service and user data 198 when received from the computer 18.

Implementations of various embodiments may include computers connecting to the Internet or other networks and computers connecting to a network including but not limited to traditional PCs non-traditional PCs (i.e. smart phones, smart tablets); purpose-built network computers (i.e. smart meters, network equipment, appliances); and computers without a user interface (i.e. machine-to-machine functionality). Various embodiments may include identifying computers which connect to a network; identifying computers which connect to each other with or without concurrent connection to a wide-area network; authenticating computer connections to an online service; authenticating users to an online service; and encrypting information stored on a computer

In implementation of the various embodiments, embodiments of the invention may comprise a personal computing device, such as a personal computer, laptop, PDA, cellular phone or other personal computing or communication devices. The payment provider system may comprise a network computing computer, such as a server or a plurality of servers, computers, or processors, combined to define a computer system or network to provide the payment services provided by a payment provider system.

In this regard, a computer system may include a bus or other communication mechanism for communicating information, which interconnects subsystems and components, such as processing component (e.g., processor, micro-controller, digital signal processor (DSP), etc.), system memory component (e.g., RAM), static storage component

(e.g., ROM), disk drive component (e.g., magnetic or optical), network interface component (e.g., modem or Ethernet card), display component (e.g., CRT or LCD), input component (e.g., keyboard or keypad), and/or cursor control component (e.g., mouse or trackball). In one embodiment, disk drive component may comprise a database having one or more disk drive components.

The computer system may perform specific operations by processor and executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from another computer readable medium, such as static storage component or disk drive component. In other embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the embodiments.

Logic may be encoded in a computer readable and executable medium, which may refer to any medium that participates in providing instructions to the processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In one embodiment, the computer readable medium is non-transitory. In various implementations, non-volatile media includes optical or magnetic disks, such as disk drive component, volatile media includes dynamic memory, such as system memory component, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus. In one example, transmission media may take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

Some common forms of computer readable and executable media include, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, ROM, E2PROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted.

In various embodiments, execution of instruction sequences for practicing the invention may be performed by a computer system. In various other embodiments, a plurality of computer systems coupled by communication link (e.g., LAN, WLAN, PTSN, or various other wired or wireless networks) may perform instruction sequences to practice the invention in coordination with one another.

Computer system may transmit and receive messages, data, information and instructions, including one or more programs (i.e., application code) through communication link and communication interface. Received program code may be executed by processor as received and/or stored in disk drive component or some other non-volatile storage component for execution.

Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa – for example, a virtual implementation or a logical hardware implementation.

Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable and executable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

The foregoing disclosure is not intended to limit the present invention to the precise forms or particular fields of use disclosed. It is contemplated that various alternate embodiments or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described various example embodiments of the disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the invention. Thus, the invention is limited only by the claims.

CLAIMS

What is claimed is:

1. A method of dynamic key cryptography, the method comprising:

selecting a subset from a set of minutia types;

for a particular device, sending a challenge to the device, wherein:

the challenge includes information from which the device can collect actual values of minutia corresponding to the selected subset of minutia types in order to form a cryptographic key;

the cryptographic key is never transmitted from the device across any communication channel; and

the cryptographic key is used to encrypt an actual response to the challenge;

pre-processing a set of responses to the challenge based on tracking updates of minutia from which the selected subset of minutia types is selected, wherein:

the set of pre-processed responses covers a range of all actual responses possible to be received from the particular device if the combination of the particular device with collected actual values of minutia is valid;

comparing the actual response from the particular device to the set of pre-processed responses; and

validating the combination of the particular device with the collected actual values if the actual response is included in the set of pre-processed responses for the particular device.

2. The method of claim 1, wherein:

validating the combination of the particular device with the collected actual values enables one or more of authentication of the device, data protection for data transmitted to or from the device, or digital signature of a message digest.

3. The method of claim 1, wherein:

customization of the particular device differentiates the particular device from a second device, wherein: the particular device is differentiated from the second device if the

second device with a second set of actual values of minutia cannot be validated as the particular device with the collected actual values of minutia.

4. The method of claim 3, wherein:

increasing customization of the particular device increases differentiation of the particular device from the second device.

5. The method of claim 1, wherein:

validating the combination of the particular device with the collected actual values enables using the tracking of all known or projected updates of minutia to be used to update a device image for the particular device, without the actual response carrying any information about the current device image, and

a pattern of change in the device image is used with usage heuristics, consistency checks, or anomaly modeling for validating the combination of the particular device with the collected actual values.

6. The method of claim 1, wherein:

validating the combination of the particular device with the collected actual values enables using the cryptographic key to decrypt the response, without the cryptographic key ever having been sent across any communication channel.

7. The method of claim 1, wherein:

the set of minutia types includes one or more of hardware minutia, firmware minutia, software minutia, geo-location data, calling app data, user secrets, or biometric information.

8. The method of claim 1, wherein:

selecting the subset from the set of minutia types changes from one time to the next.

9. The method of claim 1, wherein:

a correspondence between values of minutia and the set of minutia types, from which the correspondence of values of minutia corresponding to the selected subset of minutia types is derived for the particular device, varies from device to device.

10. The method of claim 1, further comprising:

providing a dynamic key crypto library to the device for encrypting an actual response to the challenge.

11. The method of claim 1, wherein tracking updates of minutia includes:

tracking all known or projected updates by applying knowledge from the updates for selecting the subset of minutia types so that a pattern of change on the device can be detected, without the actual response carrying any information about the current device image, wherein

the pattern of change is used with usage heuristics, consistency checks, or anomaly modeling for validating the combination of the particular device with the collected actual values.

12. The method of claim 1, wherein:

the subset is selected to include a computer minutia type and at least one of a user secret minutia type and a biometric minutia type; and

a digital signature is provided using the cryptographic key, without the cryptographic key ever having been sent across any communication channel.

13. A method comprising:

selecting at least one type of minutia from a plurality of minutia types;

forming a challenge that conveys the selection of minutia types;

computing a plurality of pre-processed responses possible to receive from a valid device, wherein:

each pre-processed response is computed using a key; and

each key is computed using values that are possible for the selection of minutia types;

sending the challenge to the device;

receiving an actual response to the challenge from the device, wherein:

the actual response is computed using an actual key;

the actual key is computed using:

a deduction of the selection of minutia types from the challenge; and

actual values of the selection of minutia types;

comparing the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

14. The method of claim 13, wherein selecting further comprises:

choosing the selection of minutia from a plurality of minutia including hardware minutia, firmware minutia, software minutia, geo-location data, calling app data, user secrets, or biometric information.

15. The method of claim 13, wherein selecting further comprises:

choosing the selection of minutia to be a triplet of computer minutia types including a hardware minutia H, a firmware minutia F, and a software minutia S.

16. The method of claim 13, further comprising:

choosing the selection of minutia according to a particular cataloging scheme of minutia.

17. The method of claim 13, further comprising:

choosing the selection of minutia using expectations for changes to the current device image.

18. The method of claim 13, further comprising:

choosing the selection of device minutia using knowledge of all industry updates that can occur on the device, whether or not actually occurring on the device.

19. The method of claim 13, further comprising:

choosing the selection of device minutia using knowledge of changes actually occurring on the device, wherein:

changes actually occurring on the device are inferred from the pre-processed responses, and

no information about actual values of the minutia currently on the device is carried by the actual response to the challenge.

20. The method of claim 13, wherein:

choosing the selection of device minutia includes choosing triplets according to a cataloging scheme that varies from one issuer of the challenge to another.

21. The method of claim 13, further comprising:

using knowledge of the current device image to choose the selection of device minutiae.

22. The method of claim 13, further comprising:

using the actual response to update knowledge of the current device image.

23. The method of claim 13, wherein processing a range of possible changes to a current device image further comprises:

pre-processing all possible responses from the device independently of receiving the actual response from the device.

24. A system comprising a server configured to communicate with a device, wherein:

the server selects at least one type of minutia from a plurality of minutia types;

the server forms a challenge that conveys the selection of minutia types;

the server computes a plurality of pre-processed responses possible to receive from a valid device, wherein:

each pre-processed response is computed using a key; and

each key is computed using values that are possible for the selection of minutia types;

the server sends the challenge to the device;

the server receives an actual response to the challenge from the device, wherein:

the actual response is computed using an actual key;

the actual key is computed using:

a deduction of the selection of minutia types from the challenge; and

actual values of the selection of minutia types;

the server compares the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, the server validates the combination of the device with the actual values of the selection of minutia types.

25. The system of claim 24, wherein:

the second cryptographic key is varied by varying the selected set of minutia.

26. The system of claim 24, wherein:

the set of minutiae is a triplet including a hardware minutia H, a firmware minutia F, and a software minutia S.

27. The system of claim 24, wherein:

the server uses the actual response to update knowledge of the current device image without decoding any information about the current device image from the actual response.

28. The system of claim 24, wherein:

the server pre-processes all possible responses from the device independently of receiving the actual response from the device to calculate the plurality of pre-processed responses.

29. The system of claim 24, wherein:

the server uses knowledge of the current device image to select the set of minutiae.

30. A computer program product comprising a non-transitory computer readable medium having computer readable and executable code for instructing a processor to perform a method, the method comprising:

selecting at least one type of minutia from a plurality of minutia types;

forming a challenge that conveys the selection of minutia types;

computing a plurality of pre-processed responses possible to receive from a valid device, wherein:

each pre-processed response is computed using a key; and

each key is computed using values that are possible for the selection of minutia types;

sending the challenge to the device;

receiving an actual response to the challenge from the device, wherein:

the actual response is computed using an actual key;

the actual key is computed using:

a deduction of the selection of minutia types from the challenge; and

actual values of the selection of minutia types;

comparing the actual response to the pre-processed responses for a match; and

based on whether or not a match was found, validating the combination of the device with the actual values of the selection of minutia types.

31. The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia from a plurality of types of computer minutia including hardware minutia H, firmware minutia F, or software minutia S.

32. The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia according to a particular cataloging scheme of minutia.

33. The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia using knowledge of all industry updates that can occur on the device, whether or not any particular update actually has occurred on the device.

34. The computer program product of claim 30, wherein the method further comprises:

selecting the types of minutia using expectations for changes to the current device image.

ABSTRACT

Dynamic key cryptography validates mobile device users to cloud services by uniquely identifying the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device. Processes for uniquely identifying and validating the device include: selecting a subset of minutia from a plurality of minutia types; computing a challenge from which the user device can form a response based on the selected combination of minutia; computing a set of pre-processed responses that covers a range of all actual responses possible to be received from the device if the combination of the particular device with the device's collected actual values of minutia is valid; receiving an actual response to the challenge from the device; determining whether the actual response matches any of the pre-processed responses; and providing validation, enabling authentication, data protection, and digital signatures.

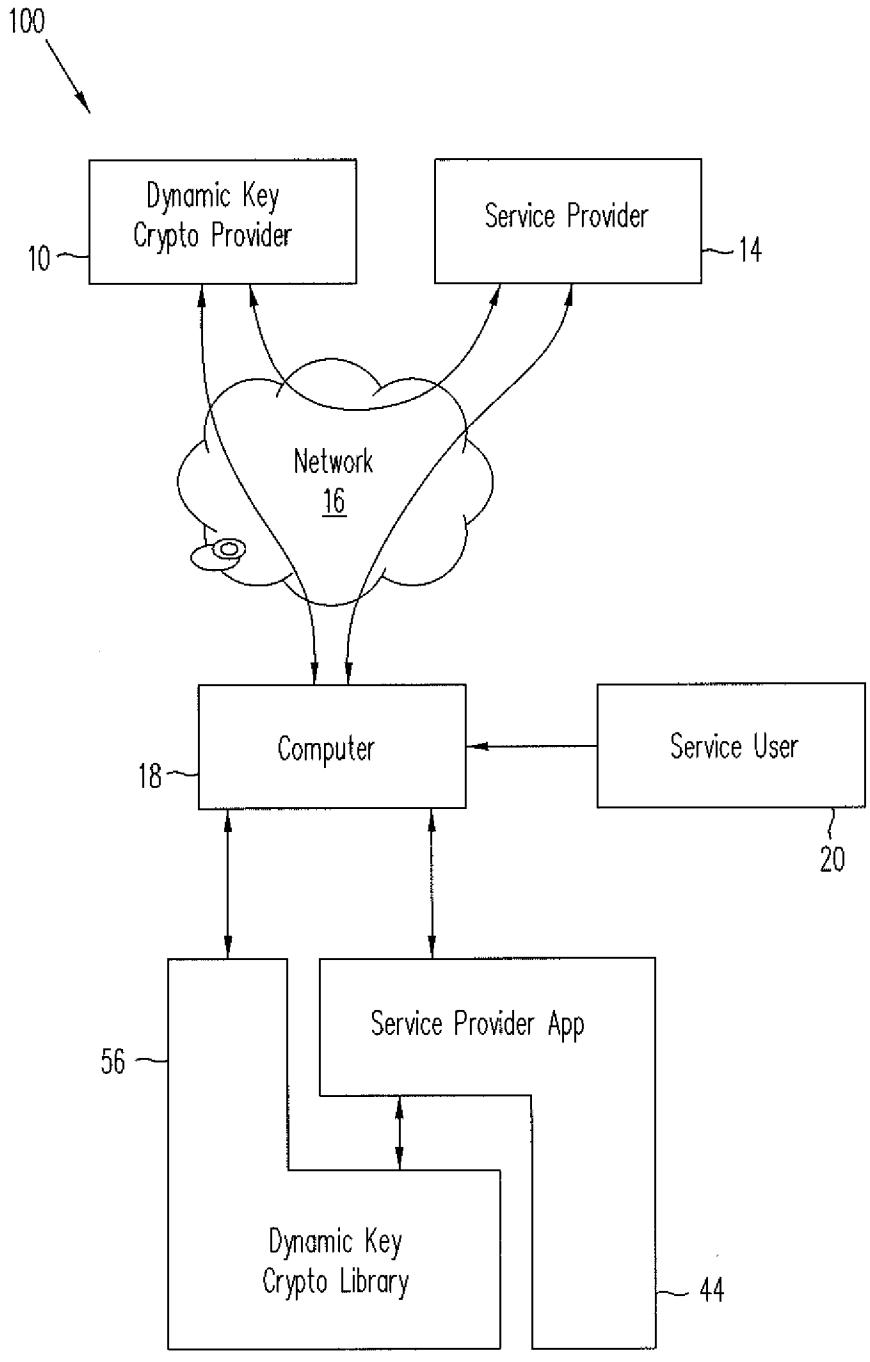
100
Dynamic Key
Crypto Provider
10
Service Provider
14
Network
16
Computer
18
Service User
20
Service Provider App
56
Dynamic Key
Crypto Library
44

FIG. 1

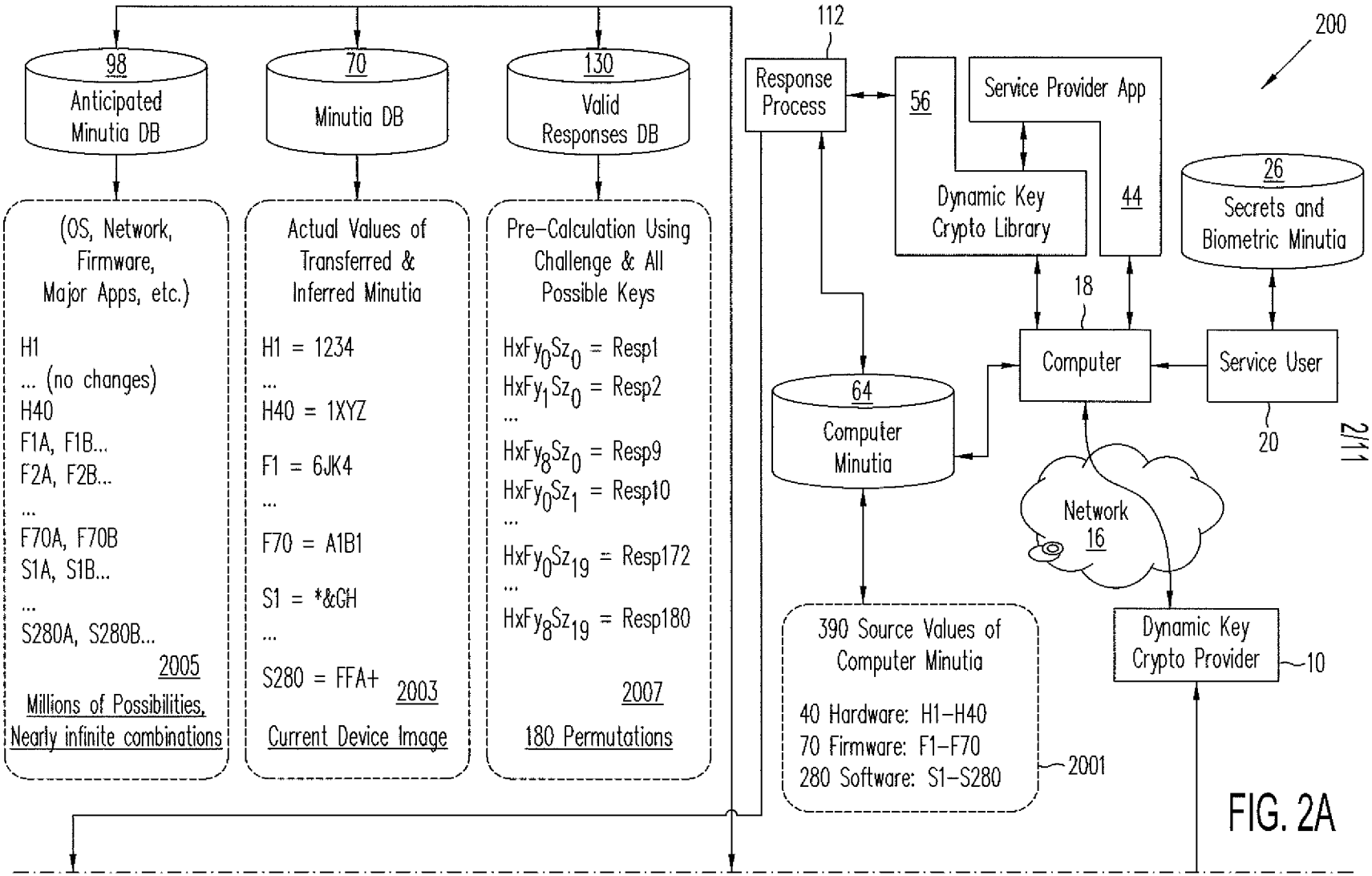
98
Anticipated Minutia DB
70
Minutia DB
130
Valid Responses DB
(OS, Network, Firmware, Major Apps, etc.)
H1
... (no changes)
H40
F1A, F1B...
F2A, F2B...
...
F70A, F70B
S1A, S1B...
...
S280A, S280B...
2005
Millions of Possibilities, Nearly infinite combinations
Actual Values of Transferred & Inferred Minutia
H1 = 1234
...
H40 = 1XYZ
F1 = 6JK4
...
F70 = A1B1
...
S1 = *&GH
...
S280 = FFA+
2003
Current Device Image
Pre-Calculation Using Challenge & All Possible Keys
HxFy0Sz0 = Resp1
HxFy1Sz0 = Resp2
...
HxFy8Sz0 = Resp9
HxFy0Sz1 = Resp10
...
HxFy0Sz19 = Resp172
...
HxFy8Sz19 = Resp180
2007
180 Permutations
112
Response Process
56
Service Provider App
Dynamic Key Crypto Library
44
200
26
Secrets and Biometric Minutia
18
Computer
Service User
20
64
Computer Minutia
Network
16
390 Source Values of Computer Minutia
40 Hardware: H1-H40
70 Firmware: F1-F70
280 Software: S1-S280
2001
Dynamic Key Crypto Provider
10
2/11

FIG. 2A

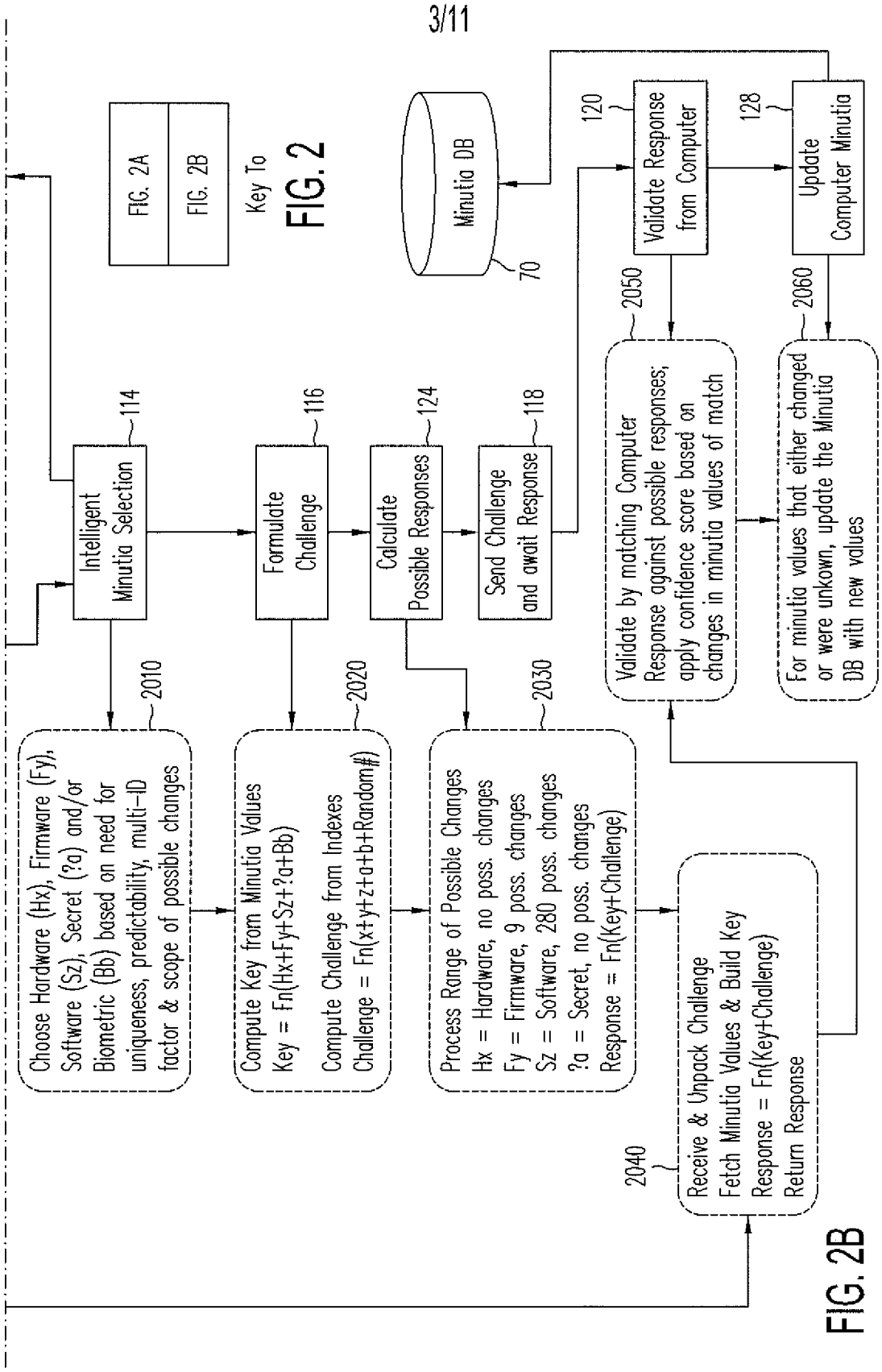
FIG. 2A
FIG. 2B
Key To
FIG. 2
Minutia DB
70
120
Validate Response from Computer
128
Update Computer Minutia
2050
2060
Intelligent Minutia Selection
114
Formulate Challenge
116
Calculate Possible Responses
124
Send Challenge and await Response
118
2010
2020
2030
Choose Hardware (Hx), Firmware (Fy), Software (Sz), Secret (?a) and/or Biometric (Bb) based on need for uniqueness, predictability, multi-ID factor & scope of possible changes
Compute Key from Minutia Values
Key = Fn(Hx+Fy+Sz+?a+Bb)
Compute Challenge from Indexes
Challenge = Fn(x+y+z+a+b+Random#)
Process Range of Possible Changes
Hx = Hardware, no poss. changes
Fy = Firmware, 9 poss. changes
Sz = Software, 280 poss. changes
?a = Secret, no poss. changes
Response = Fn(Key+Challenge)
Validate by matching Computer Response against possible responses; apply confidence score based on changes in minutia values of match
For minutia values that either changed or were unkown, update the Minutia DB with new values
2040
Receive & Unpack Challenge
Fetch Minutia Values & Build Key
Response = Fn(Key+Challenge)
Return Response

FIG. 2B

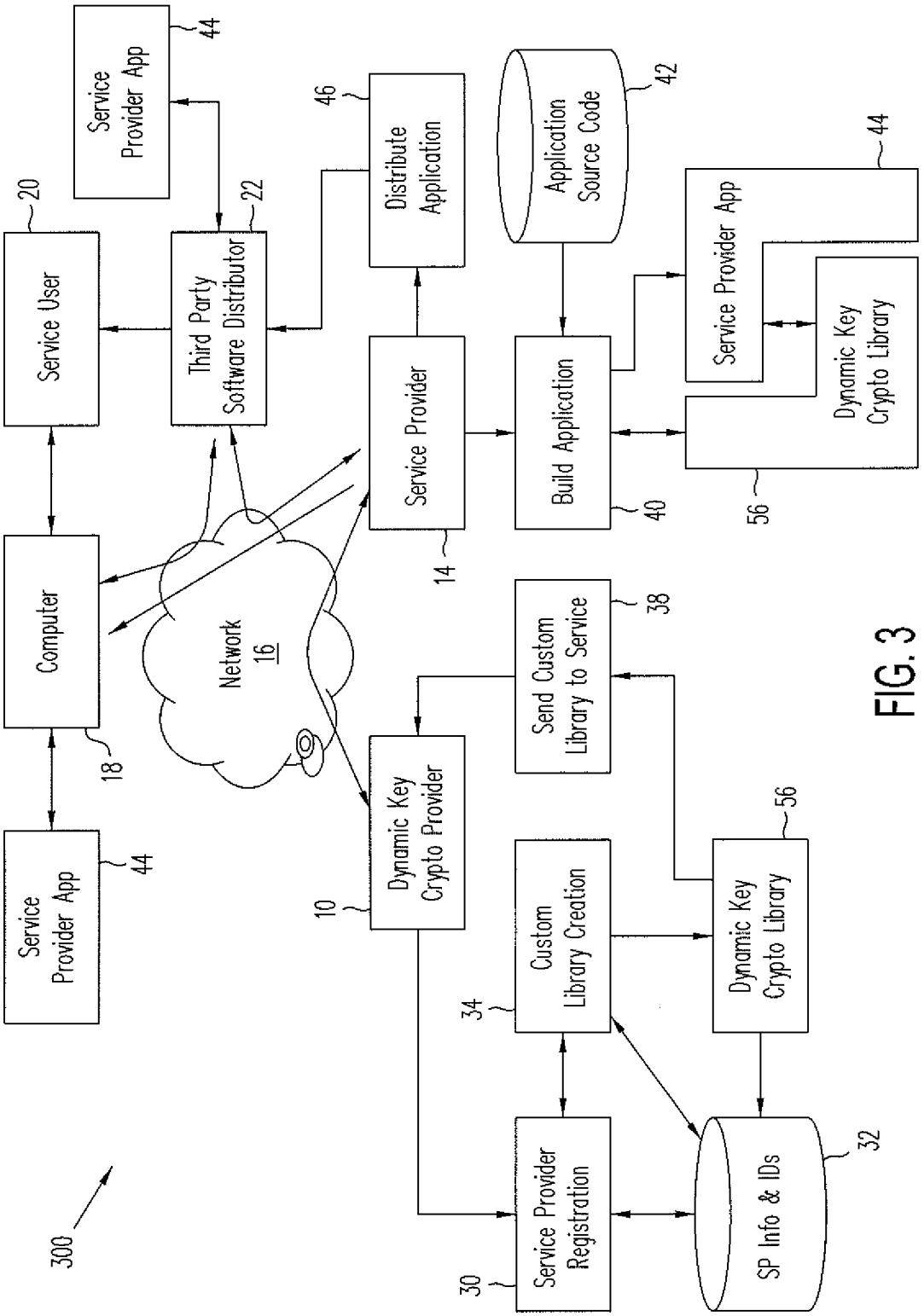
300
Service Provider App
44
Computer
18
Service User
20
Service Provider App
44
Third Party Software Distributor
22
Network 16
Distribute Application
46
Application Source Code
42
Service Provider
14
Build Application
40
Service Provider App
44
Dynamic Key Crypto Library
56
Send Custom Library to Service
38
Dynamic Key Crypto Provider
10
Custom Library Creation
34
Dynamic Key Crypto Library
56
Service Provider Registration
30
SP Info & IDs
32

FIG. 3

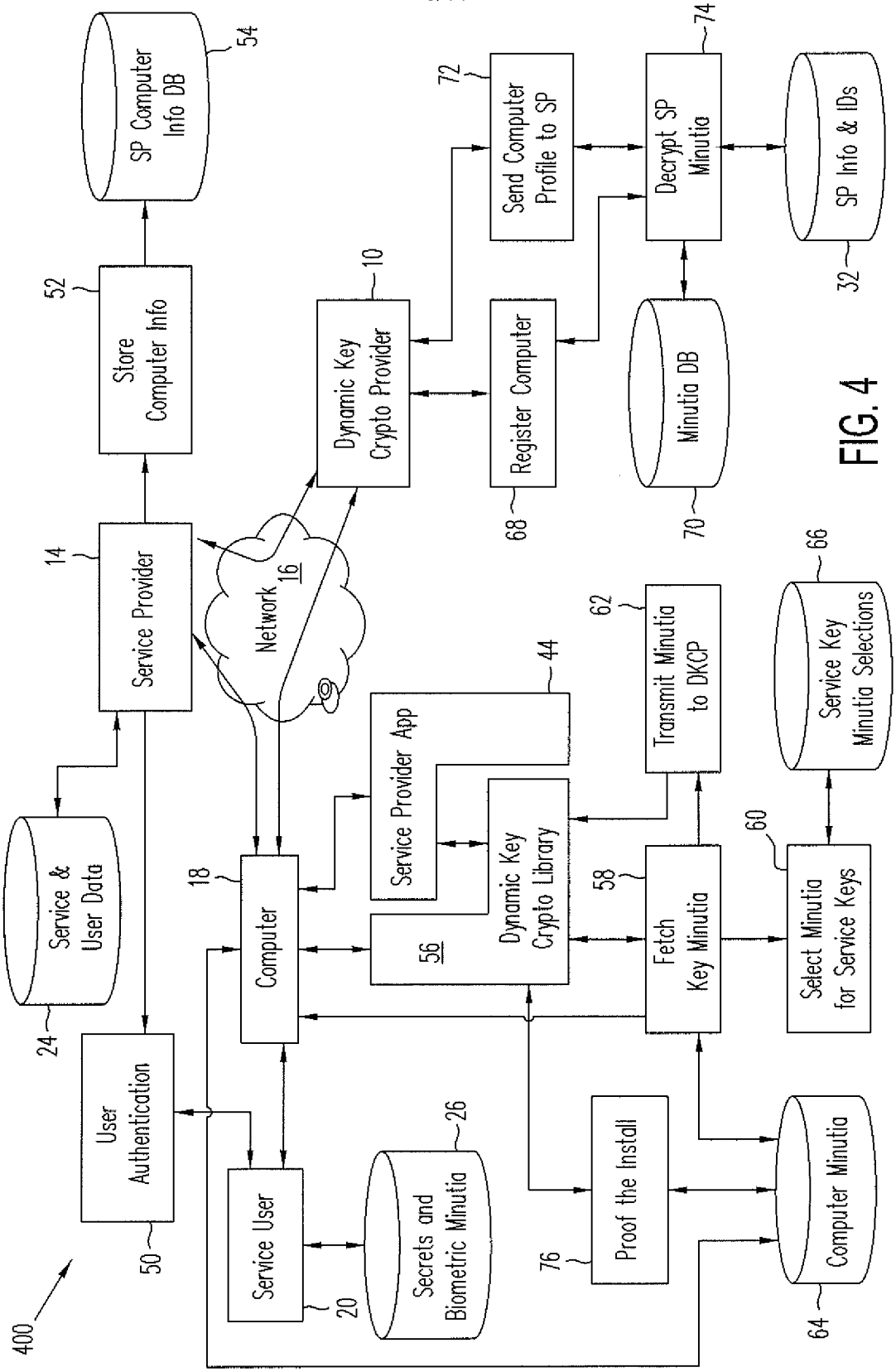
400
User Authentication
50
Service & User Data
24
Service Provider
14
Store Computer Info
52
SP Computer Info DB
54
Network
16
Dynamic Key Crypto Provider
10
Register Computer
68
Send Computer Profile to SP
72
Decrypt SP Minutia
74
SP Info & IDs
32
Minutia DB
70
Computer
18
Service Provider App
44
Dynamic Key Crypto Library
56
Transmit Minutia to DKCP
62
Service Key Minutia Selections
66
Fetch Key Minutia
58
Select Minutia for Service Keys
60
Service User
20
Secrets and Biometric Minutia
26
Proof the Install
76
Computer Minutia
64

FIG. 4

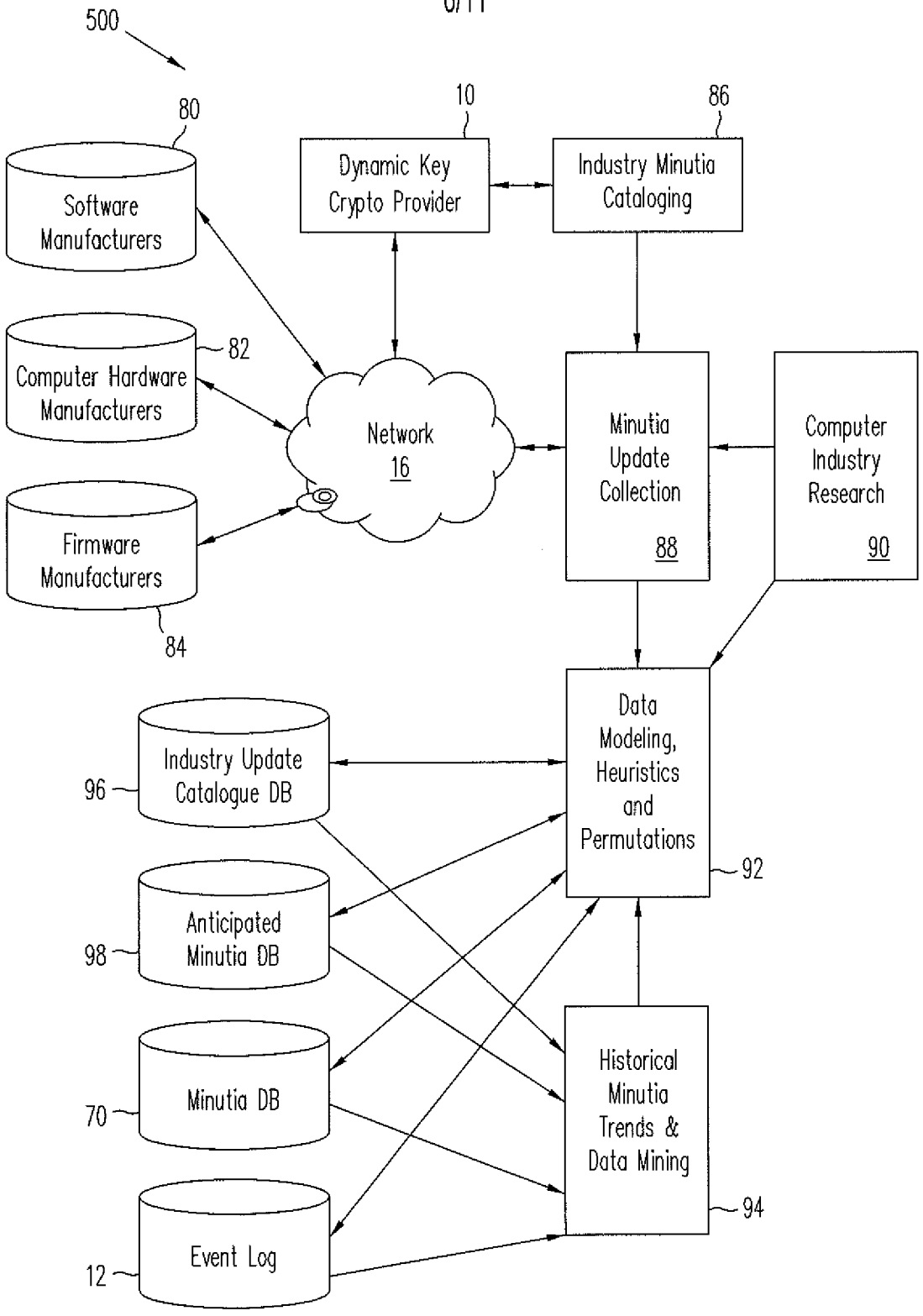
500
80
Software Manufacturers
10
Dynamic Key Crypto Provider
86
Industry Minutia Cataloging
82
Computer Hardware Manufacturers
Network 16
Minutia Update Collection 88
Computer Industry Research 90
Firmware Manufacturers
84
Data Modeling, Heuristics and Permutations
92
96
Industry Update Catalogue DB
98
Anticipated Minutia DB
70
Minutia DB
12
Event Log
Historical Minutia Trends & Data Mining
94

FIG. 5

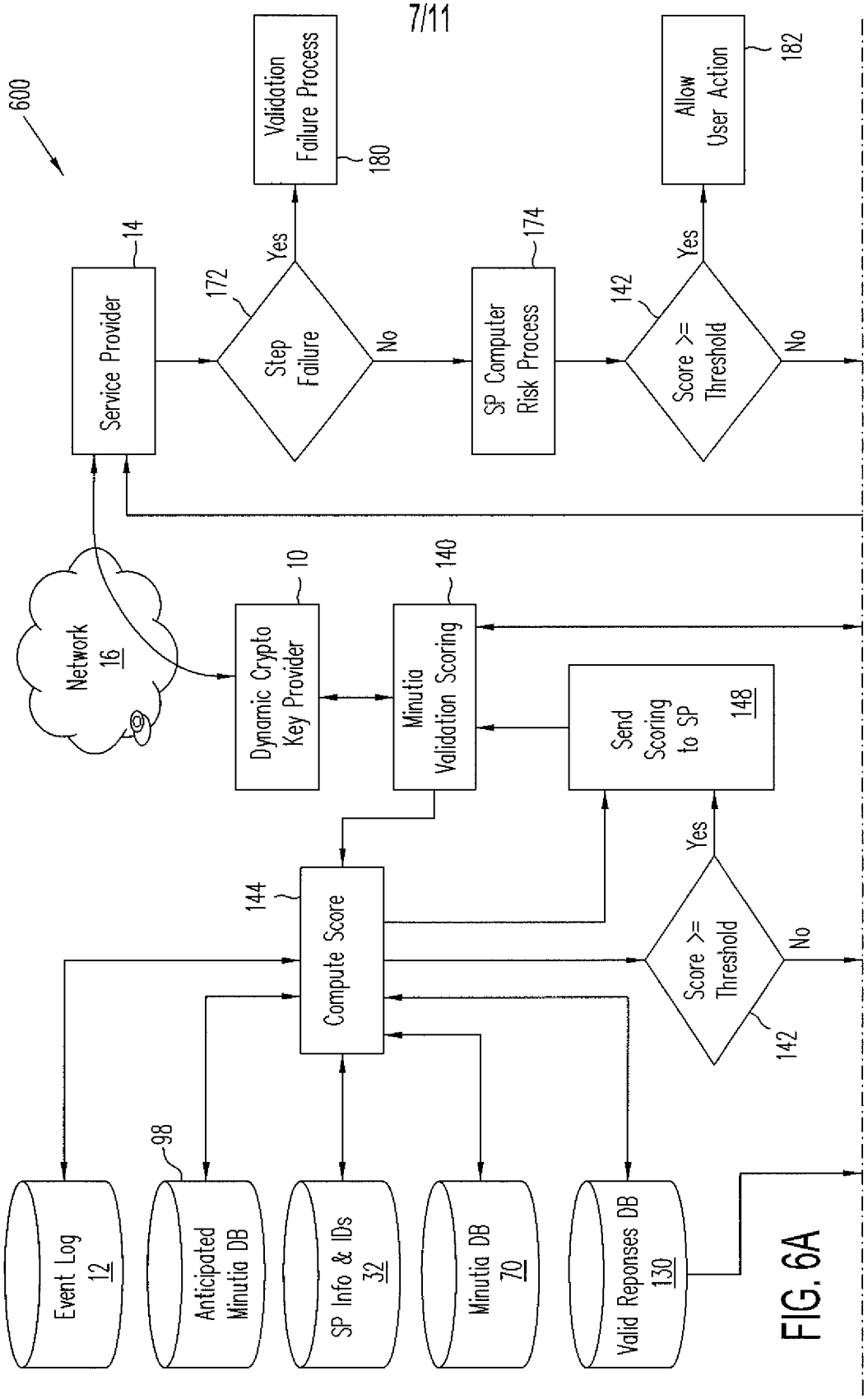
600
Service Provider
14
Step Failure
172
Yes
No
Validation Failure Process
180
SP Computer Risk Process
174
Score >= Threshold
142
Yes
No
Allow User Action
182
Network 16
Dynamic Crypto Key Provider
10
Minutia Validation Scoring
140
Send Scoring to SP
148
Compute Score
144
Score >= Threshold
142
Yes
No
Event Log 12
Anticipated Minutia DB
98
SP Info & IDs 32
Minutia DB 70
Valid Reponses DB 130

FIG. 6A

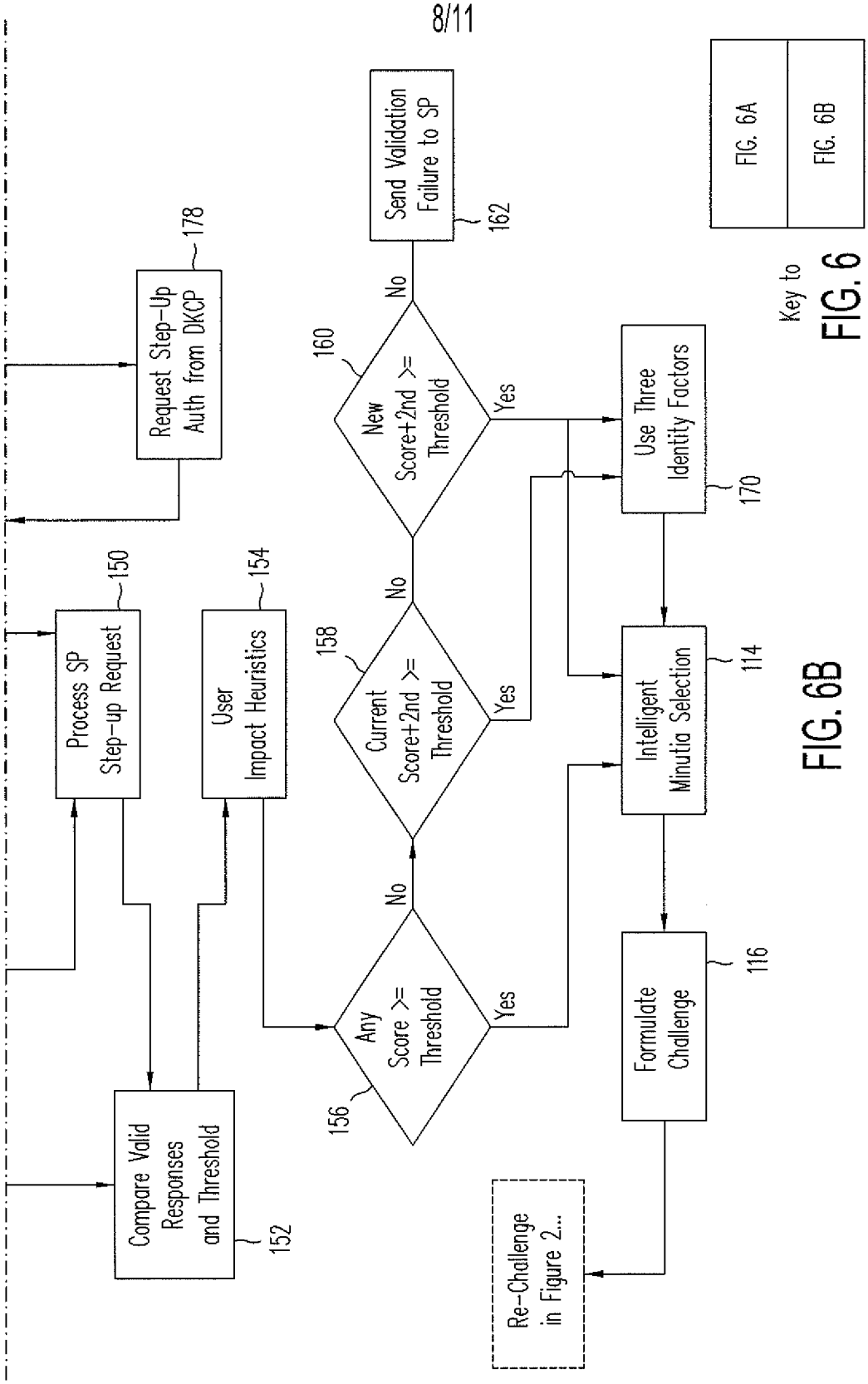
Request Step-Up Auth from DKCP
178
Process SP Step-up Request
150
User Impact Heuristics
154
Compare Valid Responses and Threshold
152
Any Score >= Threshold
156
No
Yes
Current Score+2nd >= Threshold
158
No
Yes
New Score+2nd >= Threshold
160
No
Yes
Send Validation Failure to SP
162
Use Three Identity Factors
170
Intelligent Minutia Selection
114
Formulate Challenge
116
Re-Challenge in Figure 2...
FIG. 6A
FIG. 6B
Key to
FIG. 6

FIG. 6B

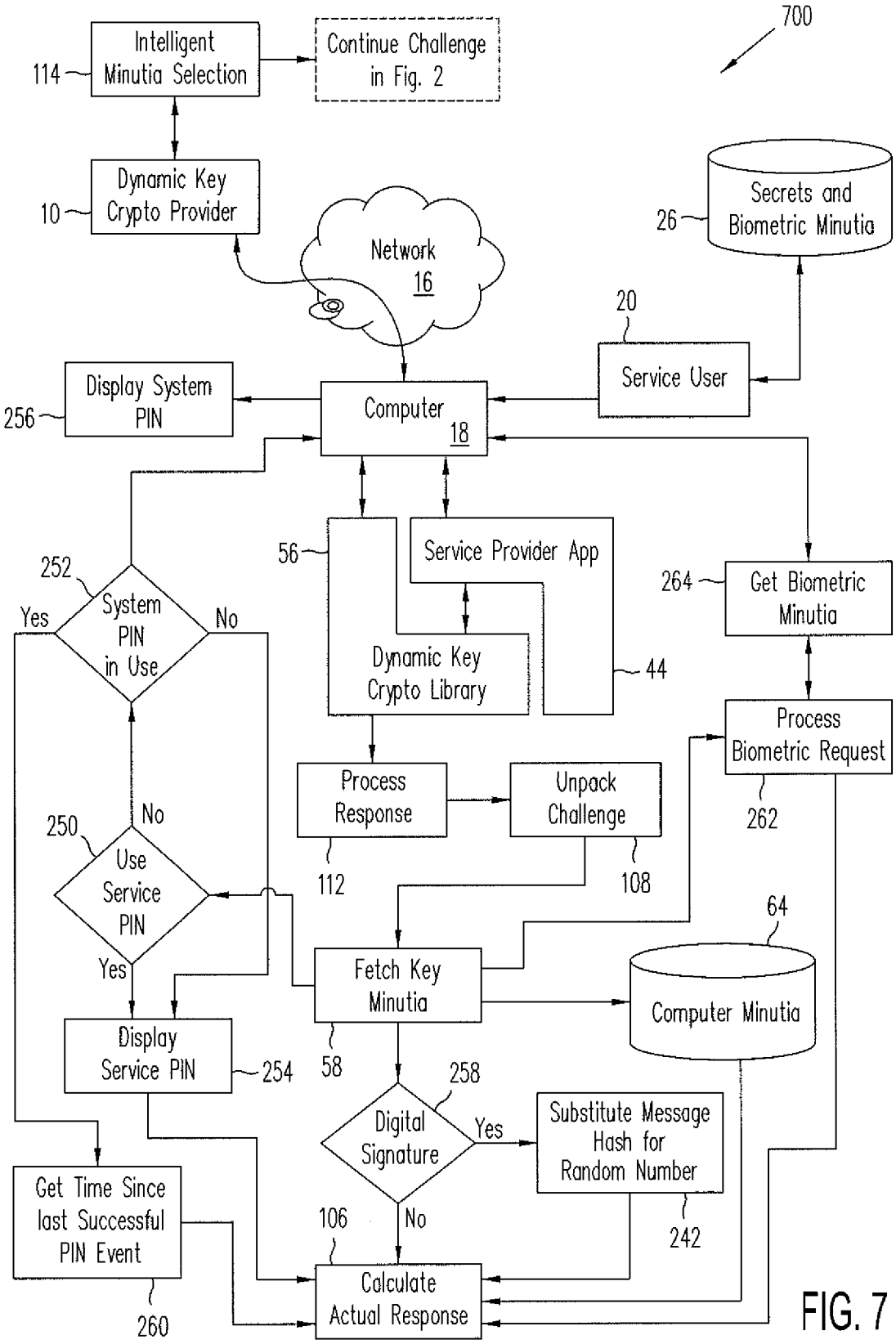
700
Intelligent Minutia Selection
114
Continue Challenge in Fig. 2
Dynamic Key Crypto Provider
10
Network 16
Secrets and Biometric Minutia
26
20
Service User
Display System PIN
256
Computer 18
56
Service Provider App
Dynamic Key Crypto Library
44
252
System PIN in Use
Yes
No
264
Get Biometric Minutia
Process Biometric Request
262
Process Response
112
Unpack Challenge
108
250
Use Service PIN
No
Yes
64
Fetch Key Minutia
Computer Minutia
Display Service PIN
254
58
258
Digital Signature
Yes
Substitute Message Hash for Random Number
242
Get Time Since last Successful PIN Event
260
106
No
Calculate Actual Response

FIG. 7

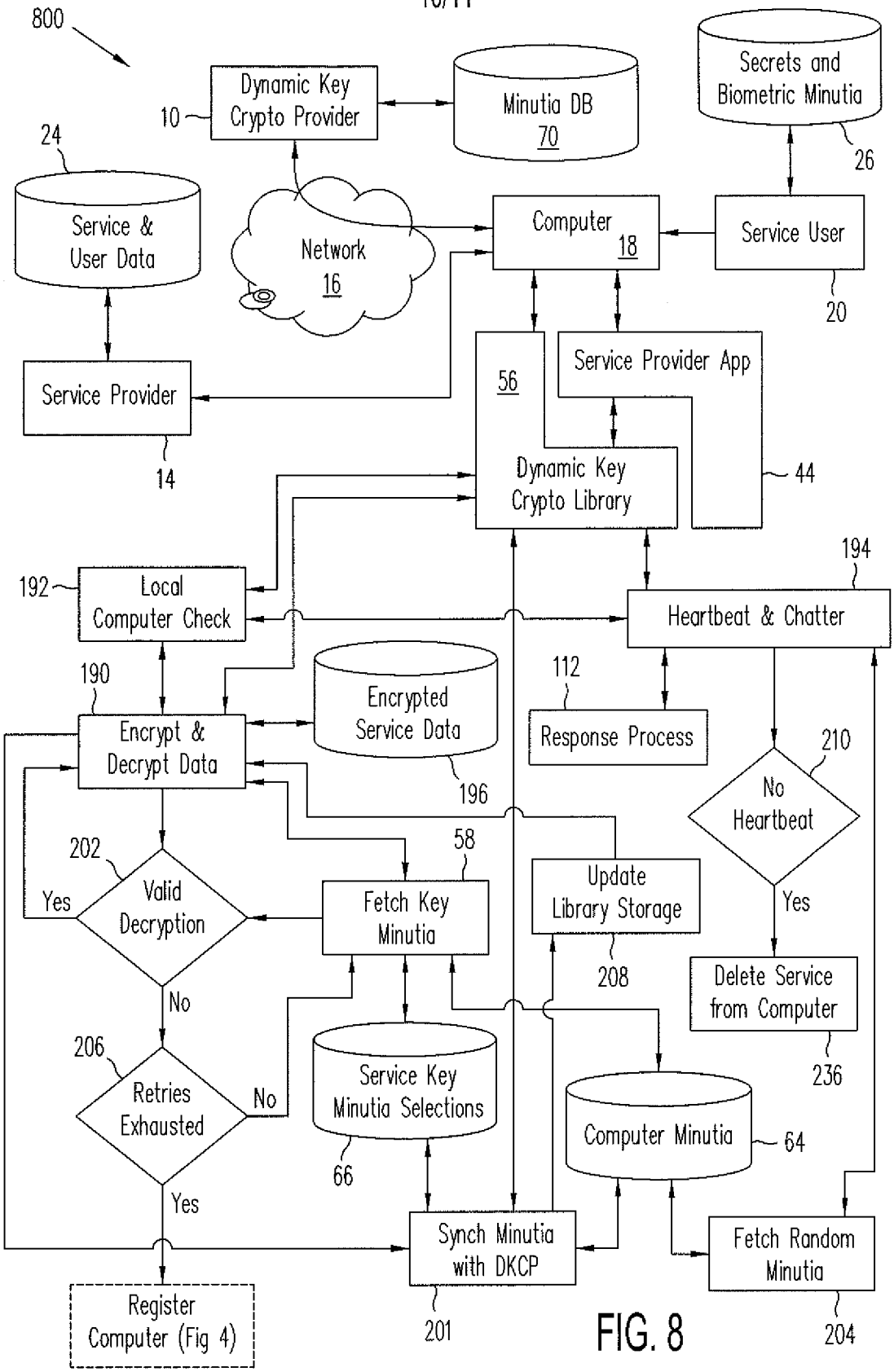
800
Dynamic Key Crypto Provider
10
Minutia DB 70
Secrets and Biometric Minutia
26
24
Service & User Data
Network 16
Computer 18
Service User
20
Service Provider
14
56
Service Provider App
Dynamic Key Crypto Library
44
192
Local Computer Check
194
Heartbeat & Chatter
190
Encrypted Service Data
196
112
Response Process
Encrypt & Decrypt Data
210
No Heartbeat
202
Valid Decryption
Yes
58
Fetch Key Minutia
Update Library Storage
208
Yes
Delete Service from Computer
236
No
206
Retries Exhausted
No
Service Key Minutia Selections
66
Computer Minutia
64
Yes
Synch Minutia with DKCP
201
Fetch Random Minutia
204
Register Computer (Fig 4)

FIG. 8

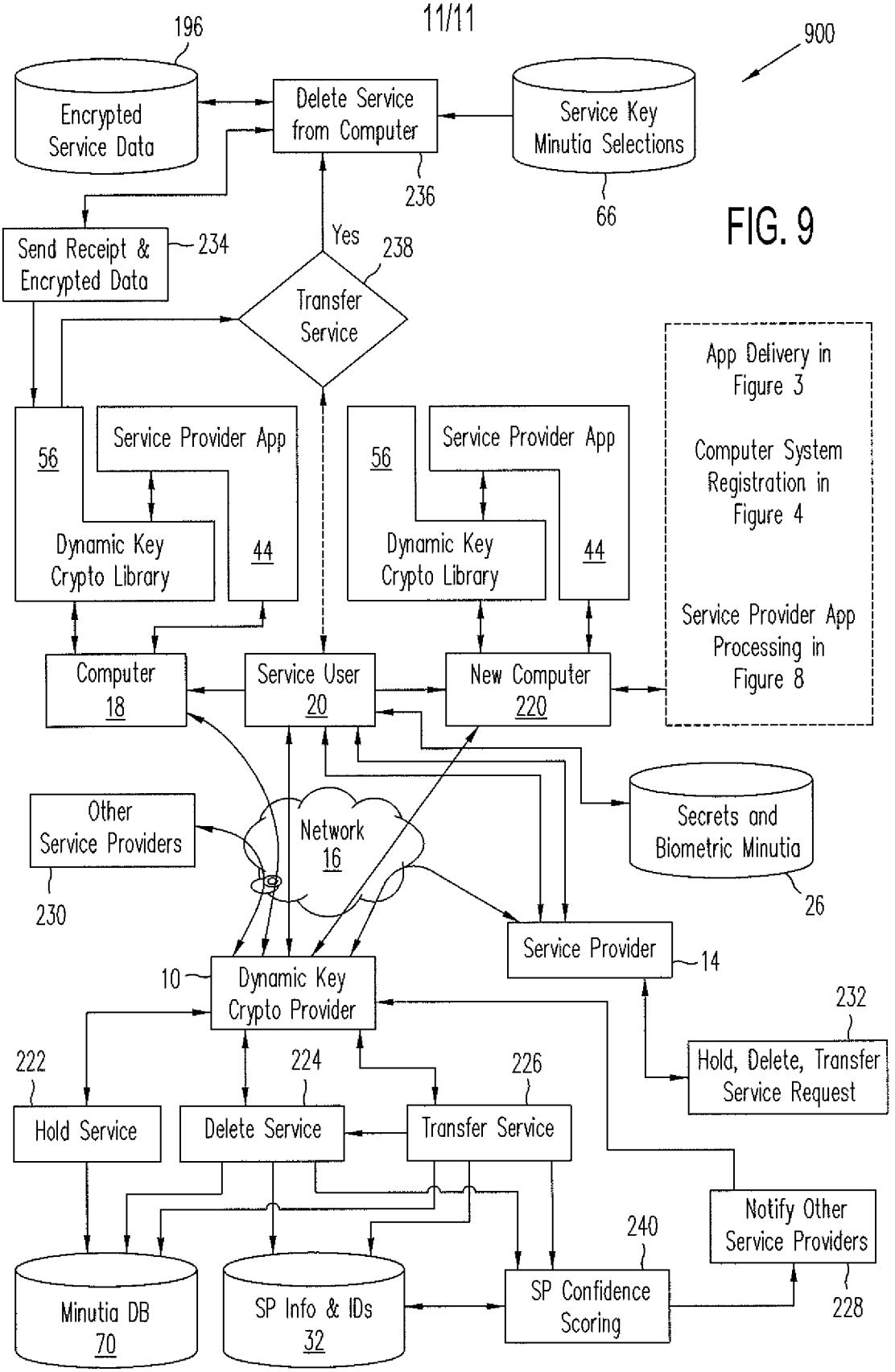
196
900
Encrypted Service Data
Delete Service from Computer
Service Key Minutia Selections
236
66
Send Receipt & Encrypted Data
234
Yes
238
Transfer Service
App Delivery in Figure 3
Computer System Registration in Figure 4
Service Provider App Processing in Figure 8
56
Service Provider App
Dynamic Key Crypto Library
44
56
Service Provider App
Dynamic Key Crypto Library
44
Computer 18
Service User 20
New Computer 220
Other Service Providers
230
Network 16
Secrets and Biometric Minutia
26
Service Provider
14
10
Dynamic Key Crypto Provider
232
Hold, Delete, Transfer Service Request
222
224
226
Hold Service
Delete Service
Transfer Service
Notify Other Service Providers
240
228
Minutia DB 70
SP Info & IDs 32
SP Confidence Scoring

FIG. 9

DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

As a below named inventor, I/we hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I/we believe I/we am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of subject matter (process, machine, manufacture, or composition of matter, or an improvement thereof) which is claimed and for which a patent is sought by way of the application entitled

CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE

which (check)
- ☒ is attached hereto.
- ☐ and is amended by the Preliminary Amendment attached hereto.
- ☐ was filed on as Application Serial No.
- ☐ and was amended on (if applicable).

I/we hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I/we acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I/we hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
Number	Country	Day/Month/Year Filed	Yes	No
			☐	☐

I/we hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Provisional Application Number	Filing Date
61/462,474	February 3, 2011

We hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or PCT international application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, we acknowledge the duty to disclose information, which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)

We hereby appoint the following practitioners to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Customer No. 27683

Please address all correspondence to: **Customer No. 27683**

Please direct all telephone calls to: **David Bowls**

Telephone: 949-202-3000
Facsimile: 949-202-3001

I declare that all statements made herein of my own knowledge are true, all statements made herein on information and belief are believed to be true, and all statements made herein are made with the knowledge that whoever, in any matter within the jurisdiction of the Patent and Trademark Office, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be subject to the penalties including fine or imprisonment or both as set forth under 18 U.S.C. 1001, and that violations of this paragraph may jeopardize the validity of the application or this document, or the validity or enforceability of any patent, trademark registration, or certificate resulting therefrom.

Full name of first joint inventor:	**Paul Timothy Miller**		
Inventor's Signature:		Date:	3 Feb 2012
Residence:	Irvine, California		
Post Office Address:	10 Wandering Rill	Citizenship:	US
	Irvine, California 92603		

Full name of first joint inventor:	**George Allen Tuvell**		
Inventor's Signature:		Date:	3 Feb 2012
Residence:	Thompson's Station, Tennessee		
Post Office Address:	2617 Clayton Arnold Road	Citizenship:	US
	Thompson's Station, Tennessee 37179		