This application is officially maintained in electronic form. To View: Click the desired Document Description. To Download and Print: Check the desired document(s) and click Start Download.

Available Documents

Mail Room Date	Document Code	Document Description	Document Category	Page Count
08-08-2012	ABN	Abandonment	PROSECUTION	2
04-19-2012	EABN	Letter Express Abandonment of the application	PROSECUTION	2
04-19-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
03-12-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
03-12-2012	NPL	Non Patent Literature	PROSECUTION	7
03-12-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
03-09-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
03-09-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
03-06-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
03-06-2012	NPL	Non Patent Literature	PROSECUTION	3
03-06-2012	NPL	Non Patent Literature	PROSECUTION	4
03-06-2012	NPL	Non Patent Literature	PROSECUTION	3
03-06-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
03-05-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
03-05-2012	NPL	Non Patent Literature	PROSECUTION	40
03-05-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
03-05-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
03-05-2012	FOR	Foreign Reference	PROSECUTION	16
03-05-2012	FOR	Foreign Reference	PROSECUTION	9
03-05-2012	FOR	Foreign Reference	PROSECUTION	12
03-05-2012	FOR	Foreign Reference	PROSECUTION	20
03-05-2012	FOR	Foreign Reference	PROSECUTION	13
03-05-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
01-14-2012	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
01-14-2012	NPL	Non Patent Literature	PROSECUTION	17
01-14-2012	NPL	Non Patent Literature	PROSECUTION	1
01-14-2012	N417	EFS Acknowledgment Receipt	PROSECUTION	2
11-22-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	4
11-22-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
10-11-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	1
10-11-2011	APP.FILE.REC	Filing Receipt	PROSECUTION	3
06-29-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	3
06-29-2011	TRAN.LET	Transmittal Letter	PROSECUTION	2
06-29-2011	NPL	Non Patent Literature	PROSECUTION	2
06-29-2011	NPL	Non Patent Literature	PROSECUTION	2
06-29-2011	NPL	Non Patent Literature	PROSECUTION	4
06-29-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
04-28-2011	NTC.PUB	Notice of Publication	PROSECUTION	1
03-04-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	2
03-04-2011	TRAN.LET	Transmittal Letter	PROSECUTION	2
03-04-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
02-10-2011	IDS	Information Disclosure Statement (IDS) Form	PROSECUTION	1

		(SB08)		
02-10-2011	NPL	Non Patent Literature	PROSECUTION	2
02-10-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
02-10-2011	NPL	Non Patent Literature	PROSECUTION	24
01-21-2011	NTC.MISS.PRT	Notice to File Missing Parts	PROSECUTION	2
01-21-2011	APP.FILE.REC	Filing Receipt	PROSECUTION	3
01-21-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	1
01-21-2011	WCLM	Claims Worksheet (PTO-2022)	PROSECUTION	1
01-21-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	2
01-21-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
01-11-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	2
01-11-2011	NPL	Non Patent Literature	PROSECUTION	30
01-11-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	2
01-06-2011	TRNA	Transmittal of New Application	PROSECUTION	2
01-06-2011	OATH	Oath or Declaration filed	PROSECUTION	4
01-06-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	6
01-06-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	2
01-06-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	2
01-06-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	3
01-06-2011	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	2
01-06-2011	DRW	Drawings-only black and white line drawings	PROSECUTION	7
01-06-2011	FOR	Foreign Reference	PROSECUTION	23
01-06-2011	FOR	Foreign Reference	PROSECUTION	53
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	6
01-06-2011	NPL	Non Patent Literature	PROSECUTION	1
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	1
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	4
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	3
01-06-2011	NPL	Non Patent Literature	PROSECUTION	1
01-06-2011	NPL	Non Patent Literature	PROSECUTION	5
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	1
01-06-2011	NPL	Non Patent Literature	PROSECUTION	5
01-06-2011	NPL	Non Patent Literature	PROSECUTION	10
01-06-2011	NPL	Non Patent Literature	PROSECUTION	21
01-06-2011	NPL	Non Patent Literature	PROSECUTION	9
01-06-2011	NPL	Non Patent Literature	PROSECUTION	7
01-06-2011	NPL	Non Patent Literature	PROSECUTION	31
01-06-2011	NPL	Non Patent Literature	PROSECUTION	2
01-06-2011	NPL	Non Patent Literature	PROSECUTION	4
01-06-2011	WFEE	Fee Worksheet (SB06)	PROSECUTION	2
01-06-2011	N417	EFS Acknowledgment Receipt	PROSECUTION	6
01-06-2011	SPEC	Specification	PROSECUTION	26
01-06-2011	CLM	Claims	PROSECUTION	5
01-06-2011	ABST	Abstract	PROSECUTION	1
01-06-2011	EARLYPUB	Request for Early Publication	PROSECUTION	1

Close Window

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.
12/985,351	01/06/2011	William Grecia		4165

70984 7590 08/08/2012

The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
08/08/2012	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

cs2cd@yahoo.com
sa.cs2cd@gmail.com
bally5@aol.com

Notice of Abandonment	Application No.	Applicant(s)
	12/985,351	GRECIA, WILLIAM
	Examiner	Art Unit
	JAMES TURCHEN	2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☐ Applicant's failure to timely file a proper reply to the Office letter mailed on _____.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 (a) to the final rejection.
   (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114).
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
   (d) ☐ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____. The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record, the assignee of the entire interest, or all of the applicants.

5. ☒ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34(a)) upon the filing of a continuing application.

6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☐ The reason(s) below:

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439

Petitions to revive under 37 CFR 1.137(a) or (b), or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

Doc Code: EABN

Document Description: Letter Express Abandonment of the application

PTO/SB/24 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

EXPRESS ABANDONMENT UNDER 37 CFR 1.138

File the petition electronically using EFS-Web
Or **Mail** the petition to:
Mail Stop Express Abandonment
Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Application Number	12985351
Filing Date	01-06-2011
First Named Inventor	William Grecia
Art Unit	2432
Examiner Name	Barron Jr, Gilberto
Attorney Docket Number	

Please **check only one** of boxes 1 or 2 below:
(If no box is checked, this paper will be treated as a request for express abandonment as if box 1 is checked.)

1. ☐ **Express Abandonment**
I request that the above-identified application be expressly abandoned as of the filing date of this paper.

2. ☒ **Express Abandonment in Favor of a Continuing Application**
I request that the above-identified application be expressly abandoned as of the filing date accorded the continuing application filed previously or herewith.

NOTE: A paper requesting express abandonment of an application is not effective unless and until an appropriate USPTO official recognizes and acts on the paper. See the Manual of Patent Examining Procedure (MPEP), section 711.01.

TO AVOID PUBLICATION, USE FORM PTO/SB/24A INSTEAD OF THIS FORM.

TO REQUEST A REFUND OF SEARCH FEE AND EXCESS CLAIMS FEE (IF ELIGIBLE), USE FORM PTO/SB/24B INSTEAD OF THIS FORM.

I am the:

☒ applicant.

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☐ attorney or agent of record. Attorney or agent registration number is _____

☐ attorney or agent acting under 37 CFR 1.34, who is authorized under 37 CFR 1.138(b) because the application is expressly abandoned in favor of a continuing application (box 2 above must be checked). Attorney or agent registration number is _____.

/william grecia/ — Signature

04-19-2012 — Date

William Grecia — Typed or printed name

(212) 372-0293 — Telephone Number

Note: Signature of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.138. 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: Mail Stop Express Abandonment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	12576562
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-APR-2012
Filing Date:	06-JAN-2011
Time Stamp:	07:09:46
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	Letter Express Abandonment of the application	sb0024_ea.pdf	216836 912df02fef681027cd92e2d38d594771f34cd141	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	216836

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	William Grecia
Art Unit	2432
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7266839	82	2007-09-04	Bowers et al.	
	2	7567987	82	2009-07-28	Shappell et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070266095	A1	2007-11-15	Billsus et al.	
	2	20090100060	A1	2009-04-16	Livnat et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

If you wish to add additional Foreign Patent Document citation information please click the Add button			Add
NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Simon L. Garfinkel, "Email-Based Identification and Authentication: An Alternative to PKI?", IEEE Security & Privacy, http://computer.org/security/, published November 2003, pages 20-26.	☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2012-03-12
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	12286424
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	12-MAR-2012
Filing Date:	06-JAN-2011
Time Stamp:	21:29:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	appleicloud_IDS2.pdf	612641 1d89ed2089ad2a19f67294b66518e7152bc e69a0	no	4

Warnings:	
Information:	

2	Non Patent Literature	IEEE.pdf	266225 3ac62be599b7f355e7e6912b8a7ca492cf105a23	no	7

Warnings:	
Information:	
Total Files Size (in bytes):	878866

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	William Grecia
Art Unit	2432
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070010334		2007-01-11	Multerer; Boyd C	
	2	20060036554		2006-02-16	Schrock; Christian E.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Video Interview - Title: Mitch Singer, Sony Pictures - Publication Source: Youtube.com [URL: http://youtu.be/ nqlSakADFII] - (INTERNET PUBLICATION 6-24-2008) NOTE: ATTACHED URL FOR MEDIA NPL REFERENCE.	☐
	2	Video Interview - Title: Jeff Bewkes and Brian Roberts discuss the TV Everywhere model and upcoming trial on Comcast - Publication Source: Youtube.com [URL: http://youtu.be/q8Rt9idJV9I] - (INTERNET PUBLICATION 6-25-2009) NOTE: ATTACHED URL FOR MEDIA NPL REFERENCE.	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2012-03-09
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	12274165
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	09-MAR-2012
Filing Date:	06-JAN-2011
Time Stamp:	22:15:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	updated_IDS3.pdf	612636 d6f937931e5cf581167a89e7a937688e69e1c815	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	612636

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13397517
Filing Date	2012-02-15
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	1	AUTHOR: William Grecia (patent applicant) - Publication Source: AMAZON WEB SERVICES Products and Solutions Catalog - TITLE: STR3EM Digital Distribution System (Ultraviolet - Keychest) - INTERNET PUBLICATION: http://aws.amazon.com/customerapps/2621 [Publication date: June 22, 2009]	☐
	2	AUTHOR: NICHOLAS DELEON - Publication Source: TechCrunch - TITLE: Movie studios launch Epix: 720p streaming video for free - INTERNET PUBLICATION: http://techcrunch.com/2009/06/08/movie-studios-launch-epix-720p-streaming-video-for-free/ [Publication date: June 8, 2009]	☐
	3	AUTHOR: MATT BURNS - Publication Source: TechCrunch - TITLE: TV Everywhere is Comcast and Time Warner's answer to free Internet video - INTERNET PUBLICATION: http://techcrunch.com/2009/06/24/tv-everywhere-is-comcast-and-time-warners-answer-to-free-internet-video/ [Publication date: June 24, 2009]	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2012-03-06
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	12230953
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-MAR-2012
Filing Date:	06-JAN-2011
Time Stamp:	10:47:20
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	Information Disclosure Statement (IDS) Form (SB08)	TVeverywhere_IDS.pdf	612713 2913b3a492929c17501b1c201c38c3113ce78ec2	no	4

Warnings:	
Information:	

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

2	Non Patent Literature	aws1p.pdf	440023 2e8b1eb2fdef1791c2c6775379f0d9e05435b734	no	3
Warnings:					
Information:					
3	Non Patent Literature	techcrunch1p.pdf	411943 f660b5f7eb54054ebf874f55538c4602a9763bd3	no	4
Warnings:					
Information:					
4	Non Patent Literature	epixp5.pdf	482688 66296782e4f6806d1418adbb9c5974efe9befdb1	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	1947367		

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13397517
Filing Date	2012-02-15
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7634734	B2	2009-12-15	Fuller et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2008/111052	WO	A2	2008-09-18	GHOST, Inc.		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2012-03-05
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	12219162
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	05-MAR-2012
Filing Date:	06-JAN-2011
Time Stamp:	02:35:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	March_5_IDS.pdf	612357 69159d32b1cc8b310ed1f78d83d57dd72944c7a0	no	4

Warnings:	
Information:	

2	Non Patent Literature	IDS_ghost.pdf	1624600 540e579808421e604dee5dc5aa2f8082a3c12697	no	40

Warnings:	
Information:	
Total Files Size (in bytes):	2236957

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13397517
Filing Date	2012-02-15
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030018491	A1	2003-01-23	Nakahara	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2007-183935	JP	A	2007-07-19	SAMSUNG ELECTRONICS CO LTD		☐
	2	10-2005-0028244	KR	A	2005-03-22	SAMSUNG ELECTRONICS CO LTD		☐
	3	10-2004-0107602	KR	A	2004-12-23	SAMSUNG ELECTRONICS CO LTD		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	4	10-0708203	KR	B1	2007-04-16	SAMSUNG ELECTRONICS CO LTD		☐
	5	1 0-2005-0060685	KR	A	2005-06-22	SK TELECOM CO., LTD		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13397517
	Filing Date	2012-02-15
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2012-03-05
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2007-183935**
(43)Date of publication of application : **19.07.2007**

(51)Int.Cl. *G06F 21/20 (2006.01)*
G06F 21/24 (2006.01)
G06Q 10/00 (2006.01)
G06F 13/00 (2006.01)

(21)Application number : **2006-332274**
(22)Date of filing : **08.12.2006**

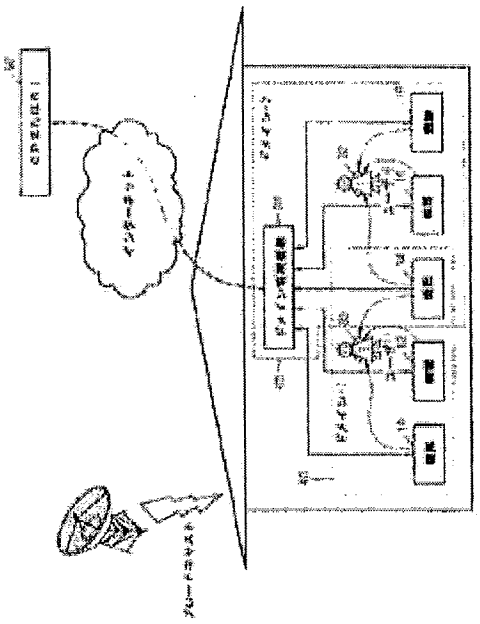
(71)Applicant : **SAMSUNG ELECTRONICS CO LTD**
(72)Inventor : **KIM BONG-SEON**
YOON YOUNG-SUN
NAM SU-HYUN

(30)Priority

Priority number	Priority date	Priority country
2006 755098	**03.01.2006**	**US**
2006 200626985	**24.03.2006**	**KR**

(54) DOMAIN MANAGEMENT METHOD AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a management method and a device for a home network domain allowing sharing of a content by connecting apparatuses with a central focus on consumers.
SOLUTION: This domain management method managing at least one domain by a domain manager positioned inside a home includes: a step for determining whether to register a first apparatus positioned inside the home into the domain or not; and a step for providing data for sharing the content to between an already registered second apparatus and the first apparatus on the basis of a determination result. Thereby, the apparatuses are connected with the central focus on consumers, and the content can be shared to reduce a management burden on a content provider.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-183935
(P2007-183935A)
(43)公開日　平成19年7月19日(2007.7.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B017
G06F 21/24	(2006.01)	G06F	12/14	530E	5B089
G06Q 10/00	(2006.01)	G06F	17/60	176A	5B285
G06F 13/00	(2006.01)	G06F	12/14	560B	
		G06F	13/00	357A	

審査請求 未請求　請求項の数 42　OL　（全 15 頁）

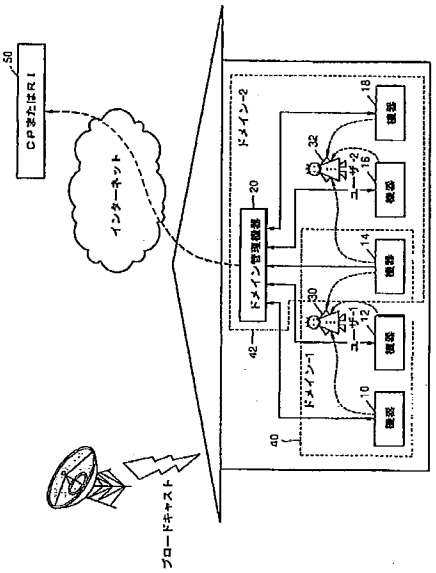
(21)出願番号　特願2006-332274 (P2006-332274)
(22)出願日　平成18年12月8日 (2006.12.8)
(31)優先権主張番号　60/755,098
(32)優先日　平成18年1月3日 (2006.1.3)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10-2006-0026985
(32)優先日　平成18年3月24日 (2006.3.24)
(33)優先権主張国　韓国 (KR)

(71)出願人　390019839
三星電子株式会社
Samsung Electronics Co., Ltd.
大韓民国京畿道水原市霊通区梅灘洞４１６
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　金　奉　禪
大韓民国京畿道城南市盆唐区金谷洞　青率マウル住公９團地アパート９０３棟４１１号（番地なし）

最終頁に続く

(54)【発明の名称】ドメイン管理方法及びその装置

(57)【要約】
【課題】　ドメイン管理方法及びその装置を提供する。
【解決手段】　ホーム内に位置したドメインマネージャが少なくても一つのドメインを管理する方法において、ホーム内に位置した第１機器をドメインに登録するか否かを決定するステップと、決定結果に基づいて第１機器とドメインに既登録された第２機器との間にコンテンツを共有するためのデータを提供するステップと、を含むドメイン管理方法である。これにより、消費者中心に機器を連結してコンテンツを共有でき、コンテンツ提供者の管理負担を減らしうる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
ホーム内に位置したドメインマネージャが少なくとも一つのドメインを管理する方法において、
前記ホーム内に位置した第１機器をドメインに登録するか否かを決定するステップと、
前記決定結果に基づいて、前記第１機器と前記ドメインに既登録された第２機器との間にコンテンツを共有するためのデータを提供するステップとを含むことを特徴とするドメイン管理方法。
【請求項２】
前記ドメインマネージャを前記ドメインに登録するステップをさらに含むことを特徴とする請求項１に記載のドメイン管理方法。
【請求項３】
前記第１機器との隣接性検査を行うステップをさらに含み、
前記決定するステップは、前記隣接性検査結果に基づいて登録するか否かを決定することを特徴とする請求項１に記載のドメイン管理方法。
【請求項４】
前記データは、
前記ドメインに登録された機器として有効な資格を表すドメインメンバーシップの有効性情報を含むことを特徴とする請求項１に記載のドメイン管理方法。
【請求項５】
前記データは、
前記コンテンツの復号化に使われるドメインキーを含むことを特徴とする請求項１に記載のドメイン管理方法。
【請求項６】
前記管理されるドメインについての情報を、前記ホーム内に位置した機器に提供するステップをさらに含むことを特徴とする請求項１に記載のドメイン管理方法。
【請求項７】
前記データを更新し、前記更新された結果を前記登録された機器に通知するステップをさらに含むことを特徴とする請求項１に記載のドメイン管理方法。
【請求項８】
ドメイン内の登録された機器の変動または保安上の危険を感知して、前記データを更新するか否かを決定するステップをさらに含むことを特徴とする請求項７に記載のドメイン管理方法。
【請求項９】
前記更新結果を通知された機器の要請に応答して、前記更新されたデータを提供するステップをさらに含むことを特徴とする請求項７に記載のドメイン管理方法。
【請求項１０】
セキュアタイム及び機器撤回情報のうち少なくとも一つを含むセキュリティデータを前記登録された機器に提供するステップをさらに含み、
前記セキュアタイムは、ドメイン内のコンテンツの有効時間を算定する基準となる時間情報であり、
前記機器撤回情報は、撤回された機器についての情報であることを特徴とする請求項１に記載のドメイン管理方法。
【請求項１１】
前記セキュリティデータを提供するステップは、
登録された機器から前記セキュリティデータを要請されるステップと、
前記要請した機器に前記セキュリティデータを提供するステップとを含むことを特徴とする請求項１０に記載のドメイン管理方法。
【請求項１２】
前記提供するステップは、

各ドメインに登録された機器のセキュリティデータが最新であるか否かを判断するステップと、

最新でないセキュリティデータを有する登録された機器があると判断されれば、最新のセキュリティデータを前記機器に提供するステップとを含むことを特徴とする請求項１０に記載のドメイン管理方法。

【請求項１３】

機器のドメイン脱退要請によって前記機器に対して保存された機器情報を削除し、前記ドメイン内のコンテンツの共有に必要なデータを更新するステップをさらに含むことを特徴とする請求項１に記載のドメイン管理方法。

【請求項１４】

各ドメインに登録される機器の数または各機器が登録するドメインの数を所定数に制限するステップを含むことを特徴とする請求項１に記載のドメイン管理方法。

【請求項１５】

ホーム内に位置して少なくとも一つのドメインを管理する装置において、

前記ホーム内に位置した第１機器をドメインに登録するか否かを決定し、前記決定結果に基づいて前記第１機器と前記ドメインに既登録された第２機器との間にコンテンツを共有するためのデータを提供するドメインデータ提供部を備えることを特徴とするドメイン管理装置。

【請求項１６】

前記第１機器との隣接性検査を行う隣接性検査部をさらに備え、

前記ドメインデータ提供部は、前記隣接性検査結果に基づいて登録するか否かを決定することを特徴とする請求項１５に記載のドメイン管理装置。

【請求項１７】

前記管理されるドメインについての情報を前記ホーム内に位置した機器に提供するドメイン情報提供部をさらに備えることを特徴とする請求項１５に記載のドメイン管理装置。

【請求項１８】

前記ドメインデータ提供部は、

前記データを更新し、前記更新された結果を前記登録された機器に通知することを特徴とする請求項１５に記載のドメイン管理装置。

【請求項１９】

セキュアタイム及び機器撤回情報のうち少なくとも一つを含むセキュリティデータを前記登録された機器に提供するセキュリティデータ提供部をさらに備え、

前記セキュアタイムは、ドメイン内のコンテンツの有効時間を算定する基準となる時間情報であり、

前記機器撤回情報は、撤回された機器についての情報であることを特徴とする請求項１５に記載のドメイン管理装置。

【請求項２０】

前記登録された機器の機器情報を保存する機器情報保存部をさらに備え、

前記ドメインデータ提供部は、脱退要請した機器の機器情報を前記機器情報保存部から削除し、前記脱退要請されたドメインのドメインデータを更新することを特徴とする請求項１５に記載のドメイン管理装置。

【請求項２１】

請求項１に記載の方法を行うプログラムを収録したコンピュータで読み取り可能な記録媒体。

【請求項２２】

ディバイスをドメインに登録する方法において、

前記ドメインのドメイン情報提供部にドメイン情報を要請するステップと、

前記ドメイン情報提供部から前記ドメインについての情報を受信するステップと、

前記ドメイン情報を利用して前記ドメインのドメインデータ提供部にドメイン登録を要請するステップと、

前記ドメイン情報提供部から前記ドメインのドメインキーを受信するステップとを含むことを特徴とするドメイン登録方法。

【請求項２３】

前記ドメインについての情報は、

ドメイン識別子及び前記ドメイン識別子に該当するドメインのドメインデータ提供部の位置についての情報を含むことを特徴とする請求項２２に記載のドメイン登録方法。

【請求項２４】

前記ドメインについての情報は、

前記ドメイン識別子に該当するドメインのドメイン政策識別子及びユーザ情報をさらに含むことを特徴とする請求項２３に記載のドメイン登録方法。

【請求項２５】

前記ディバイスについての情報を保存するステップをさらに含むことを特徴とする請求項２２に記載のドメイン登録方法。

【請求項２６】

前記ディバイスについての情報は、

ディバイスの識別子が前記ディバイスのドメインメンバーシップ有効性情報を含むことを特徴とする請求項２５に記載のドメイン登録方法。

【請求項２７】

前記ドメインメンバーシップの有効性情報は、

前記ディバイスがドメインのメンバーとして有効な期間を表す情報であることを特徴とする請求項２６に記載のドメイン登録方法。

【請求項２８】

前記ディバイスと前記ドメインデータ提供部との隣接性を検査するステップをさらに含むことを特徴とする請求項２２に記載のドメイン登録方法。

【請求項２９】

ディバイスをドメインに登録する方法において、

前記ディバイスから前記ドメインについての情報を要請を受けるステップと、

前記ドメインについての情報を前記ディバイスに伝送するステップと、

前記ディバイスから前記ドメインへの登録を要請されるステップと、

前記ディバイスの物理的な距離を測定するステップと、

前記ドメインのドメインキーを前記ディバイスに伝送するステップとを含むことを特徴とするディバイス登録方法。

【請求項３０】

前記ドメインについての情報は、ドメイン情報提供部が伝送し、前記ドメインキーはドメインデータ提供部が提供することを特徴とする請求項２９に記載のデバイス登録方法。

【請求項３１】

前記ドメインについての情報は、

ドメイン識別子及び前記ドメイン識別子に該当するドメインのドメインデータ提供部の位置についての情報を含むことを特徴とする請求項３０に記載のデバイス登録方法。

【請求項３２】

前記ドメインについての情報は、

前記ドメイン識別子に該当するドメインのドメイン政策識別子及びユーザ情報をさらに含むことを特徴とする請求項３１に記載のドメイン登録方法。

【請求項３３】

前記ディバイスについての情報を保存するステップをさらに含むことを特徴とする請求項２９に記載のデバイス登録方法。

【請求項３４】

前記ディバイスに対する情報は、

ディバイスの識別子と前記ディバイスのドメインメンバーシップ有効性情報とを含むことを特徴とする請求項３３に記載のデバイス登録方法。

【請求項３５】
前記ドメインメンバーシップ有効性情報は、
前記ディバイスがドメインのメンバーとして有効な期間を表す情報であることを特徴とする請求項３４に記載のデバイス登録方法。
【請求項３６】
一つのドメインで使用可能なコンテンツを生成する方法において、
前記ドメインのセキュリティデータ提供部にセキュアタイムを要請するステップと、
前記セキュアタイムを受信するステップと、
前記セキュアタイムを前記コンテンツが前記ドメインで使用可能なコンテンツとして生成された時間に設定するステップと、を含むことを特徴とするコンテンツ生成方法。
【請求項３７】
前記ドメインの機器撤回情報を要請するステップと、
前記ドメインの機器撤回情報によって前記コンテンツの生成を制御するステップとをさらに含むことを特徴とする請求項３６に記載のコンテンツ生成方法。
【請求項３８】
前記機器撤回情報に前記コンテンツを生成するディバイスの情報が含まれた場合、前記コンテンツの生成を中止するステップを含むことを特徴とする請求項３７に記載のコンテンツ生成方法。
【請求項３９】
前記コンテンツを暗号化するためのドメインキーを要請するステップをさらに含むことを特徴とする請求項３６に記載のコンテンツ生成方法。
【請求項４０】
前記ドメインキーを利用して前記コンテンツの暗号化キーを暗号化するステップをさらに含むことを特徴とする請求項３９に記載のコンテンツ生成方法。
【請求項４１】
ドメインに属する機器から前記ドメインで使用可能なコンテンツの生成時間であるセキュアタイムを要請されるステップと、
前記セキュアタイムを提供するステップと、
前記ドメインに属する機器から前記ドメインに登録されていない機器についての情報であるドメイン機器撤回情報を要請されるステップと、
前記ドメイン機器撤回情報を提供するステップとを含むことを特徴とするコンテンツ生成方法。
【請求項４２】
前記ドメインのドメインキーについての要請を受けるステップと、
前記ドメインキーを伝送するステップとをさらに含むことを特徴とする請求項４１に記載のコンテンツ生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ドメイン管理方法及び装置に係り、さらに詳細には、ホーム内のコンテンツを再生／共有できるホーム内機器の集合であるドメインを消費者中心に管理する装置及び方法に関する。
【背景技術】
【０００２】
最近、ホーム内で放送、音楽、ゲームなどを楽しめる機器が多様になり、機器で使用できるコンテンツも豊富になる趨勢で、消費者は、それらの有する多様な機器でコンテンツを便利に共有しようとする要求をしている。このような要求事項に相応して、消費者中心に機器を連結してコンテンツを共有可能にするホームネットワークドメインについての研究が活発に進められている。
【０００３】

図１は、ホーム内でコンテンツを共有する一般的な方法を示す図である。図１を参照して説明すれば、コンテンツを提供するコンテンツ提供者（コンテンツ　プロバイダ：ＣＰ）６、コンテンツに対するライセンスを提供する権限発行者（ライト　イシュアー：ＲＩ）６が存在し、これらが提供するコンテンツを使用するユーザ５は、これらＣＰまたはＲＩにユーザ情報を通じて登録した後にコンテンツを獲得しうる。ドメイン構成のためにユーザだけでなく、ユーザが使用する機器１，２，３，４もインターネットまたは通信線を通じてドメイン管理機能を有するＣＰ　６またはＲＩ　６に連結して登録し、ドメインについての情報及びドメイン内のコンテンツ共有のために必要な情報を提供される。ここで、ドメインとは、コンテンツが共有される機器の集合を意味し、このようなドメインは、インターネットを通じて接続されるＣＰまたはＲＩによって構成されかつ管理される。

【０００４】

すなわち、ユーザはもとより、ユーザが使用する機器を、インターネットを通じてＣＰまたはＲＩに登録し、ＣＰからコンテンツ共有のために必要な情報を受ける。このような登録過程以後に登録された機器の間でコンテンツ共有が起きる。

【０００５】

しかし、このような方法は、ドメインを管理する機能を有する主体、例えば、ＣＰまたはＲＩとホーム外部のインターネットを通じて連結せねばならない。すなわち、コンテンツ共有、保安及び各種の管理のために、ドメイン関連データ及びセキュリティデータの更新が何れもインターネット連結を要する。

【０００６】

したがって、コンテンツの活用のために全ての機器がインターネットでホーム外部と連結されて初めて、正常的にコンテンツを活用できる前述した一般的な方法は、ユーザの便宜上、非効率的であり、かつ不便なシステムである。また、インターネット上のＣＰまたはＲＩは、やはり各ユーザの情報を管理し、個々のユーザごとに有するドメインを管理することが相当な負担となる。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

本発明が解決しようとする技術的課題は、消費者中心に機器を連結してコンテンツを共有可能にするホームネットワークドメインの管理方法及び装置を提供することである。

【課題を解決するための手段】

【０００８】

前記課題を達成するための本発明によるドメイン管理方法は、ホーム内に位置したドメインマネージャが少なくても一つのドメインを管理する方法において、前記ホーム内に位置した第１機器をドメインに登録するか否かを決定するステップと、前記決定結果に基づいて前記第１機器と前記ドメインに既登録された第２機器との間にコンテンツを共有するためのデータを提供するステップとを含む。

【０００９】

前記課題を達成するための本発明によるドメイン管理装置は、ホーム内に位置して少なくとも一つのドメインを管理する装置において、前記ホーム内に位置した第１機器をドメインに登録するか否かを決定し、前記決定結果に基づいて前記第１機器と前記ドメインに既登録の第２機器との間にコンテンツを共有するためのデータを提供するドメインデータ提供部を備える。

【発明の効果】

【００１０】

本発明によれば、ホーム内に位置した管理機器が、他の機器にホーム内に設定されたドメインについての情報、ドメイン内のコンテンツ活用に必要な情報、ドメインの保安と関連したセキュリティ情報を提供する機能を有することによって、管理機器は、ユーザ中心に効率的かつ安全にドメインを管理及び維持でき、ドメインに含まれる機器が何れも外部ネットワークに接続する機能を有さずとも、ドメイン加入及び活動が可能である。また、

ユーザは、多様なコンテンツソースからコンテンツを受けて使用しても同じドメインを維持し、ドメイン内の機器が多様なコンテンツソースから受けたコンテンツを同一に共有可能であり、各コンテンツソース別にドメインを構成する場合に、それぞれのコンテンツ提供者への登録の面倒さを避けうる。

【発明を実施するための最良の形態】

【００１１】

以下、添付された図面を参照して本発明による方法及び装置について詳細に説明する。

【００１２】

本発明は、消費者中心に機器を連結してコンテンツを共有可能にするホームネットワークドメインの管理方法及び装置である。すなわち、ユーザ機器からなるドメインを管理する機能を有する機器をホーム内に置くことによって、ユーザの便宜性を向上させ、コンテンツ提供者の負担を減らしうる。

【００１３】

図２は、本発明の一実施形態によるドメイン管理装置を備えるシステムを表す。図２を参照するに、そのシステムは、５個のユーザの機器１０，１２，１４，１６，１８を備え、ドメイン管理機器２０及びＣＰまたはＲＩ　５０を備える。

【００１４】

本発明によるドメイン管理機器２０は、ホーム内に位置してドメイン４０，４２を管理する役割を行う。ここで、ドメインを管理する作業の例としては、ドメインを初期生成し、ホーム内の機器を前記生成されたドメインに前記ドメインのドメイン政策によって登録した後、管理し、前記登録された機器がドメインを脱退することを管理することが挙げられる。ここで、ドメインの初期生成作業の例としては、ドメイン識別子、ドメインキーの生成が挙げられる。また、登録された機器を管理するという意味は、登録された機器がドメインに該当するコンテンツを安全に共有または再生しうるように管理することを意味し、具体的な例としては、機器のドメイン登録／脱退、リンク生成、ドメインメンバーシップ管理、ドメインキーの生成／更新が挙げられる。本発明によるドメイン管理機器２０は、他の機器１０，１２，１４，１６，１８を代表してインターネットでＣＰまたはＲＩ　５０に接続してコンテンツ活用権限に対する認証を受け、従来の方法とは異なり、他の機器１０，１２，１４，１６，１８についての機器情報をＣＰまたはＲＩ　５０に提供せずとも前記認証を受けうる。

【００１５】

また、本発明によるドメイン管理機器２０は、自身がドメイン２Ｆ４２に登録して、ドメイン内のコンテンツを活用する機能を有しうる。これは、ドメイン管理機器２０は、前述した従来のドメイン管理機能を有するＣＰまたはＲＩとは異なり、ユーザに属する機器であるために可能である。

【００１６】

一方、図２を参照するに、ユーザ１　３０、ユーザ２　３２別にそれぞれのドメイン１　４０、ドメイン２　４２を形成し、ドメイン１　４０には、そのドメインメンバーとして機器１０，１２，１４があり、ドメイン２　４２には、機器１６，１８があるということが分かる。しかし、本発明は、図２とは異なり、ユーザ基盤のドメインではない、単純に機器のみの集合で構成されたドメインを管理するＤＲＭ政策にも適用されうるということは、当業者には自明な事実である。

【００１７】

図３は、図２のドメイン管理機器２０の具体的な構成を例示するブロック図であって、インターフェース３００、ドメイン情報管理部３１０、ドメイン情報提供部３２０、ドメインデータ管理部３３０、ドメインデータ提供部３４０、隣接性検査部３５０、機器情報管理部３６０及びセキュリティデータ提供部３７０を備えて形成される。

【００１８】

インターフェース３００は、他の機器１０，１２，１４，１６，１８と通信を行う。

【００１９】

ドメイン情報管理部３１０は、ユーザの入力を受け、少なくとも一つのドメインを生成し、前記生成されたドメインについての情報を設定及び管理する。ここで、ユーザの入力によって初期化されて設定される情報の例としては、各ドメインに対するドメイン識別子、ドメイン政策識別子、ユーザ情報、ドメイン内のコンテンツの活用に必要なデータを提供する機器の位置情報が挙げられる。一方、後述するが、ドメインデータ管理部３３０に保存されるドメインキーもユーザの入力によって設定されうる。ここで、ユーザ情報の例としては、ユーザ識別子、パスワードが挙げられ、このようなユーザ情報は、前述したドメイン識別子またはドメインキーと関連させうるが、その例としては、後述するドメイン情報の提供時にユーザ識別子を提供して、前記ドメインが前記ユーザ識別子によって特定されるユーザに属するということを知らせること、パスワードまたはユーザ情報を利用したドメインキーの生成または暗号化などが挙げられる。また、ドメインと関連したユーザ情報は、ドメインに機器を登録または脱退する時に行われるユーザ確認過程にも使われうる。

【００２０】

ドメイン情報提供部３２０は、前記生成されたドメインについての情報をドメイン情報管理部３１０から読み取って前記ホーム内に位置した機器１０，１２，１４，１６，１８に提供する。提供する方法の例としては、機器１０，１２，１４，１６，１８の要請によって提供するか、または要請と関係なく、一定周期ごとに前記情報を提供する方法が挙げられるが、必ずしもこれに限定されるものではない。ここで、提供される情報は、前述したように、ドメイン情報管理部３１０に保存された情報が挙げられる。

【００２１】

ドメインデータ管理部３３０は、ドメイン内コンテンツを共有するためのデータを保存する。ここで、保存されるデータの例としては、ドメイン内コンテンツの復号化に使われるドメインキーが挙げられる。

【００２２】

ドメインデータ提供部３４０は、ホーム内に位置した機器をドメインに登録するか否かを決定し、前記登録決定された機器にドメイン内コンテンツを共有するためのデータを提供する。ここで、提供されるデータの例としては、ドメインキー、ドメインメンバーシップ有効性情報が挙げられる。ドメインメンバーシップ有効性情報については後述する。

【００２３】

一方、ドメイン政策が隣接性要件、機器情報の有効性要件を充足する機器に対してのみ登録すると決まったならば、ドメインデータ提供部３４０は、隣接性検査の結果及び機器の有効性要件を充足するか否かを基礎として登録如何を決定する。ここで、機器の有効性検査とは、ドメイン管理機器２０が管理する対象となる機器であるか否かを検査することであり、隣接性検査の例としては、ドメイン管理機器２０と機器との物理的距離が物理的距離の制限条件を満足させるか否かの検査が挙げられるが、必ずしもこれに限定されるものではない。

【００２４】

隣接性検査部３５０は、ドメインデータ提供部３４０の制御によってドメイン管理機器２０自体と機器との隣接性を検査し、隣接性検査の結果をドメインデータ提供部３４０に提供する。

【００２５】

機器情報保存部３６０は、登録決定された機器についての機器情報を保存する。ここで、保存される機器情報の例としては、登録要請した機器から受信された機器識別子、機器キー及び登録決定時にドメインデータ提供部３４０によって生成されるドメインメンバーシップ有効性情報が挙げられる。機器キーは、ドメイン管理機器２０から機器に伝送する経路上のデータの暗号化に使われ、そのデータの例としては、ドメインキーが挙げられる。また、ドメインメンバーシップ有効性情報は、ドメインに登録された機器として有効な資格を表す情報を表し、その例としては、登録された機器がドメインメンバーとして有効な期間がいつまでであるかを表す時間情報が挙げられる。

【００２６】
以上の内容は、ドメイン生成、ドメインメンバー登録及びコンテンツの共有のためのデータの提供を中心に説明し、その次にコンテンツの共有のためのデータの更新過程を図３を参照して説明する。
【００２７】
ドメインデータ提供部３４０は、前述した機能以外にコンテンツの共有のためのデータを更新し、その更新されたデータをドメインデータ管理部３３０に保存した後、その更新された結果を登録された機器に通知する機能を行う。ここで、更新するか否かを決定する方法の例としては、ドメイン内の登録された機器の変動または保安上の危険を感知して決定することが挙げられる。また、ドメインデータ提供部３４０は、前記更新結果を通知された機器の要請に応答して、前記更新されたデータをドメインデータ管理部３３０から読み取って前記要請した機器に提供する。
【００２８】
セキュリティデータ提供部３７０は、セキュアタイム、機器撤回情報のように、保安と関連したセキュリティデータを登録された機器に提供する。ここで、セキュアタイムは、ドメイン内のコンテンツの有効時間を算定する基準となる時間情報であって、コンテンツインポーティング時に使われる。また、機器撤回情報は、所定の理由によって撤回された機器についての情報を意味し、撤回された機器は、他の機器とコンテンツを共有できなくなる。
【００２９】
一方、ドメインデータ提供部３４０は、登録された機器から脱退要請をインターフェース３００を通じて受けた場合、前記脱退要請した機器についての機器情報を前記機器情報保存部３６０から削除し、前記脱退要請されたドメインのコンテンツの共有に必要なデータを更新する。
【００３０】
図４は、本発明の一実施形態によるドメイン管理方法において、ドメイン生成、メンバー登録及びデータ伝達過程を表すフローチャートである。図４を参照するに、ドメイン管理機器２０は、少なくとも一つのドメインを生成し、前記生成されたドメインについての情報がドメイン情報管理部３１０に保存される（Ｓ４００）。すなわち、ドメイン情報管理部３１０は、ドメイン生成のためにユーザが入力した情報によって初期化されて安全に保存される。初期化される情報の例としては、前述したように、各ドメインに対するドメイン識別子、ドメイン政策識別子及びドメインキー、ユーザ情報、ドメイン内のコンテンツ活用のためのデータを提供する機器の位置情報が挙げられる。一方、Ｓ４００またはその以後に、ドメイン管理機器２０は、自身をドメインに登録し、前記ドメイン内のコンテンツの共有に必要なデータを保存しうる。このデータの例としては、ドメインキー、ドメインメンバーシップ有効性情報が挙げられる。
【００３１】
次いで、ドメイン情報保存部３２０は、ホーム内に位置した機器１０，１２，１４，１６，１８から前記生成されたドメインについての情報を要請され、その応答としてドメイン情報管理部３１０から読み取って前記要請した機器１２に提供する（Ｓ４１０）。その後、機器１２は、提供された情報に基づいてドメイン２　４２に加入することを決定し、ドメイン管理機器２０に登録を要請する。ここで、登録要請時、機器１２の機器識別子、機器キーがドメイン管理機器２０に提供され、これは、インターフェース３００を通じてドメインデータ提供部３４０に伝達される。
【００３２】
ドメインデータ提供部３４０は、機器１２をドメイン２　４２に登録するか否かを決定するが、隣接性検査部３５０による隣接性検査の結果、機器の有効性検査に基づいて登録如何を決定する（Ｓ４２０）。このような検査は、ドメイン２　４２のドメイン政策によって行われる。
【００３３】

ドメインデータ提供部３４０は、ドメイン内のコンテンツの共有のためのデータを機器１２に安全に提供する（Ｓ４３０）。このためにドメインデータ提供部３４０が行う過程の例としては、機器１２についてのドメインメンバーシップ有効性情報を生成し、ドメインデータ管理部３３０からドメインキーを読み取ってＳ４１０で提供された機器キーを利用して前記読み取られたドメインキー及び前記生成されたドメインメンバーシップ有効性情報を暗号化する過程が挙げられる。一方、ここで、提供されるデータの例として、ドメインキー、ドメインメンバーシップ有効性情報のみを述べたが、これだけでなく、機器１２がドメイン２　４２に属するというリンク情報も共に提供されうるというのは、当業者には自明な事実である。

【００３４】

この後、ドメインデータ提供部３４０は、Ｓ４３０で生成されたドメインメンバーシップ有効性情報やＳ４１０で提供された機器識別子、機器キーを機器情報管理部３６０に保存する（Ｓ４４０）。

【００３５】

以後、機器１２は、ドメイン２　４２に属するコンテンツをドメインキーを利用した復号化を通じて再生または共有しうる。

【００３６】

図５は、本発明の一実施形態によるドメイン管理方法において、データ更新過程を表すフローチャートである。すなわち、ドメイン内のコンテンツの共有に必要なデータを更新する一実施形態を表し、図２で、ドメイン２　４２のデータ更新状況を前提として図３を参照して説明する。

【００３７】

まず、ドメインデータ提供部３４０は、ドメイン内のコンテンツの共有のためのデータを更新するか否かを決定する（Ｓ５００）。ここで、決定する方法の例としては、ドメインに登録された機器が脱退するなどドメインメンバーの変動が生じるか、またはドメインキーが流出されるなどの保安上の危険を感知して更新如何を決定する方法が挙げられる。

【００３８】

次いで、ドメインデータ提供部３４０は、前記決定によってデータを更新した後、前記更新されたデータをドメインデータ管理部３３０に保存し、前記更新事実を前記ドメインに登録された機器１４，１６，１８に通知する（Ｓ５１０）。更新されるデータの例としては、ドメインキーが挙げられる。

【００３９】

この後、更新事実を通知された機器１４の要請によって、ドメインデータ提供部３４０は、Ｓ５１０で更新されたデータを機器１４に安全に伝達する（Ｓ５２０）。一方、Ｓ５１０で通知される更新事実及びＳ５２０で伝えられるデータは、保存された機器情報を通じた暗号化過程を経うる。このような暗号化方法の例としては、機器１４の機器キーとして暗号化することが挙げられる。

【００４０】

Ｓ５２０を通じて更新されたデータを伝達された機器１４は、更新されたデータを保存する。以後のドメイン内のコンテンツは、更新されたドメインキーを利用して暗号化されかつ共有されて、脱退した機器（機器脱退によってドメインキーが更新された場合）あるいはハッキングのように、保安上危険に処した機器（保安上危険な問題の発生によってドメインキーが更新された場合）は、更新されたドメインキーを受けられなかったため、以後のコンテンツ共有は不可能になる。

【００４１】

図６Ａ及び図６Ｂは、本発明の一実施形態によるドメイン管理方法において、セキュリティデータ提供過程を表すフローチャートである。ここで、セキュリティデータは、前述したように、セキュアタイム、機器撤回情報を含む保安と関連したデータである。

【００４２】

図６Ａは、本発明の一実施形態によるセキュアタイムを提供するドメイン管理方法を表

すフローチャートである。図６Ａには示されていないが、Ｓ６００以前にドメイン生成及び機器登録がなされていることを前提とする。

【００４３】

図６Ａを参照するに、まず、セキュリティデータ提供部３７０は、ドメインに登録された機器からセキュアタイムを要請される（Ｓ６００）。機器がセキュアタイムを要請する場合の例としては、機器がコンテンツをインポーティングする場合が挙げられる。インポーティング時、コンテンツがいつからドメイン用コンテンツとして使われたかを表すためのタイムスタンピングが必要になるが、その基準となる時間がセキュアタイムであるためである。このようなタイムスタンピングは、インポーティング当時のドメインメンバーであった機器が以後に脱退しても、脱退した時間とコンテンツがインポーティングされた時間とを比較して、脱退以前にドメインで共有したコンテンツは、相変わらず使用可能にするための方法として使われる。

【００４４】

その後、セキュリティデータ提供部３７０は、前記要請した機器にセキュアタイムを提供する（Ｓ６１０）。この後、機器は、提供されたセキュアタイムを利用してコンテンツインポーティングを行う。

【００４５】

図６Ｂは、本発明の一実施形態による機器撤回情報を提供するドメイン管理方法を表すフローチャートである。図６Ｂには示されていないが、Ｓ６００以前にドメイン生成及び機器登録がなされていることを前提とする。

【００４６】

図６Ｂを参照するに、まず、セキュリティデータ提供部３７０は、各ドメインに登録された機器に保存されたセキュリティデータが最新であるか否かを判断する（Ｓ６５０）。ここで、ドメインに登録された機器が以前の機器撤回情報であれば、その機器撤回情報が発行された以後に、ドメインを脱退した機器とコンテンツを共有しないようにするために、ドメイン内の登録された機器に保存された機器撤回情報が最新であるか否かを判断し、これにより、登録された機器に保存された機器撤回情報を更新させる。

【００４７】

その後、最新のデータを有していない機器があると判断されれば、セキュリティデータ提供部３７０は、自身が有する最新の機器撤回情報を前記機器に提供する（Ｓ６６０）。

【００４８】

以後、ドメイン内の機器は、ドメイン管理機器２０から提供された機器撤回情報を活用してドメイン内のコンテンツを安全に共有しうる。

【００４９】

図７は、本発明の一実施形態によるドメイン管理方法において、脱退処理過程を表すフローチャートである。図２で、機器１８がドメイン２　４２を脱退する状況を前提として図３を参照して説明する。

【００５０】

図７を参照するに、まず、ドメインデータ提供部３４０は、機器１８から脱退を要請される（Ｓ７００）。すなわち、ドメインに登録されている機器のうち、それ以上ドメイン内のコンテンツ共有を所望しない機器からドメイン脱退を要請される。

【００５１】

その後、ドメインデータ提供部３４０は、前記要請した機器１８の機器情報を機器情報管理部３６０から削除し、前記ドメイン内のコンテンツ共有に必要なデータを前記ドメインのドメイン政策によって更新する（Ｓ７１０）。以後、更新結果及び更新されたデータは、図５で説明したように伝えられる。その結果、ドメインから脱退したユーザ機器は、以前ドメインキーを利用して、脱退以後にドメインに入ったコンテンツをそれ以上共有できなくなる。

【００５２】

一方、ドメイン政策が各ドメインに登録される機器の数または各機器が登録するドメイ

ンの数を所定数に制限するように設定されているならば、これに基づいて、ドメイン管理機器２０は、登録過程を行う。このようなドメイン政策による管理方法によれば、ドメイン管理機器側でもコンテンツ提供者側でも何れも管理負担が減る効果がある。

【００５３】

本発明はまた、コンピュータで読み取り可能な記録媒体にコンピュータで読み取り可能なコードとして具現することが可能である。コンピュータで読み取り可能な記録媒体は、コンピュータシステムによって読み取られるデータが保存される全ての種類の記録装置を含む。コンピュータで読み取り可能な記録媒体の例としては、ＲＯＭ、ＲＡＭ、ＣＤ－ＲＯＭ、磁気テープ、フロッピー（登録商標）ディスク、光データ保存装置があり、またキャリアウェーブ（例えば、インターネットを通じた伝送）形態で具現されるものも含む。また、コンピュータで読み取り可能な記録媒体は、ネットワークに連結されたコンピュータシステムに分散され、分散方式でコンピュータで読み取り可能なコードが保存されかつ実行されうる。そして、本発明を具現するための機能的なプログラム、コード及びコードセグメントは、本発明が属する技術分野のプログラマーによって容易に推論されうる。

【００５４】

本発明は、図面に示した実施形態を参照して説明されたが、それは、例示的なものに過ぎず、当業者ならば、これから多様な変形及び均等な他の実施形態が可能であるということが分かるであろう。したがって、本発明の真の技術的保護範囲は、特許請求の範囲の技術的思想によって決定されねばならない。

【産業上の利用可能性】

【００５５】

本発明は、ホームネットワークドメイン関連の技術分野に好適に適用可能である。

【図面の簡単な説明】

【００５６】

【図１】ホーム内でコンテンツを共有する一般的な方法を示す図である。

【図２】本発明の一実施形態によるドメイン管理装置を備えるシステムを示す図である。

【図３】図２のドメイン管理機器の具体的な構成を例示するブロック図である。

【図４】本発明の一実施形態によるドメイン管理方法において、ドメイン生成、メンバー登録及びデータ伝達過程を示すフローチャートである。

【図５】本発明の一実施形態によるドメイン管理方法において、データ更新過程を示すフローチャートである。

【図６Ａ】本発明の一実施形態によるドメイン管理方法において、セキュリティデータ提供過程を示すフローチャートである。

【図６Ｂ】本発明の一実施形態によるドメイン管理方法において、セキュリティデータ提供過程を示すフローチャートである。

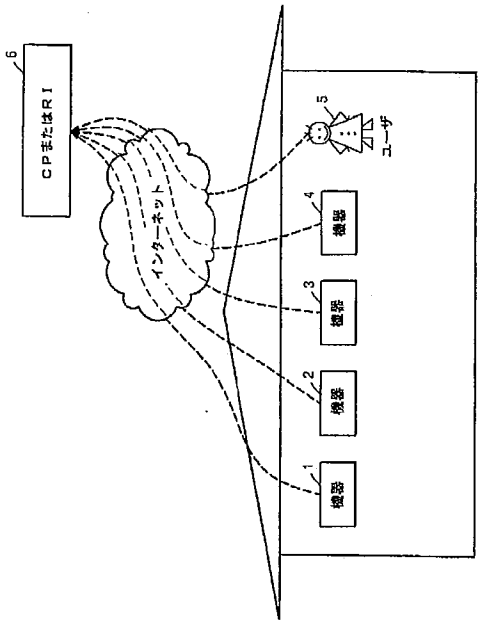
【図７】本発明の一実施形態によるドメイン管理方法において、脱退処理過程を示すフローチャートである。

【符号の説明】

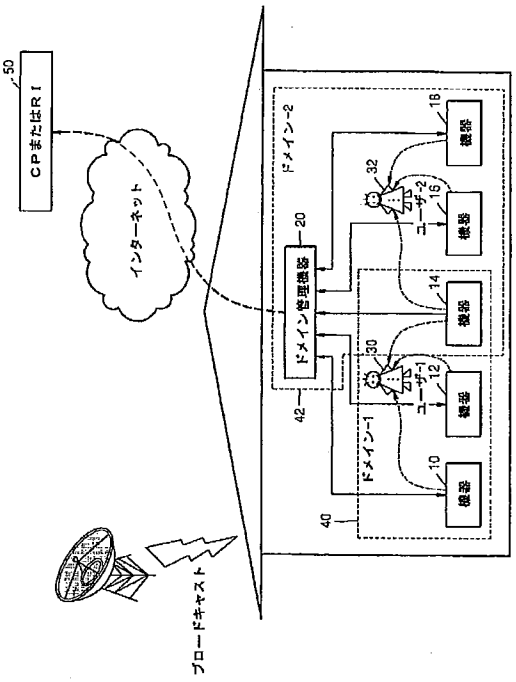
【００５７】

１０，１２，１４，１６，１８　機器
２０　ドメイン関連機器
３０　ユーザ１
３２　ユーザ２
４０　ドメイン１
４２　ドメイン２
５０　ＣＰまたはＲＩ

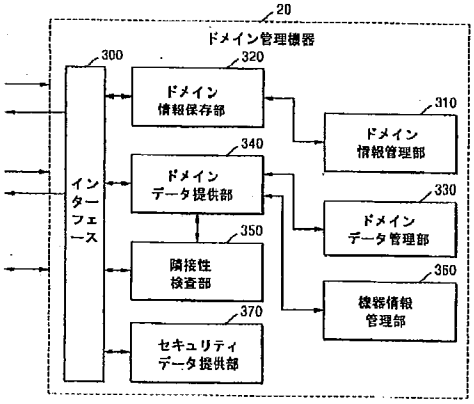
【図１】


CPまたはRI
インターネット
ユーザ
機器
機器
機器
機器

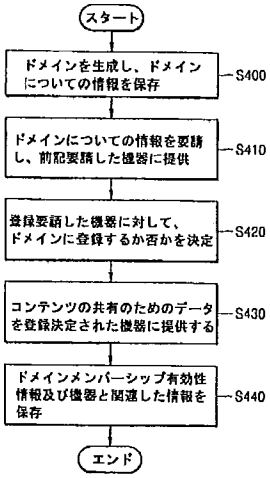
【図２】


CPまたはRI
インターネット
ドメイン-2
ドメイン管理機器
ユーザ-2
ユーザ-1
ドメイン-1
機器
ブロードキャスト

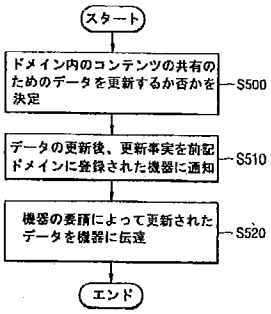
【図３】


ドメイン管理機器
インターフェース
ドメイン情報保存部
ドメイン情報管理部
ドメインデータ提供部
ドメインデータ管理部
隣接性検査部
機器情報管理部
セキュリティデータ提供部

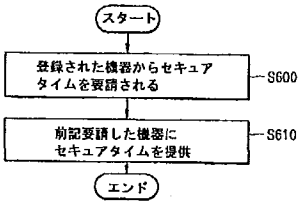
【図４】


スタート
ドメインを生成し、ドメインについての情報を保存
S400
ドメインについての情報を要請し、前記要請した機器に提供
S410
登録要請した機器に対して、ドメインに登録するか否かを決定
S420
コンテンツの共有のためのデータを登録決定された機器に提供する
S430
ドメインメンバーシップ有効性情報及び機器と関連した情報を保存
S440
エンド

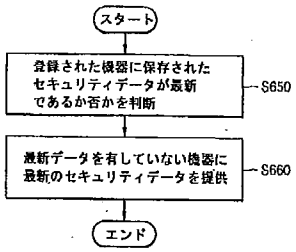
【図５】


スタート
ドメイン内のコンテンツの共有のためのデータを更新するか否かを決定
S500
データの更新後、更新事実を前記ドメインに登録された機器に通知
S510
機器の要請によって更新されたデータを機器に伝達
S520
エンド

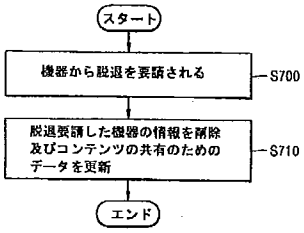
【図６Ａ】


スタート
登録された機器からセキュアタイムを要請される
S600
前記要請した機器にセキュアタイムを提供
S610
エンド

【図６Ｂ】


スタート
登録された機器に保存されたセキュリティデータが最新であるか否かを判断
S650
最新データを有していない機器に最新のセキュリティデータを提供
S660
エンド

【図７】


スタート
機器から脱退を要請される
S700
脱退要請した機器の情報を削除及びコンテンツの共有のためのデータを更新
S710
エンド

フロントページの続き

(72)発明者 尹 映 善
大韓民国京畿道水原市勸善区勸善洞 常緑アパート５１１棟７０４号（番地なし）
(72)発明者 南 秀 鉉
大韓民国ソウル特別市瑞草区方背２洞４３５－２６番地１０２号

Ｆターム(参考) 5B017 AA01 CA16
5B089 GA21 HA06 JA35 KA13
5B285 AA02 BA09 CA04 CA12 CA13 CA17 CA41 DA05

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11) Publication number: 1020050028244 A

(43) Publication date: 22.03.2005

(21) Application number: 1020030064861

(22) Application date: 18.09.2003

(71) Applicant:
- SAMSUNG ELECTRONICS CO., LTD.

(72) Inventor:
- CHANG, KYUNG AH
- LEE, BYUNG RAE

(51) Int. Cl: G06F 17/00

(54) METHOD FOR LICENSING DRM SUPPORTING MULTIPLE DEVICES TO PROCESS DIGITAL INFORMATION

(57) Abstract:

PURPOSE: A method for licensing the DRM(Digital Right Management) supporting multiple devices to process digital information is provided to enable a contents user to conveniently use contents in diverse DRM environments by making the contents executed on multiple devices with use of a license structure for playing DRM contents.

CONSTITUTION: As the contents including license information is transmitted to the devices(530-550), the license information includes unique IDs for more than two devices to play the contents. The contents are received from a DRM server(520) and the IDs are extracted from the license information. In case that the same ID as the ID of device is present among the extracted IDs, the contents are played.

Legal Status

Date of request for an examination (20030918)

Notification date of refusal decision (00000000)

Final disposal of an application (registration)

Date of final disposal of an application (20050504)

Patent registration number (1004939040000)

Date of registration (20050527)

Number of opposition against the grant of a patent ( )

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ( )

Date of requesting trial against decision to refuse ( )

Date of extinction of right ( )

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
G06F 17/00

(45) 공고일자 2005년06월10일
(11) 등록번호 10-0493904
(24) 등록일자 2005년05월27일

(21) 출원번호 10-2003-0064861
(22) 출원일자 2003년09월18일
(65) 공개번호 10-2005-0028244
(43) 공개일자 2005년03월22일

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 이병래
경기도용인시수지읍상현리만현마을성원상떼빌306동104호

장경아
서울특별시성북구삼선동1가188번지9통6반4층

(74) 대리인 김동진

심사관 : 송대종

(54) 다수의 기기를 지원하는 DRM 라이센스 방법

요약

본 발명은 DRM 라이센스에 관한 발명으로서, 본 발명에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생할 수 있는 2이상의 기기들에 대한 각각의 고유한 식별자를 포함하는 제1단계와, 상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 식별자들을 추출하는 제2단계, 및 상기 추출한 식별자들 중 자신의 식별자와 동일한 식별자가 존재하는 경우 상기 컨텐츠를 재생하는 제3단계를 포함하는 것을 특징으로 한다.

대표도

도 5

색인어

DRM 라이센스

명세서

도면의 간단한 설명

도 1은 종래의 일반적인 DRM 라이센스를 구조를 나타내는 예시도이다.

도 2는 종래의 일반적인 DRM 라이센스를 구조를 나타내는 또다른 예시도이다.

도 3은 본 발명의 실시에 따라 DRM 라이센스 구조에 다수의 기기 식별자를 기술하는 것을 나타내는 예시도이다.

도 4는 본 발명의 실시에 따라 DRM 라이센스 구조에 특정한 도메인 식별자를 기술하는 것을 나타내는 예시도이다.

도 5는 본 발명의 실시에 따라 DRM 서버를 중심으로 DRM 라이센스를 관리하는 것을 나타내는 예시도이다.

도 6은 본 발명의 실시에 따라 컨텐츠를 재생하는 기기의 갯수를 제한하기 위한 DRM 라이센스 구조를 나타내는 예시도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 DRM 라이센스에 관한 것으로서, 보다 상세하게는 디지털 정보를 처리할 수 있는 다수의 기기를 지원하는 DRM 라이센스 방법에 관한 것이다.

일반적으로 종래의 DRM 기술은 수요자가 구입한 컨텐츠(content)와 상기 컨텐츠(content)를 위한 라이센스의 내용에 따라 하나의 기기에서만 재생이 가능하였다.

즉, 일반적으로 종래의 DRM 환경에서는 수요자가 컨텐츠(content)를 컨텐츠 공급자(content provider)로부터 공급받고, 상기 컨텐츠(content)에 해당하는 라이센스를 구입하게 된다. 이 때, 라이센스는 하나의 기기에 대해서만 적용이 가능하도록 되어 있는데, 여기에는 기기 바인딩(device binding) 방식과 사용자 바인딩(user binding) 방식이 있다.

기기 바인딩(device binding) 방식은 수요자가 구입한 라이센스가 기기(device)에 종속되어 해당하는 기기(device)에서만 컨텐츠의 재생이 가능하도록 하는 방식이다. 그리고, 사용자 바인딩(user binding) 방식은 구입한 라이센스가 사용자(user)에게 종속되는 경우로서, 예컨대 SIM(Subscriber Identification Module) 카드 또는 스마트 카드 등을 이용하는 방법이 있다.

도 1은 종래의 일반적인 DRM 라이센스를 구조를 나타내는 예시도로서, XML(eXtentsible Markup Language)을 이용하여 표현하고 있다.

1라인 내지 5라인에서는 DRM 라이센스의 시작을 나타내며 XML의 해석을 위한 정보를 나타내는 XML 네임스페이스에 대한 정보를 기술하고 있다.

6라인 내지 8라인에서는 DRM 라이센스가 적용되는 DRM 시스템의 버전 정보를 기술하고 있다.

9라인 내지 21라인은 컨텐츠 정보와 DRM 라이센스의 구체적인 내용을 포함하며, 각각 <asset>엘리먼트와 <permission>엘리먼트로 표현하고 있다.

<asset>엘리먼트는 11라인 내지 13라인에서 DRM 라이센스가 적용되는 컨텐츠의 식별자(identifier)를 기술하고, 14라인 내지 16라인에서는 암호화된 컨텐츠를 복호할 수 있는 컨텐츠 암호 키(Content Encryption Key, CEK) 정보를 기술하고 있다.

<permission> 엘리먼트는 18라인 내지 20라인에서 컨텐츠 재생이 가능함을 기술하고 있다.

도 2는 종래의 일반적인 DRM 라이센스를 구조를 나타내는 또다른 예시도로서, 19라인 내지 23라인에서는 컨텐츠를 디스플레이할 수는 있지만 1회만 허용하고 있음을 기술하고 있다. 20라인의 <constraint>엘리먼트는 <count>엘리먼트 이외에도 <interval>, <accumulated>, <start>, <end>와 같은 엘리먼트들을 포함할 수 있다.

<interval>엘리먼트는 컨텐츠를 사용할 수 있는 기간을 나타내며, 그 시작 시점은 컨텐츠를 최초로 사용한 시점이다. 예를 들어, <interval>엘리먼트의 값이 '10d'로 표현되면, 컨텐츠를 사용한 시점부터 10일 동안 컨텐츠를 자유롭게 사용할 수 있다.

<accumulated>엘리먼트는 컨텐츠의 사용이 최대로 축적될 수 있는 시간을 의미한다. 예를 들어, '10h'라고 하면 전체 컨텐츠의 재생 시간이 10시간 이상이 되어서는 안되는 것을 의미한다.

<start>와 <end>엘리먼트는 함께 기술되는데, <start>엘리먼트에서 지정하는 날짜부터 <end>에서 지정하는 날짜까지 자유롭게 사용할 수 있음을 기술하고 있다.

현재 DRM에 관한 대표적 기술로는 마이크로소프트사의 DRM, OMA DRM 등이 있으며, 일반적으로 라이센스가 바인딩된 단일의 기기에서만 컨텐츠의 재생이 가능하도록 되어 있으므로, 사용자가 여러 기기를 소유하고 있는 경우에는 하나의 컨텐츠와 이에 해당하는 라이센스를 이용하여 다양한 기기에서 컨텐츠를 재생할 수 없는 불편함이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 문제점을 해결하기 위해 안출된 것으로, 다양한 기기에서 디지털 컨텐츠를 재생할 수 있는 라이센스 구조를 제시하고, 상기 구조를 이용하여 디지털 컨텐츠를 여러 기기에서 재생하는 방법을 제안한다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생할 수 있는 2이상의 기기들에 대한 각각의 고유한 식별자를 포함하는 제1단계와, 상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 식별자들을 추출하는 제2단계, 및 상기 추출한 식별자들 중 자신의 식별자와 동일한 식별자가 존재하는 경우 상기 컨텐츠를 재생하는 제3단계를 포함한다.

또한 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 논리적 영역을 구별시키는 고유한 식별자를 포함하는 제1단계와, 상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 식별자를 추출하는 제2단계, 및 상기 추출한 식별자가 기기 자신이 속하는 영역의 식별자와 동일한 경우 상기 컨텐츠를 재생하는 제3단계를 포함한다.

또한 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생하는 횟수를 나타내는 재생 횟수 정보를 포함하는 제1단계와, 상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 재생 횟수 정보를 추출하는 제2단계, 및 상기 추출한 재생 횟수 정보로부터 상기 수신한 컨텐츠를 재생할 수 있음이 확인되면 상기 컨텐츠를 재생하는 제3단계, 사용한 또는 사용할 재생 횟수를 제외하고 남아 있는 재생 횟수 정보와 라이센스를 다른 기기에 전달하고, 상기 다른 기기가 변경된 재생 횟수 정보를 추출하여 사용하는 제4단계를 포함한다.

한편, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생할 수 있는 기기들의 갯수를 나타내는 기기 갯수 정보인 것을 포함하는 제1단계와, 상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 기기 갯수 정보를 추출하는 제2단계, 및 상기 추출한 기기 갯수 정보로부터 상기 수신한 컨텐츠를 재생할 수 있음이 확인되면 상기 컨텐츠를 재생하는 제3단계, 사용한 또는 사용할 기기 갯수를 제외하고 남아 있는 기기 갯수 정보와 라이센스를 다른 기기에 전달하고, 상기 다른 기기가 변경된 기기 갯수 정보를 추출하여 사용하는 제4단계를 포함한다.

또한 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 논리적 영역을 관리하는 서버가 컨텐츠와 상기 컨텐츠에 대한 라이센스 정보를 수신하는 제1단계와, 상기 기기들이 상기 컨텐츠를 요청하면 상기 서버가 상기 제1단계에서 수신한 라이센스 정보를 확인하는 제2단계와, 상기 제2단계로부터 적법한 라이센스로 확인되면, 상기 서버는 상기 기기에게 요청된 컨텐츠를 제공하고, 자신의 라이센스 정보의 상태값을 갱신하는 제3단계를 포함한다. 이 때, 바람직하게는 라이센스 정보는 상기 컨텐츠를 재생하는 횟수를 나타내는 재생 횟수 정보이거나, 컨텐츠를 재생할 수 있는 기기들의 갯수를 나타내는 기기 갯수 정보이거나, 컨텐츠를 재생할 수 있는 총 시간을 나타내는 컨텐츠 재생 시간 정보인 것을 특징으로 한다.

한편, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 다수의 기기를 지원하는 DRM 라이센스 방법은 컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 논리적 영역을 관리하는 서버가 컨텐츠와 상기 컨텐츠에 대한 라이센스 정보를 수신하는 제1단계와, 상기 제1단계에서 수신한 라이센스 정보를 상기 영역에 속하는 기기별로 할당하는 제2단계와, 상기 제2단계에서 할당된 라이센스 정보와 제1단계에서 수신한 컨텐츠를 해당 기기로 전송하는 제3단계, 및 상기 제3단계로부터 수신한 할당된 라이센스 정보에 따라 컨텐츠를 재생하는 제4단계를 포함한다. 이 때, 바람직하게는 상기 라이센스 정보는 상기 컨텐츠를 재생하는 횟수를 나타내는 재생 횟수 정보이거나, 컨텐츠를 재생할 수 있는 기기들의 갯수를 나타내는 기기 갯수 정보이거나, 컨텐츠를 재생할 수 있는 총 시간을 나타내는 컨텐츠 재생 시간 정보인 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 일 실시예에 따른 다수의 기기를 지원하는 DRM 라이센스 방법을 설명하면 다음과 같다.

한편, DRM 라이센스는 그 상태값이 변하는 경우와 변하지 않는 경우로 나누어 생각할 수 있다. 즉, <start>, <end>엘리먼트의 기술하는 경우에는 해당 기간동안에 컨텐츠의 사용이 가능하므로 해당 값이 변하지 않는다. 그러나, 도 2의 21라인과 같이 컨텐츠 사용의 회수를 제한하고 있는 경우에는 상기 컨텐츠를 사용할 때마다 그 값이 변하게 된다. 본 발명에서는 이렇게 DRM 라이센스의 상태값이 변하는 경우와 변하지 않는 경우에 각각 적용될 수 있는 방법에 대해 설명하도록 한다. 또한, 후술할 DRM 라이센스 구조는 DRM 환경에 따라 XML로 표현되거나 별도의 오브젝트로 구현될 수 있다.

도 3은 본 발명의 실시에 따라 DRM 라이센스 구조에 다수의 기기 식별자를 기술하는 것을 나타내는 예시도로서, 컨텐츠를 재생할 수 있는 기기의 고유한 식별자를 기술하는 방법이다. 따라서, DRM 라이센스 구조에 기술된 기기 식별자에 대응하는 기기만이 컨텐츠를 이용할 수 있는 권리가 있다. 즉, DRM 기능이 있는 기기를 소유하고 있는 사용자는 여러 기기에서 재생할 수 있는 사항이 기술된 라이센스 구조를 라이센스 제공자로부터 구입한다. 상기 라이센스 구조에는 컨텐츠를 재생할 수 있는 기기의 고유한 식별자가 기술되어 있으므로, 각각의 기기들은 상기 라이센스 구조에 기술된 기기 식별자가 자신의 것과 일치하면 해당 컨텐츠를 재생할 수 있다. 이러한 방법은 DRM 라이센스의 상태값이 변하지 않는 구조에 적용하는 것이 적합하다.

도 4는 본 발명의 실시에 따라 DRM 라이센스 구조에 특정한 도메인 식별자를 기술하는 것을 나타내는 예시도로서, 컨텐츠를 재생할 수 있는 기기들을 포함하는 특정한 도메인의 고유한 식별자를 기술하는 방법이다. 따라서, DRM 라이센스 구조에 기술된 도메인 식별자에 대응하는 도메인에 포함된 기기들만이 컨텐츠를 이용할 수 있는 권리가 있다. 이러한 방법은 DRM 라이센스의 상태값이 변하지 않는 구조에 적용하는 것이 적합하다.

도 3 또는 도 4에서 제시하는 구조는 컨텐츠 제공자 또는 별도의 라이센스 생성자가 제공할 수 있고, 사용자 측에 별도의 DRM서버를 설치하지 않아도 된다.

도 5는 본 발명의 실시에 따라 DRM 서버를 중심으로 DRM 라이센스를 관리하는 것을 나타내는 예시도이다.

즉, 식별가능한 도메인(500)에는 컨텐츠를 재생할 수 있는 각종 기기들(530,540,550)과 외부로부터 수신하는 컨텐츠의 라이센스를 관리하는 DRM 서버(520)가 포함된다. 한편, 라이센스 생성자(510)는 해당 컨텐츠에 대한 라이센스 구조(560)를 제공하는데, 상기 컨텐츠를 제공하는 컨텐츠 제공자가 해당 컨텐츠와 함께 라이센스 구조를 제공할 수도 있다. 상기 DRM 서버(520)는 라이센스와 이와 관련된 라이센스 상태 정보를 관리한다. 따라서, 도 5에서 도시한 DRM 라이센스 관리 형태는 라이센스 상태값의 변화 여부에 관계없이 적용할 수 있다.

우선, DRM 서버(520)와 기기들(530,540,550)간에 인증 과정을 수행함으로써 상기 도메인(500) 내에 속한 정당한 기기인지 여부를 확인한다. 그리고 나서, DRM 서버(520)와 기기들(530,540,550) 사이에 송수신하는 정보의 보호를 위해 암호키를 생성하는 과정을 거치게 되고, 기기는 DRM 서버(520)에게 컨텐츠 사용을 요청한다. DRM 서버(520)는 상기 요청에 따라, 컨텐츠 사용을 요청한 기기가 DRM 서버(520)의 라이센스 구조에 기술된 기기인지 여부를 확인한다. 그리고 나서, 기기가 컨텐츠를 재생할 수 있도록 하고, 이에 따른 라이센스의 상태값을 수정한다.

한편, 상기 DRM 서버(520)가 라이센스 권한을 자신이 관리하는 기기들 (530,540,550)에게 할당하여 제공하면, 상기 기기들 (530,540,550)은 할당된 권한 내에서 컨텐츠를 이용할 수 있다. 예컨데, 상기 라이센스 권한이 재생 시간에 관한 것일 경우 각각의 기기별(530,540,550)로 재생할 수 있는 시간을 할당하거나, 재생 가능 횟수에 관한 것일 경우 각각의 기기별(530,540,550)로 재생할 수 횟수를 할당할 수 있다.

도 6은 본 발명의 실시에 따라 컨텐츠를 재생하는 기기의 갯수를 제한하기 위한 DRM 라이센스 구조를 나타내는 예시도이다. 즉, DRM 라이센스 구조에 컨텐츠를 재생할 수 있는 기기의 식별자를 기술하지 않고 몇 개의 기기에서 컨텐츠를 재생할 수 있는지에 대한 정보를 기술하고 도 5에서 도시한 DRM 서버(520)가 기기의 개수를 관리하는 방식이다. 도 6에서는 최대 5개의 기기까지 컨텐츠의 재생을 허용하고 있음을 나타내고 있다. 도 6에서 도시한 바와 같이 기기의 개수를 지정하는 방법은 기기의 고유한 식별자를 정확히 모르거나 새로운 기기의 추가 또는 제거시에도 DRM 서버(520)가 효율적으로 라이센스를 관리할 수 있다.

이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정하는 것은 아니다.

발명의 효과

본 발명에 따른 DRM 컨텐츠의 재생을 위한 라이센스 구조를 이용하여 상기 컨텐츠가 다수의 기기에서 실행될 수 있도록 함으로써, 컨텐츠 이용자는 다양한 DRM 환경에서 보다 편리하게 컨텐츠를 이용할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.
삭제

청구항 2.

DRM 환경에 있어서,

라이센스 정보를 포함하는 컨텐츠를 전송하는데, 상기 라이센스 정보는 상기 컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 도메인을 구별시키는 고유한 식별자를 포함하는 제1단계;

상기 컨텐츠를 수신하고, 상기 라이센스 정보로부터 상기 식별자를 추출하는 제2단계; 및

상기 추출한 식별자가 기기 자신이 속하는 도메인의 식별자와 동일한 경우 상기 컨텐츠를 재생하는 제3단계를 포함하는 것을 특징으로 하는 DRM 라이센스 방법.

청구항 3.
삭제

청구항 4.
삭제

청구항 5.

DRM 환경에 있어서,

컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 도메인을 관리하는 서버가 컨텐츠와 상기 컨텐츠에 대한 라이센스 정보를 수신하는 제1단계;

상기 기기들이 상기 컨텐츠를 요청하면 상기 서버가 상기 제1단계에서 수신한 라이센스 정보를 확인하는 제2단계;

상기 제2단계로부터 적법한 라이센스로 확인되면, 상기 서버는 상기 기기에게 요청된 컨텐츠를 제공하고, 자신의 라이센스 정보의 상태값을 갱신하는 제3단계를 포함하는 것을 특징으로 하는 DRM 라이센스 방법.

청구항 6.

제5항에 있어서,

상기 라이센스 정보는 상기 컨텐츠를 재생하는 횟수를 나타내는 재생 횟수 정보인 것을 특징으로 하는 DRM 라이센스 방법.

청구항 7.

제5항에 있어서,

상기 라이센스 정보는 컨텐츠를 재생할 수 있는 기기들의 갯수를 나타내는 기기 갯수 정보인 것을 특징으로 하는 DRM 라이센스 방법.

청구항 8.

제5항에 있어서,

상기 라이센스 정보는 컨텐츠를 재생할 수 있는 총 시간을 나타내는 컨텐츠 재생 시간 정보인 것을 특징으로 하는 DRM 라이센스 방법.

청구항 9.

DRM 환경에 있어서,

컨텐츠를 재생할 수 있는 2이상의 기기들이 속하는 도메인을 관리하는 서버가 컨텐츠와 상기 컨텐츠에 대한 라이센스 정보를 수신하는 제1단계;

상기 제1단계에서 수신한 라이센스 정보를 상기 도메인에 속하는 기기별로 할당하는 제2단계;

상기 제2단계에서 할당된 라이센스 정보와 제1단계에서 수신한 컨텐츠를 해당 기기로 전송하는 제3단계;

상기 제3단계로부터 수신한 할당된 라이센스 정보에 따라 컨텐츠를 재생하는 제4단계를 포함하는 것을 특징으로 하는 DRM 라이센스 방법.

청구항 10.

제9항에 있어서,

상기 라이센스 정보는 상기 컨텐츠를 재생하는 횟수를 나타내는 재생 횟수 정보인 것을 특징으로 하는 DRM 라이센스 방법.

청구항 11.

제9항에 있어서,

상기 라이센스 정보는 컨텐츠를 재생할 수 있는 기기들의 갯수를 나타내는 기기 갯수 정보인 것을 특징으로 하는 DRM 라이센스 방법.

청구항 12.

제9항에 있어서,

상기 라이센스 정보는 컨텐츠를 재생할 수 있는 총 시간을 나타내는 컨텐츠 재생 시간 정보인 것을 특징으로 하는 DRM 라이센스 방법.

도면

도면1

```
1라인: <o-ex:rights
2라인:              xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
3라인:             xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
4라인:              xmlns:ds="http://www.w3.org/2000/09/xmldsig#/"
5라인: >
6라인:  <o-ex:context>
7라인:      <o-dd:version>1.0</o-dd:version>
8라인:  </o-ex:context>
9라인:  <o-ex:agreement>
10라인:     <o-ex:asset>
11라인:        <o-ex:context>
12라인:           <o-dd:uid>cid:4567829547@foo.com</o-dd:uid>
13라인:        </o-ex:context>
14라인:        <ds:KeyInfo>
15라인:           <ds:KeyValue>vUEwR8LzEJociC+dgT1mgg== </ds:KeyValue>
16라인:        </ds:KeyInfo>
17라인:     </o-ex:asset>
18라인:     <o-ex:permission>
19라인:        <o-dd:play/>
20라인:     </o-ex:permission>
21라인:  </o-ex:agreement>
22라인:</o-ex: rights>
```

도면2

```
1라인: <o-ex:rights
2라인:              xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
3라인:              xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
4라인:              xmlns:ds="http://www.w3.org/2000/09/xmldsig#/"
5라인: >
6라인:  <o-ex:context>
7라인:      <o-dd:version>1.0</o-dd:version>
8라인:  </o-ex:context>
9라인:  <o-ex:agreement>
10라인:     <o-ex:asset>
11라인:        <o-ex:context>
12라인:           <o-dd:uid>cid:4567829547@foo.com</o-dd:uid>
13라인:        </o-ex:context>
14라인:        <ds:KeyInfo>
15라인:         <ds:KeyValue>vUEwR8LzEJociC+dgT1mgg== </ds:KeyValue>
16라인:      </ds:KeyInfo>
17라인:    </o-ex:asset>
18라인:    <o-ex:permission>
19라인:      <o-dd:display>
20라인:        <o-ex:constraint>
21라인:           <o-dd:count>1</o-dd:/count>
22라인:        </o-ex:constraint>
23라인:      <o-dd:display>
20라인:    </o-ex:permission>
21라인: </o-ex:agreement>
22라인:</o-ex: rights>
```

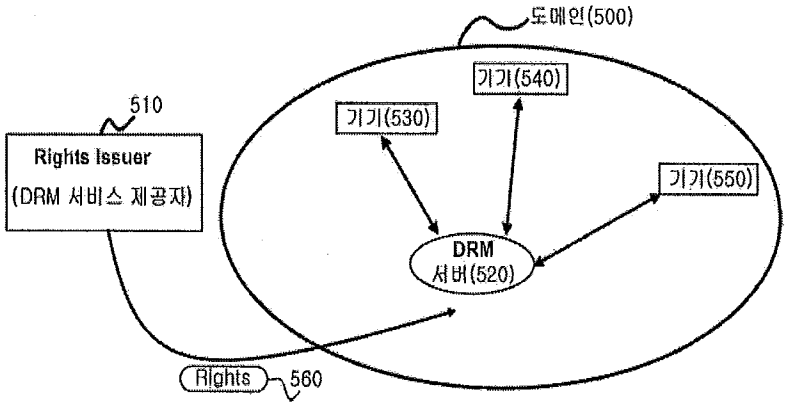
도면3

```
Rights{

Device_ID1; Device_ID2; Device_ID3; ...

}
```

도면4

```
Rights{
Domain-ID;
}
```

도면5



도면6

```
Rights{
Device 5;
}
```

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11) Publication number: 1020040107602 A

(43) Publication date: 23.12.2004

(21) Application number: 1020030036348

(22) Application date: 05.06.2003

(71) Applicant: • SAMSUNG ELECTRONICS CO., LTD.

(72) Inventor: • LEE, SEON NAM

(51) Int. Cl: H04L 9/32

(54) LICENSE MANAGEMENT SYSTEM FOR EXECUTING CONTENTS ON HOME NETWORK TO REMOVE REPACKAGING PROCESS AND REDISTRIBUTION PROCESS

(57) Abstract:

PURPOSE: A license management system for executing contents on a home network system and a method for the same are provided to reproduce easily same media files and same media streams by sharing one license within the home network system.

CONSTITUTION: A license storage module(344) is used for storing a full license received from a license server. A temporary license issue module(345) is used for issuing a temporary license by using the full license of the license storage module. A license search module(343) is used for searching a storing state of the full license and transmitting a searched result to a license request module and the temporary license issue module. The license request module(342) is used for requesting the license to the license server when there is not the full license in the license storage module.

Legal Status

Date of request for an examination (20080526)

Notification date of refusal decision (20100621)

Final disposal of an application (rejection)

Date of final disposal of an application (20100621)

Patent registration number ( )

Date of registration (00000000)

Number of opposition against the grant of a patent ( )

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ( )

Date of requesting trial against decision to refuse ( )

Date of extinction of right ( )

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.[7]
H04L 9/32

(11) 공개번호 10-2004-0107602
(43) 공개일자 2004년12월23일

(21) 출원번호 10-2003-0036348
(22) 출원일자 2003년06월05일

(71) 출원인 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 이선남
강원도춘천시운교동176-24

(74) 대리인 김동진

심사청구 : 없음

(54) 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리시스템 및 방법

요약

본 발명은 홈 네트워크안의 디바이스들마다 별도의 라이센스를 부여받을 필요 없이 하나의 라이센스로 홈 네트워크 내의 각 디바이스들이 컨텐츠를 이용할 수 있도록 하는 시스템 및 방법에 관한 것이다.

본 발명에 따른 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 시스템은 각종 다른 디바이스와 데이터를 송수신하는 송수신 모듈, 송수신 모듈을 통하여 홈디바이스로부터 라이센스 발급 요청을 받아서 해당 정식 라이센스가 라이센스 저장 모듈에 저장되어 있는지를 검색하고 검색결과를 라이센스 요청 모듈과 임시 라이센스 발급 모듈에 전달하는 라이센스검색 모듈, 라이센스가 라이센스 저장 모듈에 존재하지 않는 경우에 라이센스 서버에 해당 라이센스를 발급하여 줄 것을 송수신모듈을 통하여 요청하는 라이센스요청 모듈, 송수신 모듈을 통해 라이센스 서버로부터 다운받은 라이센스를 저장하는 라이센스 저장 모듈; 및 라이센스 저장 모듈에 저장된 정식 라이센스를 이용하여 임시 라이센스를 송수신 모듈을 통하여 해당 홈디바이스에 발급하는 임시 라이센스 발급 모듈로 이루어진다.

본 발명에 따른 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 방법은 홈디바이스가 라이센스 관리 모듈에 해당 라이센스를 요청하는 단계, 라이센스 관리 모듈내에 해당 라이센스가 있는가를 판단하는 단계, 판단 결과에 따라 상기 홈디바이스에 임시 라이센스를 부여하는 단계, 및 홈디바이스에 존재하는 컨텐츠 재생기를 이용하여 미디어를 실행하는 단계로 이루어진다.

대표도

도 5

색인어

홈 디바이스(Home Device), 패키징(Packaging), DRM(Digital Rights Management), 라이센스(Licence), 컨텐츠(Contents)

명세서

도면의 간단한 설명

도 1은 종래 기술에 따른 컨텐츠 실행을 위한 라이센스 발급과정을 간략히 도시한 것이다.

도 2는 본 발명이 제안하는 시스템을 전체적으로 나타낸 블록도이다.

도 3은 다운로드 서비스를 받아 컨텐츠를 실행하고자 하는 경우에 홈 네트워크 상에서 라이센스를 공유하는 구성을 나타낸 블록도이다.

도 4는 스트림 서비스를 받아 컨텐츠를 실행하고자 하는 경우에 홈 네트워크 상에서 라이센스를 공유하는 구성을 나타낸 블록도이다.

도 5는 본 발명이 제안하는 라이센스 관리 모듈의 구성요소의 동작을 나타낸 블록도이다.

도 6은 본 발명이 제안하는 방법에 따른 과정을 전체적으로 나타낸 흐름도이다.

도 7은 본 발명이 제안하는 방법에 따른 과정을 홈 네트워크를 중심으로 상세하게 나타낸 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷 환경에서 컨텐츠 공급자로부터 사용자에게 해당 컨텐츠를 암호화하여 전달하고 불법 복제 방지 기술을 제공하는 시스템 및 방법에 관한 것으로, 보다 상세하게는 홈 네트워크안의 디바이스들마다 별도의 라이센스를 부여받을 필요 없이 하나의 라이센스로 홈 네트워크 내의 각 디바이스들이 컨텐츠를 이용할 수 있도록 하는 시스템 및 방법에 관한 것이다.

도 1에서 보는 바와 같이, 기존 DRM(Digital Rights Management) 시스템은 미디어 파일을 배포하는 웹 서버와 각각의 디바이스에 맞게 라이센스를 부여하는 라이센스 서버, 그리고 웹 서버에서 다운로드 받은 미디어 파일과 라이센스 서버에서 인증받은 라이센스를 가지고 재생하는 디바이스로 구성된다. 한 공간에 하나의 PC가 존재한다고 가정한다면, 이와 같은 종래의 DRM 시스템을 이용하여도 별다른 문제나 제약 사항이 없다. 그러나, 홈 네트워크 상의 여러 디바이스에서 동일한 컨텐츠를 실행하는 경우가 빈번한 실정을 고려할 때, 종래의 방법은 홈 네트워크 개념을 고려하고 있지 않고 디바이스 별로 각각 다른 라이센스를 부여하고 있다. 따라서 디바이스1이 가지고 있는 미디어 파일과 디바이스2가 가지고 있는 동일한 미디어 파일에 같은 라이센스를 적용하는 것이 불가능하다. 결국, DRM 시스템을 홈 네트워크에 적용하면 홈 네트워크 내부의 각각의 디바이스마다 별도의 라이센스를 부여받아야 한다는 불편함이 있다는 것이다. 홈 네트워크는 그 개념상 홈 네트워크 안에 있는 모든 컨텐츠들의 공유가 가능하고 각 디바이스 별로 그러한 컨캔츠들의 실행이 가능하도록 하는 것이 중요한 점임을 감안할 때 현재의 DRM Architecture에 관한 수정의 필요성이 대두된다.

발명이 이루고자 하는 기술적 과제

본 발명은 디지털 미디어의 안전한 분배를 위해 라이센스를 미디어를 분리하여 실행시에 점검하도록 독립적으로 저장하여 라이센스의 변경시 재패키징 또는 재분배과정의 번거로움을 제거하는 것을 그 목적으로 한다.

또한 본 발명은 여러개의 디바이스들이 존재하는 홈 네트워킹 시스템 내에서, 각각의 디바이스들마다 별개로 라이센스를 부여받아야 하는 문제를 해결하기 위하여 홈 네트워크 상의 각각의 홈 디바이스 들이 하나의 라이센스를 공유할 수 있는 방법을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

상기의 목적을 달성하기 위하여, 본 발명은 각종 다른 디바이스와 데이터를 송수신하는 송수신 모듈; 상기 송수신 모듈을 통하여 홈디바이스로부터 라이센스 발급 요청을 받아서 해당 정식 라이센스가 라이센스 저장 모듈에 저장되어 있는지를 검색하고, 검색결과를 라이센스 요청 모듈과 임시 라이센스 발급 모듈에 전달하는 라이센스검색 모듈; 상기

라이센스가 상기 라이센스 저장 모듈에 존재하지 않는 경우에, 라이센스 서버에 해당 라이센스를 발급하여 줄 것을 상기 송수신모듈을 통하여 요청하는 라이센스요청 모듈; 상기 송수신 모듈을 통해 상기 라이센스 서버로부터 다운받은 라이센스를 저장하는 라이센스저장 모듈; 및 상기 라이센스 저장 모듈에 저장된 정식 라이센스를 이용하여 임시 라이센스를 상기 송수신 모듈을 통하 여 해당 홈디바이스에 발급하는 임시 라이센스 발급 모듈을을 포함하는 것을 특징으로 한다.

상기의 목적을 달성하기 위하여, 본 발명은 홈디바이스가 라이센스 관리 모듈에 해당 라이센스를 요청하는 단계; 상기 라이센스가 라이센스 관리 모듈내에 있는가를 판단하는 단계; 상기 판단 결과에 따라 상기 홈디바이스에 임시 라이센스를 부여하는 단계; 및 상기 홈디바이스에 존재하는 컨텐츠 재생기를 이용하여 미디어를 실행하는 단계를 포함하는 것을 특징으로 한다.

DRM(Digital Rights Management; 디지털 저작권 관리)은 보안은 물론 전체적인 디지털 콘텐츠의 저작권 관리 지원을 위한 포괄적인 시스템의 의미한다. 이를 위해서 우선 서버 차원의 보안처리를 생각할 수 있다. 즉 특정 권한을 부여받은 사용자만이 서버에 접속하여 미디어 파일을 다운로드 한다든지, 미디어 스트림을 실시간으로 전송받아 컨텐츠를 실행하는 등의 방법을 생각할 수 있다. 그러나, 한번 다운로드된 컨텐츠는 P2P(Peer to Peer) 서비스 검색기능을 통해 빠른 속도로 순식간에 배포되므로 교환 파일자체에 대한 보안처리 없이 서버 차원에서의 보안처리만으로는 대처할 수 없는 안심할 수 없다. 또한, 미디어 파일의 헤더 부분에 데이터비트를 조작하는 방법을 생각할 수 있지만, 이는 손쉬운 해킹 위험에 노출될 가능성이 크고, 검증받지 않은 미디어 파일의 조작으로 인하여 서비스가 불안할 염려가 있어 적당하지 않다. 한편, 워터마킹(Water Marking) 방법을 사용하는 것을 고려해 볼 수도 있다. 그러나 이는 본래 컨텐츠의 무단 도용이 있을 때 그 원래의 저작자 또는 그 출처를 밝히기 위한 것이다. 이는 보안 방법이라기 보다는 저작권 관리 기능에 불과하여 무단사용자의 컨텐츠 사용 자체를 차단할 수는 없다.

따라서, 파일 자체를 암호화하고 디바이스(PC, PDA 등) 단위의 고유 라이센스 발급 및 인증을 통하여 관람횟수 설정, 유효시간, 무료 관람기간 및 시간설정, 복사 가능 횟수 등 여러 가지 조합으로 라이센스를 설정할 수 있도록 하는 컨텐츠 보안 방법을 사용하는 것이 바람직하다. 또한, 이 방법은 포괄적인 의미에서의 스트림 접속의 보안과 미디어 파일의 보안에 동시에 적용할 수 있다. 또한, 이용자간 복제를 통하여 확산되는 Super Distribution는 오히려 서비스 제공자의 매출 확대에 기여하게 된다.

이하 도면에 따라 발명의 일 실시예를 상세히 설명한다.

도 2는 본 발명이 제안하는 시스템을 전체적으로 나타낸 블록도이다. 본 발명이 제안하는 시스템은 원 컨텐츠(Raw Contents), 즉 원 미디어 파일을 라이센스 키를 이용하여 암호화(Encryption)하는 패키징 모듈(Packager; 220), 상기 암호화된 미디어 파일을 각 디바이스에서 다운로드 할 수 있도록 서비스를 제공하는 웹 서버(Web Server; 230), 상기 암호화된 미디어 파일을 각 디바이스에서 실시간으로 실행시킬 수 있도록 미디어 스트림을 제공하는 미디어 서버(Media Sever; 240), 홈 디바이스의 요청을 받아서 상기 홈 디바이스의 고유의 하드웨어 ID를 파악하고 상기 홈 디바이스에서만 해당 컨텐츠를 실행할 수 있는 라이센스를 발급하는 라이센스 서버(License Server; 210)으로 구성될 수 있다.

상기 패키징 서버(220)는 컨텐츠 제공자에 의하여 제공된 원본 컨텐츠와 라 이센스 키 등의 메타데이터를 함께 패키징하여 가공된 컨텐츠를 웹 서버 또는 미디어 서버에 전달하는 역할을 수행한다. 패키징 과정을 통하여 컨텐츠 보호 유지를 목적으로 라이센스 키를 이용하여 다양한 미디어 파일에 대해 잠금(lock)을 생성하며 64비트 암호화 라이센스를 생성함으로써 안전한 파일 배포를 가능하게 한다. 컨텐츠 제공자는 상기 패키징 서버(220)를 통하여 라이센스 키 시드(License Key Seed)와 키 ID(Key ID)와 결합함으로써 패키징 과정을 수행하며, 결과적으로 암호화된 미디어 파일을 생성한다. 패키징 과정에 대한 구체적인 내용은 MS DRM Homepage http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx 또는 http://www.microsoft.com/windows/windowsmedia/wm7/DRM/tutorial.aspx 를 이용하여 확인할 수 있다.

상기 웹 서버(230)는 미디어 파일의 다운로드 서비스를 제공하는 서버로서, 컨텐츠 제공자와 동일한 주체에 의하여 운영될 수도 있고, 단순히 자료의 배포만을 담당하는 별도의 서비스 제공자에 의하여 운영될 수도 있다. 또한, 상기 미디어 서버(240)는 미디어 파일의 스트림 서비스를 제공하는 서버로서, 상기 웹 서버와 마찬가지로 컨텐츠 제공자와 동일 또는 다른 주체에 의하여 운영될 수 있다. 결국 컨텐츠는 상기 웹 서버와 스트림 서버에 의하여 디바이스 사용자에게 널리 배포(Distribution)되는 것이다.

상기 홈 네트워크(250)는 내부에 각각의 홈디바이스들을 포함하고 있으며, 본 발명에 있어서 특징적인 요소인 라이센스 관리 모듈(340)을 포함하고 있다. 이 에 대한 구체적인 동작은 도3 내지 도5에서 설명하기로 한다.

상기 라이센스 서버(210)는 컨텐츠의 사용권한을 부여하고 이에 대한 지속적 관리를 담당하는 장치이다. 본 장치는 사용자의 컨텐츠 결제 처리를 담당하는 부분과, 사용권한정보가 담겨 있는 라이센스를 발급하고 관리하는 부분 및 사

용자의 사용내역을 수집하여 이를 통계 처리하는 부분으로 구성될 수 있다. 비안가된 디바이스의 경우 컨텐츠의 실행시에 컨텐츠 사용 라이센스를 인가받아야 한다. 각 디바이스는 라이센스 서버에 실행하는 컨텐츠 재생기의 ID 및 하드웨어 ID(MAC Address를 예로 들 수 있다)를 전달하면 라이센스 생성기는 각각의 디바이스에 고유한 라이센스를 생성하여 발급한다. 이러한 개별화(individualization)를 통하여 라이센스 처리 과정에서 변조된 재생기의 정보 확인을 통해 라이센스 발급 차단 등의 조치를 취할 수 있다. 또한 각 라이센스는 각각의 디바이스에 국한되어 발급됨으로써 라이센스의 복제는 의미가 없으므로 라이센스를 안전하게 관리할 수 있다. 라이센스를 생성하는 과정을 살펴보면, 라이센스 서버(210)는 라이센스 키 시드(License Key Seed)를 상기 패키징 서버(220)에 의하여 암호화된 미디어 파일로부터 키 ID(Key ID)와 결합하여 라이센스를 생성한다. 미디어 파일 패키징과 라이센스의 발급은 공유키의 공유로 별도의 기관 또는 단체에서 수행할 수 있다. 라이센싱 과정에 대한 구체적인 내용은 MS DRM Homepage

http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx 또는 http://www.microsoft.com/windows/windowsmedia/wm7/DRM/tutorial.aspx 를 이용하여 확인할 수 있다.

도 3은 다운로드 서비스를 받아 컨텐츠를 실행하고자 하는 경우에 홈 네트워크 상에서 라이센스를 공유하는 구성을 나타낸 블록도이다. 본 실시예는 미디어 파일을 배포하는 웹 서버(230), 각각의 디바이스 및 컨텐츠에 맞게 라이센스를 부여하는 라이센스 서버(210), 상기 라이센스 서버로부터 부여받은 라이센스를 홈 네트워크 상에서 공유할 수 있게 해주는 라이센스 관리 모듈(340) 그리고 웹 서버에서 다운로드 받은 미디어 파일과 라이센스 서버로부터 발급된 라이센스를 이용하여 미디어 파일을 재생하는 컨텐츠 재생기를 갖는 홈디바이스(310, 320, 330)로 구성될 수 있다. 하나의 홈디바이스1(310)이 웹서버로부터 미디어 파일1(110)을 다운로드 받아서, 그것을 재생하고자 하는 하는 경우에 홈디바이스2(320)은 홈디바이스1에 있는 미디어 파일1(110)을 다시 다운로드하여 재생하고자 할 수 있으며, 홈디바이스3(330)은 홈디바이스1(310)에 있는 미디어 파일1(110)을 스트림 방식으로 바로 재생하고자 할 수 있다. 이 때, 홈디바이스1(310)에 의하여 라이센스 요청을 받은 라이센스 관리 모듈(340)은 라이센스 서버(210)에 상기 미디어 파일1을 실행하기 위하여 라이센스A(120)를 다운받아서 저장하게 된다. 이후 라이센스 관리 모듈은 다운로드 받은 라이센스A(120)를 이용하여 각각의 홈디바이스에 임시 라이센스를 발급한다. 그러면, 각각의 홈디바이스는 동일한 미디어 파일을 각 임시 라이센스를 이용하여 재생할 수 있다. 만약, 라이센스 정책에서 관람회수 제한으로 설정되어 있다면 각각의 홈디바이스에 실행회수의 총합이 제한회수에 해당하면 라이센스가 만료되고 재생이 더 이상되지 않을 것이다. 또한 라이센스 정책에서 유효시간 제한으로 설정되어 있다면 사용시간의 총합이, 복사기능 회수로 설정되어 있다면 홈디 바이스간의 총 복사회수의 총합이 라이센스 만료 기준이 될 수 있다.

도 4는 스트림 서비스를 받아 컨텐츠를 실행하고자 하는 경우에 홈 네트워크 상에서 라이센스를 공유하는 구성을 나타낸 블록도이다. 본 실시예에 있어서의 시스템은 상기 도 3에서와 마찬가지로 라이센스 서버(210), 라이센스 관리 모듈(340), 홈 디바이스(310, 320, 330)를 포함한다. 다만, 웹 서버 대신에 미디어 파일의 스트림 서비스를 제공하는 미디어 서버(240)를 포함한다.

다수의 홈디바이스들(310, 320, 330)이 미디어 서버(240)으로부터 미디어 스트림1(130)을 받아 실시간으로 재생하고자 하는 하는 경우에 이중 하나의 홈디바이스에 의하여 먼저 라이센스 요청을 받은 라이센스 관리 모듈(340)은 라이센스 서버(210)에 상기 미디어 스트림1(130)을 실행하기 위하여 라이센스B(140)를 다운받아서 저장하게 된다. 이후 라이센스 관리 모듈은 다운로드 받은 라이센스B(120)를 이용하여 각각의 홈디바이스에 임시 라이센스를 발급한다. 그러면, 각각의 홈디바이스는 동일한 미디어 스트림을 각 임시 라이센스를 이용하여 재생할 수 있다. 도 3의 설명에서와 마찬가지로 제한된 실행회수, 실행 유효시간 내에서 홈디바이스들의 실행회수, 실행 유효시간의 총합이 제한 범위에 해당되면 라이센스가 만료된다.

도 5는 본 발명이 제안하는 라이센스 관리 모듈(340)의 구성요소의 동작을 나타낸 블록도이다. 본 발명에서 제안하는 라이센스 관리 모듈은 홈네트워크 상에서의 모든 미디어 파일 또는 미디어 스트림에 대한 라이센스를 라이센스 서버에 요청하고, 라이센스 서버(210)로부터 다운받은 라이센스를 이용하여 임시 라이센스 를 생성, 발급하는 모듈이다. 즉 라이센스 서버로부터 다운 받은 라이센스를 각각의 디바이스에서 사용할 수 있도록 하는 역할을 수행한다. 상기 라이센스 관리 모듈(340)은 홈 네트워크 사용자가 라이센스를 공유할 수 있도록 컨텐츠 제공자가 제공할 수 있으며, 따라서 라이센스 서버(210)가 라이센스를 발급하는 과정에서 사용하는 방식을 그대로 적용할 수 있는 것이다. 각 디바이스가 라이센스 저장 모듈(344)에 컨텐츠 재생기의 ID 및 하드웨어 ID를 전달하면서 라이센스를 요청하면 상기 라이센스 관리 모듈(344)은 라이센스 서버(210)에 라이센스를 요청하여 이를 발급받아 저장하고 각 디바이스에 고유한 임시 라이센스를 발급하는 것이다.

이러한 라이센스 관리 모듈(344)는 다시 송수신 모듈(341), 라이센스 요청 모듈(342), 라이센스 검색 모듈(343), 라이센스 저장 모듈(344) 및 임시 라이센스 발급 모듈(345)로서 구성될 수 있다. 상기 송수신 모듈(341)은 홈디바이스로부터 라이센스 발급 요청을 받아들이고, 상기 라이센스 서버(210)에 라이센스 발급 요청을 전송하여 상기 라이센스 서버로부터 발급되는 정식 라이센스(상기 임시 라이센스와 대비하여 라이센스 서버에서 발급하는 라이센스를 정식 라이센스로 명명할 수 있다)를 다운받는다. 또한, 각 디바이스에 고유한 임시 라이센스를 전송하는 역할을 수행한다. 상기 라이센스 검색 모듈(343)은 상기 홈디바이스들로부터 라이센스 발급 요청을 받은 후 해당 정식 라이센스가 이미 라이센스 저장 모듈(344)에 저장되어 있는지를 검색하며, 그 검색결과를 라이센스 요청 모듈(342)과 임시 라이센스

발급 모듈(345)에 전달하는 역할을 담당한다. 상기 라이센스 저장 모듈(344)은 라이센스 검색 모듈(343)은 송수신 모듈(341)을 통해 라이센스 서버(210)로부터 다운 받은 정식 라이센스를 저장한다. 상기 라이센스 요청 모듈(342)은 홈 디바이스 및 컨텐츠에 상응하는 정식 라이센스가 저장 모듈(344)에 존재하지 않는 경우에, 라이센스 서버(210)에 해당 정식 라이센스를 발급하여 줄 것을 송수신모듈(341)을 통하여 요청하는 역할을 수행한다. 그리고, 상기 임시 라이센스 발급 모듈(345)은 상기 라이센스 저장 모듈(344)에 저장된 정식 라이센스를 이용하여 다른 디바이스에서도 미디어 파일 또는 미디어 스트림을 사용할 수 있도록 하는 임시 라이센스를 상기 송수신 모듈(341)을 통하여 발급하는 역할을 수행한다.

도 6은 본 발명이 제안하는 방법에 따른 과정을 전체적으로 나타낸 흐름도이다. 먼저, 컨텐츠 제공자에 의해 암호화된 원본 컨텐츠와 라이센스 키를 함께 패키징하여 암호화된 컨텐츠를 생성하는 과정이다(S610). 다음 단계로서 웹 서버 또는 미디어 서버를 통하여 상기 암호화된 컨텐츠를 사용자에게 배포하는 단계이다(S620). 디지털 컨텐츠 배포는 컨텐츠 구매 및 사용 유형 정의 단계로 사용자의 다양한 서비스 요구를 지원한다. 초기의 DRM은 컨텐츠 분배시 다운로드한 단말에 대해서만 가능하도록 한정하였으나, 현재에는 홈 네트워크 상의 다양한 장치로의 이동(super distribution)이나 사용자가 소유한 여러 단말에 대한 로밍(roaming)을 통하여 배포될 수 있다. 컨텐츠와 라이센스가 분리되어 있으므로, 패키징된 컨텐츠에 대한 접근은 자유롭게 허용되나 사용시에는 반드시 해당 라이센스를 발급받아야 하므로 컨텐츠의 무단 복제에 안정하게 대응할 수 있는 것이다. 다음 단계로서 라이센스 정책 설정하는 단계이다(S630). 컨텐츠 제공자의 정책에 따라 관람회수 설정, 유효시간, 무료관람기간 및 시간 설정, 복사가능 회수 등 여 라가지 조합으로 설정할 수 있으며, 기존 파일 다운로드 형태의 오프라인 서비스 이외의 동영상 스트리밍 서비스와 같은 온라인 서비스 유형을 고려할 수 있다. 온라인 서비스의 경우 컨텐츠 사용 규칙 또는 복호화 등의 관련 정보를 서버에 저장할 수 있고 사용 규칙의 동적 변경으로 사용권 제어 능력의 향상 및 홈네트워크에서 라이센스 처리시의 절차 등을 보다 단순화 할 수 있다. 다음으로는 라이센스 관리 모듈이 라이센스 서버에 라이센스를 발급해 줄 것을 요청하는 단계이다(S650). 본 과정은 미디어를 실행하려는 홈디바이스로부터 라이센스 관리 모듈에 라이센스 발급 요청을 받은 라이센스 관리 모듈이 해당 라이센스가 존재하지 않으면 라이센스 서버에 해당 라이센스의 발급을 요청하는 것이다. 다음 과정으로서 각각의 홈디바이스에서 컨텐츠를 실행할 수 있도록 라이센스 관리 모듈이 상기 발급받은 라이센스를 가공하여 각각의 임시 라이센스를 발급한다(S670). 마지막으로 각 디바이스는 상기 임시 라이센스를 이용하여 상호 동일한 컨텐츠를 실행할 수 있다.

도 7은 본 발명이 제안하는 방법에 따른 과정을 홈 네트워크를 중심으로 상세하게 나타낸 흐름도이다. 하나의 홈디바이스가 웹 서버 또는 미디어 서버에 접속하여 미디어 파일을 다운받아 컨텐츠 재생기로 실행하거나 또는 미디어 스트림을 전송받아 상기 재생기를 통해 실시간으로 실행한다(S710). 처음에는 홈디바이스 내부에 라이센스가 존재하지 않아서 실행이 불가능하므로, 각 홈디바이스는 라이센스 관리 모듈에 라이센스의 발급을 요청하게 된다(S720). 라이센스 발급 모듈내의 라이센스 검색 모듈은 상기 한 요청에 따라 해당하는 라이센스가 라이센스 저장 모듈에 존재하는지를 검색하여 그 존재여부를 판단한다(S730). 만약 라이센스 저장 모 듈에 해당 라이센스가 존재하지 않는다면, 라이센스 발급 모듈중의 라이센스 요청 모듈은 라이센스 서버에 해당 라이센스를 요청하고 이를 다운로드한다(S750). 그리고, 상기 다운로드한 라이센스와 동일한 라이센스를 임시 라이센스로서 상기 홈디바이스에 부여한다(S760). 이 경우는 하나의 미디어 파일 또는 미디어 스트림에 대하여 처음으로 라이센스를 요청하는 경우로서 라이센스 서버가 발급한 라이센스를 그래도 홈디바이스에 부여하여도 문제가 없기 때문에 이와 동일한 임시 라이센스를 홈디바이스에 부여하는 것이다. 그후 부여받은 임시 라이센스를 이용하여 컨텐츠 재생기로 하여금 미디어 파일 또는 미디어 스트림을 실행하게 한다(S770).

만약 라이센스 저장 모듈에 해당 라이센스가 존재한다면 상기 홈디바이스의 하드웨어 ID, 컨텐츠 재생기의 ID 및 기 발급된 라이센스로부터 상기 홈디바이스에서만 실행가능한 임시 라이센스를 부여받는다(S740). 그후 부여받은 임시 라이센스를 이용하여 컨텐츠 재생기로 하여금 미디어 파일 또는 미디어 스트림을 실행하게 한다(S770).

이상, 본 발명을 바람직한 실시예를 들어 상세하게 설명하였으나, 본 발명은 상기 실시예에 한정되지 않으며, 본 발명의 기술적 사상의 범위 내에서 당해 분야에서 통상의 지식을 가지는 자에 의하여 여러 가지 변형이 가능하다.

발명의 효과

본 발명에 의하면 이로써 홈 네트워크 내에서의 모든 디바이스들은 하나의 라이센스를 공유함으로써 동일한 미디어 파일이나 미디어 스트림을 하나의 라이센스를 통하여 재생할 수 있는 편리함을 제공하는 효과가 있다.

또한 본 발명에 의하면 홈 네트워크 전체에 하나의 라이센스를 이용하여 전체적 제한 조건하에서 각각의 홈 디바이스들 간에 다양한 실행조건을 분배할 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.
라이센스 서버가 제공한 정식 라이센스를 저장하는 라이센스저장 모듈; 및

상기 라이센스 저장 모듈에 저장된 정식 라이센스를 이용하여 네트워크내 홈디바이스에서 사용할 수 있는 임시 라이센스를 발급하는 임시 라이센스 발급 모듈을 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 장치.

청구항 2.
제1항에 있어서,

홈디바이스로부터 라이센스 발급 요청을 받아서 해당 정식 라이센스가 라이센스 저장 모듈에 저장되어 있는지를 검색하고, 검색결과를 라이센스 요청 모듈과 임시 라이센스 발급 모듈에 전달하는 라이센스검색 모듈; 및

상기 정식 라이센스가 상기 라이센스 저장 모듈에 존재하지 않는 경우에는 라이센스 서버에 해당 라이센스를 발급하여 줄 것을 요청하는 라이센스 요청 모듈을 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 장치.

청구항 3.
각각의 홈디바이스 및 컨텐츠에 맞게 라이센스를 부여하는 라이센스 서버;

상기 컨텐츠의 다운로드 서비스를 제공하는 웹 서버;

상기 웹 서버로부터 다운받은 컨텐츠와 라이센스 서버로부터 발급된 라이센 스를 이용하여 미디어 파일을 재생하는 컨텐츠 재생기를 포함하는 홈 디바이스; 및

상기 라이센스 서버로부터 부여받은 라이센스를 홈 네트워크 상에서 공유할 수 있게 해주는 라이센스 발급 모듈을 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 시스템.

청구항 4.
제3항에 있어서,

원본 컨텐츠를 패키징함으로써 암호화된 컨텐츠를 생성하는 패키징 서버를 더 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 시스템.

청구항 5.
제3항 또는 제4항에 있어서,

상기 컨텐츠의 스트림 서비스를 제공하는 미디어 서버를 더 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 시스템.

청구항 6.
제3항 또는 제4항에 있어서, 상기 라이센스 발급 모듈은

라이센스 서버가 제공한 정식 라이센스를 저장하는 라이센스저장 모듈; 및

상기 라이센스 저장 모듈에 저장된 정식 라이센스를 이용하여 네트워크내 홈디바이스에서 사용할 수 있는 임시 라이센스를 발급하는 임시 라이센스 발급 모듈을 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 시스템.

청구항 7.
제6항에 있어서, 상기 라이센스 발급 모듈은

홈디바이스로부터 라이센스 발급 요청을 받아서 해당 정식 라이센스가 라이센스 저장 모듈에 저장되어 있는지를 검색하고, 검색결과를 라이센스 요청 모듈과 임시 라이센스 발급 모듈에 전달하는 라이센스검색 모듈; 및

상기 정식 라이센스가 상기 라이센스 저장 모듈에 존재하지 않는 경우에는 라이센스 서버에 해당 라이센스를 발급하여 줄 것을 요청하는 라이센스 요청 모듈을 더 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위

한 라이센스 관리 시스템.

청구항 8.
홈디바이스가 라이센스 관리 모듈에 해당 라이센스를 요청하는 단계;

상기 라이센스가 라이센스 관리 모듈내에 있는가를 판단하는 단계;

상기 판단 결과에 따라 상기 홈디바이스에 임시 라이센스를 부여하는 단계; 및

상기 홈디바이스에 존재하는 컨텐츠 재생기를 이용하여 미디어를 실행하는 단계를 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 방법.

청구항 9.
제8항에 있어서, 상기 판단한 결과 해당 라이센스가 라이센스 관리 모듈에 없으면, 상기 홈디바이스에 임시 라이센스를 부여하는 단계는

라이센스 서버로부터 라이센스를 다운로드하는 단계; 및

다운로드한 라이센스와 동일한 임시 라이센스를 부여하는 단계를 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 방법.

청구항 10.
제8항에 있어서, 상기 판단한 결과 해당 라이센스가 라이센스 관리 모듈에 있으면, 상기 홈디바이스에 임시 라이센스를 부여하는 단계는

하드웨어 ID 및 재생기 ID를 이용하여 임시 라이센스를 부여하는 단계를 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 방법.

청구항 11.
제8항 내지 제10항 중 어느 한 항에 있어서, 상기 라이센스 관리 모듈에 해당 라이센스를 요청하는 단계 이전 단계로서,

원 컨텐츠를 패키징하는 단계;

패키징된 컨텐츠를 배포하는 단계;

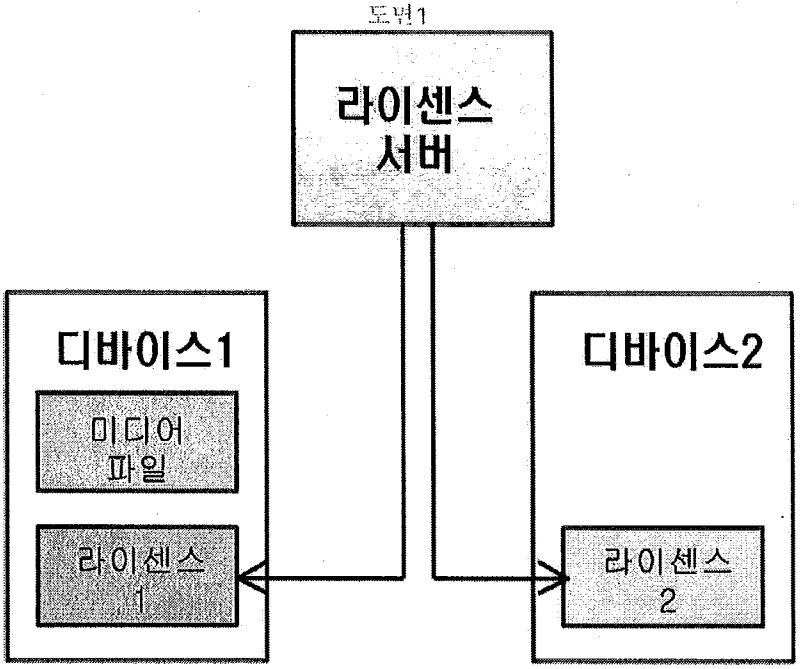
라이센스 정책을 설정하는 단계; 및

홈디바이스가 컨텐츠를 다운로드하는 단계를 더 포함하는 것을 특징으로 하는 홈 네트워크 상에서의 컨텐츠 실행을 위한 라이센스 관리 방법.

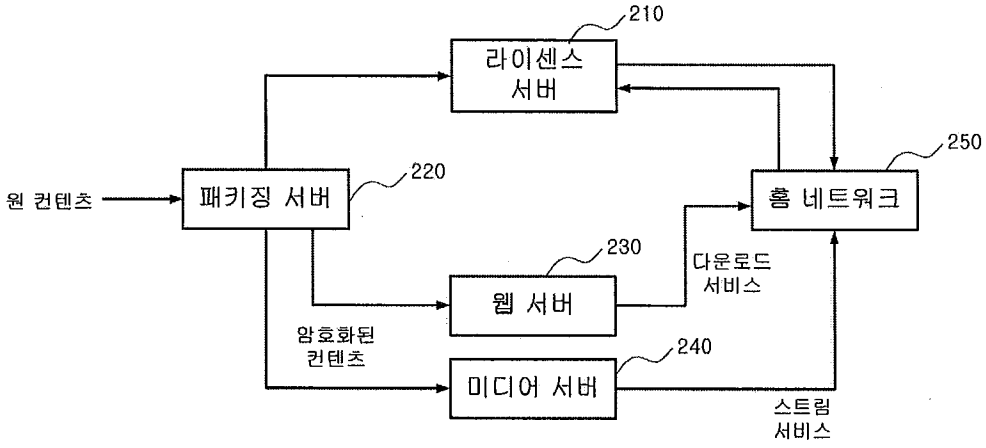
청구항 12.
제8항 내지 제10항 중 어느 한 항에 있어서, 상기 방법을 실행하기 위한 컴 퓨터 프로그램을 컴퓨터로 판독 가능한 포맷으로 기록한 기록매체.

도면

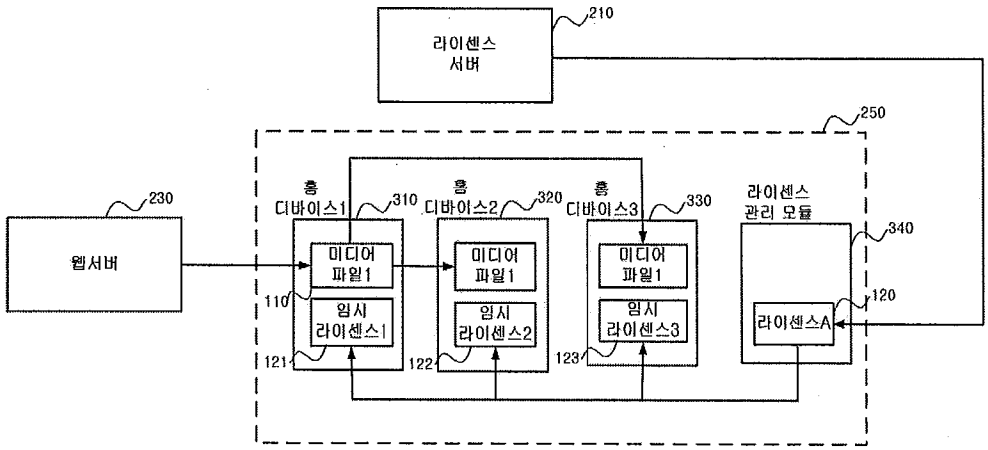
도면1


라이센스
서버
디바이스1
미디어
파일
라이센스
1
디바이스2
라이센스
2

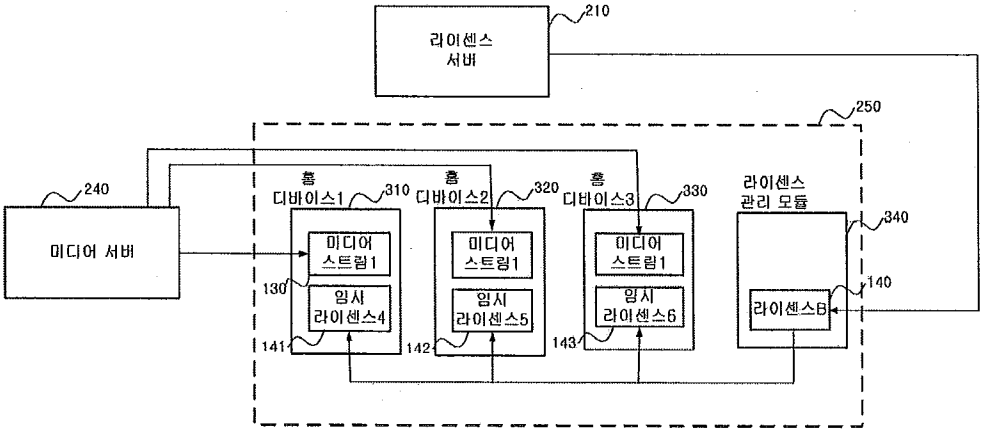
도면2


210
라이센스
서버
250
원 컨텐츠
220
패키징 서버
홈 네트워크
230
웹 서버
다운로드
서비스
암호화된
컨텐츠
240
미디어 서버
스트림
서비스

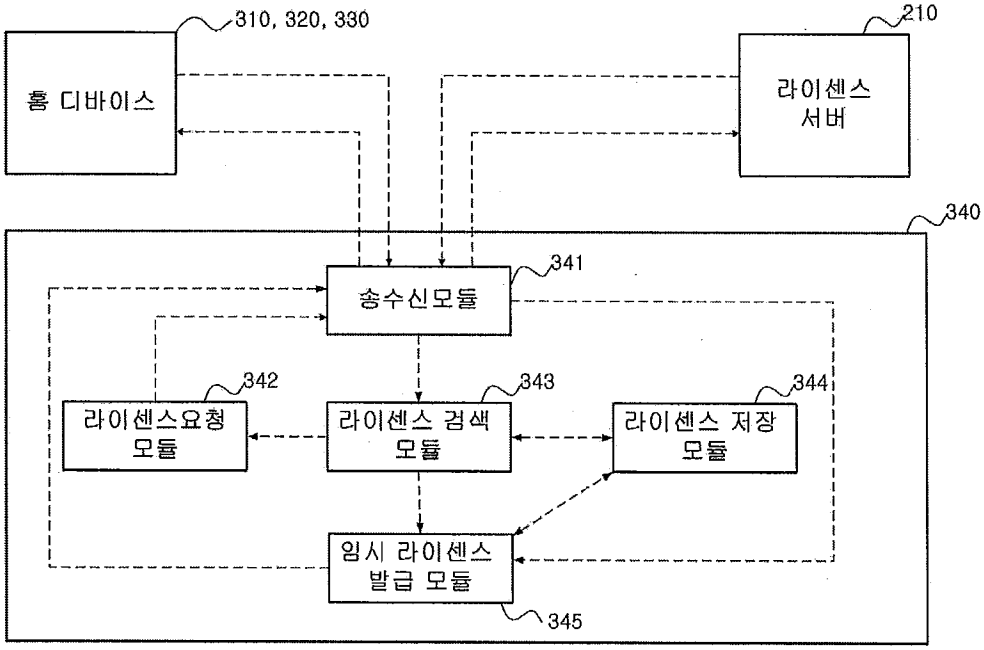
도면3


210
라이센스
서버
250
230
웹서버
홈
디바이스1
310
홈
디바이스2
320
홈
디바이스3
330
라이센스
관리 모듈
340
미디어
파일1
미디어
파일1
미디어
파일1
110
임시
라이센스1
임시
라이센스2
임시
라이센스3
120
라이센스A
121
122
123

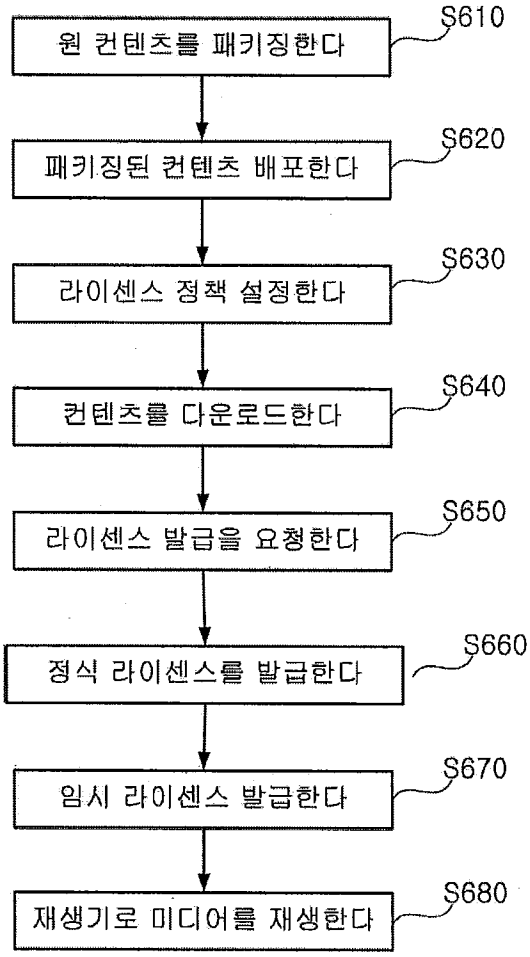
도면4


라이센스
서버
210
250
240
미디어 서버
홈
디바이스1
310
홈
디바이스2
320
홈
디바이스3
330
라이센스
관리 모듈
340
미디어
스트림1
미디어
스트림1
미디어
스트림1
130
임시
라이센스4
임시
라이센스5
임시
라이센스6
라이센스B
140
141
142
143

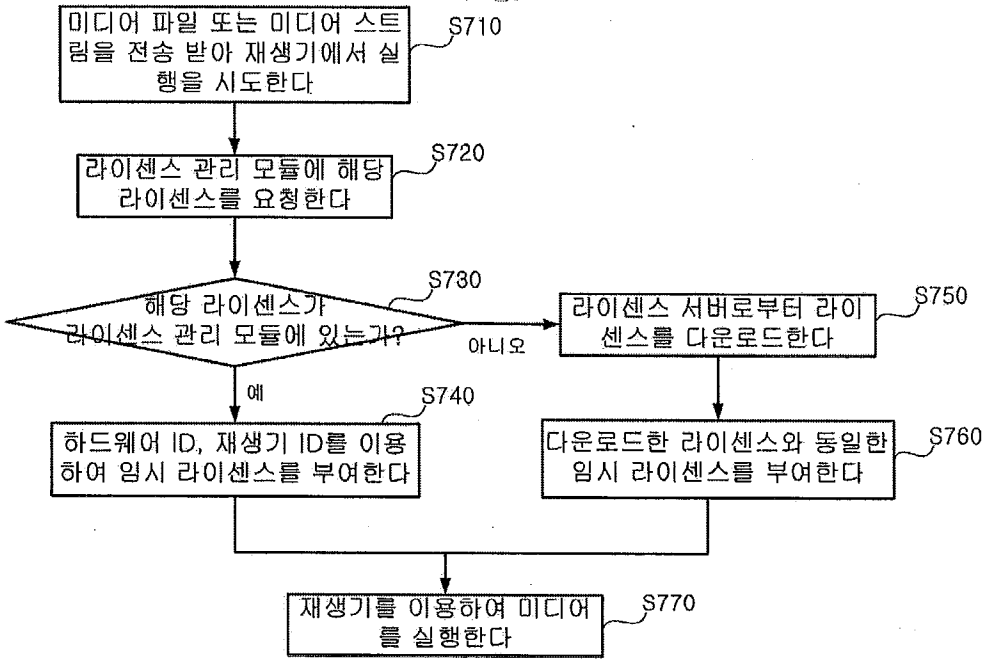
도면5


310, 320, 330
홈 디바이스
210
라이센스
서버
340
341
송수신모듈
342
343
344
라이센스요청
모듈
라이센스 검색
모듈
라이센스 저장
모듈
임시 라이센스
발급 모듈
345

도면6


원 컨텐츠를 패키징한다
S610
패키징된 컨텐츠 배포한다
S620
라이센스 정책 설정한다
S630
컨텐츠를 다운로드한다
S640
라이센스 발급을 요청한다
S650
정식 라이센스를 발급한다
S660
임시 라이센스 발급한다
S670
재생기로 미디어를 재생한다
S680

도면7


미디어 파일 또는 미디어 스트림을 전송 받아 재생기에서 실행을 시도한다
S710
라이센스 관리 모듈에 해당 라이센스를 요청한다
S720
해당 라이센스가 라이센스 관리 모듈에 있는가?
S730
아니오
라이센스 서버로부터 라이센스를 다운로드한다
S750
예
하드웨어 ID, 재생기 ID를 이용하여 임시 라이센스를 부여한다
S740
다운로드한 라이센스와 동일한 임시 라이센스를 부여한다
S760
재생기를 이용하여 미디어를 실행한다
S770

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11) Registration number: 100708203 B1

(45) Issue date: 10.04.2007

(24) Registration date: 10.04.2007

(21) Application number: 1020060018430

(22) Application date: 24.02.2006

(73) Proprietor:

(72) Inventor: • KWON, WON SEOK

(51) Int. Cl: H04L 12/12
H04L 12/16
H04L 29/06
H04L 12/28

(54) **CONTROL PERMISSION METHOD OF A DEVICE CAPABLE OF ALLOWING A DEVICE TO SELECTIVELY PERMIT ITS CONTROL ONLY TO A PARTICULAR CONTROL POINT WHICH IS ALREADY PARTICIPATING IN A DOMAIN IN WHICH THE DEVICE IS ALSO PARTICIPATING, TO THUS BE CONTROLLED ONLY BY THE PARTICULAR CONTROL POINT**

(57) Abstract:

PURPOSE: A control permission method of a device using the same are provided to prevent a control point connected with the same network from controlling a device unless it participates in a domain.

CONSTITUTION: A device checks whether a domain identifier can be extracted from a received participation message(300,310). When a domain identifier can be extracted, the device extracts the domain identifier from the received participation message(320). The device checks whether the extracted domain identifier has been previously registered in a list of domain identifiers(330). When the domain identifier has been registered in the

list, a control point can participate in a domain, so the device transmits a response message to the control point(340).

Legal Status

Date of request for an examination (20060224)

Notification date of refusal decision (00000000)

Final disposal of an application (registration)

Date of final disposal of an application (20070226)

Patent registration number (1007082030000)

Date of registration (20070410)

Number of opposition against the grant of a patent ( )

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ( )

Date of requesting trial against decision to refuse ( )

Date of extinction of right ( )

(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/12 (2006.01)
H04L 12/16 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(45) 공고일자 2007년04월16일
(11) 등록번호 10-0708203
(24) 등록일자 2007년04월10일

(21) 출원번호 10-2006-0018430
(22) 출원일자 2006년02월24일
심사청구일자 2006년02월24일

(65) 공개번호
(43) 공개일자

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 권원석
경기 수원시 영통구 망포동 방죽마을 영통뜨란채 1006-1503

(74) 대리인 리앤목특허법인

(56) 선행기술조사문헌
KR20030055766 A
KR20040111426 A
KR20050053471 A
KR20040014731 A
KR20050028244 A
KR20050059027 A
* 심사관에 의하여 인용된 문헌

심사관 : 양찬호

전체 청구항 수 : 총 19 항

(54) 디바이스의 제어 허용 방법 및 그를 이용한 디바이스

(57) 요약

본 발명은 제어 포인트에게 제어를 허용하는 UPnP(Universal Plug and Play) 디바이스에 관한 것으로, 디바이스가 참가한 도메인에 제어 포인트가 이미 참가하였는지 여부를 판단하여 제어 포인트에게 디바이스에 대한 제어를 선택적으로 허용함으로써 특정한 제어 포인트에게만 디바이스의 제어를 허용할 수 있다.

대표도

도 3a

특허청구의 범위

청구항 1.

적어도 하나의 디바이스를 제어하는 제어 포인트에게 소정의 디바이스가 제어를 허용하는 방법에 있어서,

상기 소정의 디바이스가 참가한 도메인에 상기 제어 포인트가 이미 참가하였는지 여부를 판단하는 단계; 및

상기 판단된 결과에 따라 상기 제어 포인트에게 상기 소정의 디바이스에 대한 제어를 선택적으로 허용하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2.

제1항에 있어서, 상기 허용하는 단계는

상기 제어 포인트가 이미 참가하였다고 판단된다면, 상기 소정의 디바이스에 대한 제어를 허용하는 것을 특징으로 하는 방법.

청구항 3.

제1항에 있어서, 상기 판단하는 단계는

상기 소정의 디바이스를 제어할 수 있는 권한을 나타내는 제어 포인트의 식별자를 이용하여 상기 제어 포인트가 이미 참가하였는지 여부를 판단하는 것을 특징으로 하는 방법.

청구항 4.

제3항에 있어서, 상기 제어 포인트의 식별자는

상기 제어 포인트가 참가하고자 하는 도메인에 상기 소정의 디바이스로부터 참가가 허용된 경우 생성되는 것을 특징으로 하는 방법.

청구항 5.

제1항에 있어서,

상기 제어 포인트로부터 상기 소정의 디바이스의 상태를 알리는 이벤트에 대한 가입을 요청받는 단계; 및

상기 판단하는 단계에서 판단된 결과에 따라 상기 요청한 소정의 디바이스의 상태에 관한 메시지를 선택적으로 상기 요청한 제어 포인트에게 송신하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 6.

제1항에 있어서,

상기 제어 포인트로부터 상기 도메인에서 탈퇴를 요청받는 단계; 및

상기 판단하는 단계에서 판단된 결과에 따라 상기 요청한 제어 포인트를 상기 도메인에서 탈퇴시키는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 7.

적어도 하나의 디바이스를 제어하는 제어 포인트에게 소정의 디바이스가 참가를 허용하는 방법에 있어서,

상기 소정의 디바이스가 참가한 도메인에 상기 제어 포인트가 참가할 수 있는 여부를 판단하는 단계; 및

상기 판단된 결과에 따라 상기 제어 포인트를 상기 도메인에 선택적으로 참가를 허용하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 8.

제7항에 있어서, 상기 판단하는 단계는

상기 제어 포인트가 참가하고자 하는 도메인의 식별자와 상기 디바이스가 참가한 도메인의 식별자의 동일 여부를 기초로 하여 판단하는 것을 특징으로 하는 방법.

청구항 9.

제7항에 있어서, 상기 허용하는 단계는

상기 참가가 허용된 제어 포인트에 대하여 상기 소정의 디바이스를 제어할 수 있는 권한을 나타내는 제어 포인트의 식별자를 생성하여 상기 제어 포인트에게 전송함으로서 허용하는 것을 특징으로 하는 방법.

청구항 10.

제1항 내지 제9항 중 어느 한 항에 기재된 발명을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

청구항 11.

적어도 하나의 디바이스를 제어하는 제어 포인트에게 제어를 허용하는 디바이스에 있어서,

상기 디바이스가 참가한 도메인에 상기 제어 포인트가 이미 참가하였는지 여부를 판단하는 제어포인트 판단부; 및

상기 판단된 결과에 응답하여 상기 제어 포인트에게 상기 디바이스에 대한 제어를 선택적으로 허용하는 제어 허용부를 포함하는 것을 특징으로 하는 디바이스.

청구항 12.

제11항에 있어서, 상기 제어 허용부는

상기 제어포인트 판단부에서 참가하였다고 판단되면, 상기 디바이스에 대한 제어를 허용하는 것을 특징으로 하는 디바이스.

청구항 13.

제11항에 있어서, 상기 제어포인트 판단부는

상기 디바이스를 제어할 수 있는 권한을 나타내는 제어 포인트의 식별자를 이용하여 상기 제어 포인트가 이미 참가하였는지 여부를 판단하는 것을 특징으로 하는 디바이스.

청구항 14.

제13항에 있어서, 상기 제어 포인트의 식별자는

상기 제어 포인트가 참가하고자 하는 도메인에 상기 디바이스로부터 참가가 허용된 경우 생성되는 것을 특징으로 하는 디바이스.

청구항 15.

제11항에 있어서,

상기 디바이스가 참가한 도메인에 상기 제어 포인트가 참가할 수 있는지 여부를 판단하는 참가 판단부; 및

상기 참가 판단부에서 판단된 결과에 응답하여 상기 제어 포인트를 상기 도메인에 선택적으로 참가를 허용하는 참가 허용부를 더 포함하는 것을 특징으로 하는 디바이스.

청구항 16.

제15항에 있어서, 상기 참가 판단부는

상기 제어 포인트가 참가하고자 하는 도메인의 식별자와 상기 디바이스가 참가한 도메인의 식별자의 동일 여부를 기초로 하여 판단하는 것을 특징으로 하는 디바이스.

청구항 17.

제15항에 있어서,

상기 참가가 허용된 제어 포인트에 대하여 상기 디바이스를 제어할 수 있는 권한을 나타내는 제어 포인트의 식별자를 생성하는 식별자 생성부를 더 포함하는 것을 특징으로 하는 디바이스.

청구항 18.

제11항에 있어서,

상기 제어 포인트로부터 상기 디바이스의 상태를 알리는 이벤트에 대한 가입을 요청받는 가입 수신부; 및

상기 제어포인트 판단부에서 판단된 결과에 응답하여 상기 요청한 제어 포인트에게 상기 디바이스의 상태에 관한 메시지를 선택적으로 송신하는 가입 허용부를 더 포함하는 것을 특징으로 하는 디바이스.

청구항 19.

제11항에 있어서,

상기 제어 포인트로부터 상기 도메인에서 탈퇴를 요청받는 탈퇴 수신부; 및

상기 제어포인트 판단부에서 판단된 결과에 응답하여 상기 요청한 제어 포인트를 상기 도메인에서 탈퇴를 허용하는 탈퇴 허용부를 더 포함하는 것을 특징으로 하는 디바이스.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 UPnP(Universal Plug and Play)에 관한 것으로, 보다 상세하게는 UPnP 디바이스(Device)와 제어 포인트(Control Point)로 구성된 UPnP 네트워크에 관한 것이다.

현재, 윈도우(Windows)를 OS(Operating System)로 구동하는 PC(Personal Computer)는 플러그 앤 플레이(Plug and Play) 기능을 사용하여 주변 장치를 자동으로 인식할 수 있도록 하고 있다. 이에 따라, 사용자의 입장에서 주변 장치의 설치가 매우 용이해졌다. UPnP는 이러한 기능을 네트워크 전체에 확장시킨 기술로서 네트워크에 연결된 전자 제품(Electric Appliance)이 서로를 자동으로 인식할 수 있도록 하는 프로토콜(protocol)의 일종이다.

도 1a 및 도 1b는 UPnP 네트워크(120)를 설명하기 위한 개념도를 도시한 것이다.

UPnP 네트워크(120)는 제어 포인트(100) 및 디바이스(110)로 구성된다. 여기서, 디바이스(110)는 피제어 기기(Controlled Device)로서 소정의 서비스를 제공한다. 그리고 제어 포인트(100)는 디바이스(110)가 제공하는 서비스를 제어하여 사용자가 원하는 결과를 획득할 수 있게 한다.

먼저, 제어 포인드(100)가 서비스를 제어할 디바이스(110)를 검색하는 발견(130, Discovery)을 수행한다. 여기서, 발견(130)은 일반적으로 다음과 같은 두가지 방법으로 구현된다. 첫째, 제어 포인트(100)가 HTTP 프로토콜을 전송(Transport) 매개로 하여 M-SEARCH SSDP 메시지를 멀티캐스트(Multicast)하면, 디바이스(110)가 메시지를 수신하여 존재를 응답함으로써 디바이스(110)를 발견한다. 둘째, 디바이스(110)가 새롭게 UPnP 네트워크(120)에 참여하게 되면, HTTP 프로토콜을 전송 매개로 하여 NOTIFY SSDP 메시지를 멀티캐스트하면, 제어 포인트(100)는 메시지를 수신함으로로써 디바이스(110)를 발견한다.

발견(130)에서 제어 포인트(100)가 디바이스(110)를 발견한 후, 디바이스의 역할을 알리는 기기 설명과 서비스 설명을 전송하는 명세(140, Description)를 수행한다. 명세(140)에서 제어 포인트(100)는 HTTP GET Method에 의하여 발견(130)에서 얻을 수 있는 기기 접속 URI(Uniform Resource Identifier)를 통해 디바이스(100)의 역할을 설명하는 기기 설명이 기술된 XML 문서를 얻게 되며, XML 문서를 통해 디바이스(100)가 제공하는 제어 가능한 서비스 설명이 기술된 XML도 얻을 수 있다.

제어(150, Control)는 제어 포인트(100)가 서비스 설명을 획득함으로써 디바이스(110)의 제어를 수행한다. 제어(150)가 가능한 서비스는 작업(Action)이라는 형태로 제공되며, 서비스 설명은 다양한 작업들의 정의를 설명한다. 제어(150)에서 제어 포인트(100)는 서비스 설명을 기반으로 하여 작업을 호출할 수 있는 SOAP 메시지를 작성하여 HTTP를 전송 매개로 하여 디바이스(110)로 메시지를 전송한다. 이러한 전송된 메시지를 수신한 디바이스(110)는 작업에 부합되는 동작을 수행한 후 제어 포인트(100)에 작업의 호출 결과를 전송한다.

상태(160, Eventing)는 디바이스(110)에서 상태 변수가 변경될 때 제어 포인트(100)로 변경된 상태 변수의 값을 GENA 메시지로 구성하여 메시지로 알린다. 디바이스(110)는 사전에 메시지 수신을 등록한 제어 포인트(100)에만 전송한다.

이러한 종래의 UPnP 네트워크(120)의 시나리오에 의하면, 제어 포인트(100)가 디바이스(110)와 네트워크에 의하여 연결되고 발견(130)한 경우 제어 포인트(100)가 디바이스(110)를 제어할 권한이 있는지 여부에 관계없이 제어(150)할 수 있는 문제점을 갖는다. 그러나 점차 UPnP 네트워크가 스마트폰, PDA 등과 같은 이동성이 있고 네트워크 구성이 가능한 제품들로 이용되는 범위가 확대됨에 따라 디바이스와 네트워크에 의하여 연결된 제어 포인트 가운데 특정한 제어 포인트만이 디바이스를 제어할 수 있는 UPnP 네트워킹 시나리오가 요구되고 있다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는, 디바이스가 참가한 도메인에 이미 참가한 특정 제어 포인트에게만 제어를 선택적으로 허용하는 디바이스의 제어 허용 방법 및 그를 이용한 디바이스를 제공하는 것이다.

발명의 구성

상기의 과제를 이루기 위한 본 발명에 의한 디바이스의 제어 허용 방법은, 디바이스가 참가한 도메인에 제어 포인트가 이미 참가하였는지 여부를 판단하는 단계 및 상기 판단된 결과에 따라 상기 제어 포인트에게 상기 디바이스에 대한 제어를 선택적으로 허용하는 단계를 포함하는 것을 특징으로 한다.

상기된 발명을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체인 것을 특징으로 한다.

상기의 과제를 이루기 위한 본 발명에 의한 디바이스는, 디바이스가 참가한 도메인에 제어 포인트가 이미 참가하였는지 여부를 판단하는 판단부 및 상기 판단된 결과에 응답하여 상기 제어 포인트에게 상기 디바이스에 대한 제어를 선택적으로 허용하는 제어 허용부를 포함하는 것을 특징으로 한다.

이하, 첨부된 도면들을 참조하여 본 발명의 바람직한 실시예에 따른 디바이스의 제어 허용 방법 및 그를 이용한 디바이스에 대해 상세히 설명한다.

도 2는 본 발명의 바람직한 일 실시예에 따른 디바이스의 제어 허용 방법 및 그를 이용한 디바이스를 설명하기 위한 개념도를 도시한 것이다.

제1 내지 제6 디바이스(231 내지 236)는 제1 제어 포인트(211) 및 제2 제어 포인트(212)에 대하여 피제어 기기로서 소정의 서비스를 제공한다. 제1 및 제2 제어 포인트(211 및 212)는 제1 내지 제6 디바이스(231 내지 236)가 제공하는 서비스를 제어하여 사용자가 원하는 결과를 획득할 수 있게 한다.

여기서, 제1 내지 제6 디바이스(231 내지 236), 제1 및 제2 제어 포인트(211 및 212)는 동일한 네트워크에 연결되어 있지만, 제1 제어 포인트(211), 제1 내지 제3 및 제5 디바이스(231 내지 233 및 235)는 제1 도메인(201)에 참가되어 있으며, 제2 제어 포인트(212), 제2 내지 제5 디바이스(232 내지 235)는 제2 도메인(202)에 참가되어 있다.

본 실시예에 의한 디바이스의 제어 허용 방법 및 그를 이용한 디바이스에 의한 UPnP 네트워크 시나리오에 따르면, 디바이스와 네트워크에 의하여 연결된 제어 포인트 가운데 디바이스와 동일한 도메인에 참가된 제어 포인트만이 디바이스를 제어할 수 있도록 한다. 예를 들어, 제1 제어 포인트(211)는 제1 도메인(201)에 참가되어 있는 제1 내지 제3 및 제5 디바이스(231 내지 233 및 235)를 제어할 수 있지만, 제1 제어 포인트(211)가 제2 도메인(202)에는 참가되어 있지 않으므로 네트워크에 의하여 연결되어 있는 제4 및 제6 디바이스(234 및 236)를 제어할 수 없다. 또한, 제2 제어 포인트(212)도 제2 도메인(202)에 참가되어 있는 제2 내지 제5 디바이스(232 내지 235)를 제어 할 수 있지만, 제2 제어 포인트(212)가 제1 도메인(201)에 참가되어 있지 않으므로 제1 디바이스(231)를 제어할 수 없다.

도 3a는 본 발명에 의한 디바이스의 제어 허용 방법에서 참가(join)의 일 실시예를 흐름도로 도시한 것이다.

먼저, 제300단계에서 디바이스(110)는 제어 포인트(100)로부터 참가 메시지를 수신받는다. 도 3b에 도시된 [REQUEST] 메시지는 참가 메시지의 일 실시예를 도시한 것이다. 제300단계에서 참가 메시지는 소정의 도메인에 참가하기 위한 메시지로서 UPnP 네트워크를 구분하는 소정의 도메인을 나타내는 도메인 식별자(DOMAIN-ID, domain identifier)를 포함한다.

여기서, 도메인 식별자는 UPnP 프로토콜의 범위 밖에서 설정되고, 도메인 식별자에 대한 기밀성은 UPnP 프로토콜 범위 밖에서 유지되며, 도메인에 참가하는 모든 UPnP 디바이스는 동일한 식별자를 가지고 있다. 제어 포인트는 참가하고자 하는 UPnP 네트워크에 대한 도메인 식별자가 사전에 기 설정되어 있으며, 디바이스는 외부에서 사용자에 의해 도메인이 설정된다.

제300단계에서 수신받은 참가 메시지에서 디바이스(110)는 도메인 식별자를 추출할 수 있는지 여부를 판단한다(제310단계).

제310단계에서 도메인 식별자를 추출할 수 없다고 판단되면, 제300단계에서 수신받은 참가 메시지가 도메인 식별자에 대한 필드(field)를 가지고 있지 않는 경우로서 제어 포인트(100)는 도메인에 참가할 수 없으므로 디바이스(110)는 제300단계에서 수신된 참가 메시지에 응답하지 않음으로써 처리를 종료한다.

제310단계에서 도메인 식별자를 추출할 수 있다고 판단되면, 디바이스(110)는 제300단계에서 수신된 참가 메시지에 포함된 도메인 식별자를 추출한다(제320단계).

제320단계에서 추출된 도메인 식별자가 도메인 식별자의 목록에 기 등록되어 있는지 여부를 디바이스(110)는 판단한다(제330단계). 여기서, 도메인 식별자의 목록은 디바이스(110)가 이미 참가한 도메인의 식별자들이 저장된 리스트를 말한다.

제330단계에서 도메인 식별자의 목록에 등록되어 있지 않다고 판단되면, 제어 포인트(100)는 도메인에 참가할 수 없으므로 디바이스(110)는 제300단계에서 수신된 참가 메시지에 응답하지 않음으로써 처리를 종료한다. 왜냐하면, 제어 포인트(100)가 참가하고자 하는 도메인과 디바이스(110)가 참가한 도메인이 상이하기 때문이다.

제330단계에서 도메인 식별자의 목록에 등록되어 있다고 판단되면, 제어 포인트(100)는 도메인에 참가할 수 있으므로 디바이스(110)는 응답 메시지를 제어 포인트(100)로 전송한다(제340단계). 제340단계에서는 제어 포인트(100)가 참가하고자 하는 도메인과 디바이스(110)가 참가한 도메인이 동일하므로 디바이스(110)에 대한 제어를 제어 포인트(100)에 허용한다.

제340단계에서 디바이스(110)는 디바이스(110)를 제어할 수 있는 권한을 나타내는 제어 포인트 식별자(CP-ID, control point identifier)를 생성하고, 응답 메시지에 생성된 제어 포인트 식별자를 포함시켜 전송한다. 제340단계에서 생성된 제어 포인트 식별자는 제어가 허용된 제어 포인트의 리스트에 해당하는 제어 포인트 식별자의 목록에 등록하여 저장한다. 도 3b에 도시된 [RESPONSE] 메시지는 응답 메시지의 일 실시예를 도시한 것이다.

도 4a는 본 발명에 의한 디바이스의 제어 허용 방법에서 제어(control)의 일 실시예를 흐름도로 도시한 것이다.

먼저, 제400단계에서 디바이스(110)는 제어 포인트(100)로부터 제어 메시지를 통하여 액션(action)의 호출을 수신받는다. 여기서, 액션의 호출에 해당하는 SOAP 메시지는 HTTP 헤더(header)에 제어 포인트 식별자를 포함한다. 도 4b에 도시된 [REQUEST] 메시지는 제어 메시지의 일 실시예를 도시한 것이다.

제400단계에서 수신받은 제어 메시지에서 제어 포인트 식별자를 추출할 수 있는지 여부를 디바이스(110)는 판단한다(제410단계).

제410단계에서 제어 포인트 식별자를 추출할 수 없다고 판단되면, 제400단계에서 수신된 제어 메시지에 제어 포인트 식별자에 대한 필드를 가지고 있지 않는 경우로서 제340단계에서 디바이스(110)에 대한 제어가 허용되지 않은 제어 포인트(100)이므로 디바이스(110)는 제400단계에서 수신된 제어 메시지에 응답하지 않음으로써 처리를 종료한다.

제410단계에서 제어 포인트 식별자를 추출할 수 있다고 판단되면, 디바이스(110)는 제400단계에서 수신된 제어 메시지의 HTTP 헤더에서 제어 포인트 식별자를 추출한다(제420단계).

제420단계에서 추출된 제어 포인트 식별자가 제340단계에서 저장된 제어 포인트 식별자의 목록에 등록되어 있는지 여부를 디바이스(110)는 판단한다(제430단계).

제430단계에서 제어 포인트 식별자의 목록에 등록되어 있지 않다고 판단되면, 디바이스(110)는 제400단계에서 수신된 제어 메시지에 응답하지 않음으로써 처리를 종료한다. 이는 디바이스(110)가 참가한 도메인과 동일한 도메인에 제어 포인트(100)가 참가하여 제340단계에서 응답 메시지에 포함되어 전송받은 제어 포인트 식별자를 가지고 있지 않으므로 제어 포인트(100)가 디바이스(110)에 대한 제어가 허용되지 않았기 때문이다.

제430단계에서 제어 포인트 식별자의 목록에 등록되어 있다고 판단되면, 디바이스(110)는 제400단계에서 수신받은 제어 메시지를 처리하여 UPnP 규격 상의 액션을 수행한다(제440단계).

제440단계 후에, 디바이스(110)는 응답 메시지를 제어 포인트(100)로 전송한다(제450단계). 제450단계에서 응답 메시지는 제440단계에서 수행된 작업 결과 및 제어 포인트 식별자를 포함한다. 도 4b에 도시된 [RESPONSE] 메시지는 응답 메시지의 일 실시예를 도시한 것이다.

도 5a는 본 발명에 의한 디바이스의 제어 허용 방법에서 가입(subscribe)의 일 실시예를 흐름도로 도시한 것이다.

먼저, 디바이스(110)는 제어 포인트(100)로부터 가입 메시지를 수신받는다(제500단계). 제500단계에서 가입 메시지는 제어 포인트 식별자를 포함한다. 도 5b에 도시된 [REQUEST] 메시지는 가입 메시지의 일 실시예를 도시한 것이다.

제500단계에서 수신받은 가입 메시지에서 제어 포인트 식별자를 추출할 수 있는지 여부를 디바이스(110)는 판단한다(제510단계).

제510단계에서 제어 포인트 식별자를 추출할 수 없다고 판단되면, 제500단계에서 수신된 제어 메시지에서 제어 포인트 식별자에 대한 필드를 가지고 있지 않는 경우로서 디바이스(110)는 제500단계에서 수신된 가입 메시지에 응답하지 않음으로써 처리를 종료한다.

제510단계에서 제어 포인트 식별자를 추출할 수 있다고 판단되면, 디바이스(110)는 제500단계에서 수신된 가입 메시지에서 제어 포인트 식별자를 추출한다(제520단계).

제520단계에서 추출된 제어 포인트 식별자가 제340단계에서 저장된 제어 포인트 식별자의 목록에 등록되어 있는지 여부를 디바이스(110)는 판단한다(제530단계).

제530단계에서 제어 포인트 식별자의 목록에 등록되어 있지 않다고 판단되면, 디바이스(100)로부터 제어를 허용받은 제어 포인트(100)가 아니므로 디바이스(110)는 제500단계에서 수신된 가입 메시지에 응답하지 않음으로써 처리를 종료한다. 이는 디바이스(110)가 참가한 도메인과 동일한 도메인에 제어 포인트(100)가 참가하여 제340단계에서 응답 메시지에 포함되어 전송받은 제어 포인트 식별자를 가지고 있지 않으므로 제어 포인트(100)가 디바이스(110)에 대한 제어가 허용되지 않았기 때문이다.

제530단계에서 도메인 식별자의 목록에 등록되어 있다고 판단되면, 디바이스(110)는 디바이스(110)에 가입한 제어 포인트의 목록에 해당하는 가입 리스트에 제어 포인트(100)를 등록한다(제540단계).

제540단계 후에, 현재 디바이스(110)의 상태 변수값을 포함한 응답 메시지를 전송한다(제550단계). 제550단계에서 응답 메시지는 제어 포인트 식별자를 포함한다. 도 5b에 도시된 [RESPONSE] 메시지는 응답 메시지의 일 실시예를 도시한 것이다.

도 6a는 본 발명에 의한 디바이스의 제어 허용 방법에서 탈퇴(leave)의 일 실시예를 흐름도로 도시한 것이다.

먼저, 제600단계에서 디바이스(110)는 제어 포인트(100)로부터 탈퇴 메시지를 수신받는다. 제600단계에서 탈퇴 메시지는 제어 포인트(100)가 구성되었던 도메인에서 탈퇴를 표시하며, 제어 포인트 식별자를 포함한다. 도 6b에 도시된 [REQUEST] 메시지는 탈퇴 메시지의 일 실시예를 도시한 것이다.

제600단계에서 수신받은 탈퇴 메시지에서 제어 포인트 식별자를 추출할 수 있는지 여부를 디바이스(110)는 판단한다(제610단계).

제610단계에서 제어 포인트 식별자를 추출할 수 없다고 판단되면, 제600단계에서 수신받은 탈퇴 메시지에 제어 포인트 식별자에 대한 필드를 가지고 있지 않는 경우로서 도메인에 참가하여 디바이스(110)는 제600단계에서 수신된 탈퇴 메시지에 응답하지 않음으로써 처리를 종료한다.

제610단계에서 제어 포인트 식별자를 추출할 수 있다고 판단되면, 디바이스(110)는 제600단계에서 수신된 탈퇴 메시지에 포함된 제어 포인트 식별자를 추출한다(제620단계).

제620단계에서 추출된 제어 포인트 식별자가 제340단계에서 저장된 제어 포인트 식별자의 목록에 등록되어 있는지 여부를 디바이스(110)는 판단한다(제630단계).

제630단계에서 제어 포인트 식별자의 목록에 등록되어 있지 않다고 판단되면, 디바이스(110)는 제600단계에서 수신된 탈퇴 메시지에 응답하지 않음으로써 처리를 종료한다. 이는 제어 포인트(100)가 디바이스(110)가 참가한 도메인과 동일한 도메인에 참가하지 않았으므로 디바이스(110)로부터 생성된 제어 포인트 식별자를 전송받지 못했기 때문이다.

제630단계에서 도메인 식별자의 목록에 등록되어 있다고 판단되면, 디바이스(110)는 제340단계에서 저장된 제어 포인트 식별자의 목록에서 해당하는 제어 포인트 식별자를 삭제한다(제640단계).

제640단계 후에, 디바이스(110)는 응답 메시지를 제어 포인트(100)로 전송한다(제650단계). 제650단계에서 응답 메시지는 도메인 식별자를 포함한다. 도 6b에 도시된 [RESPONSE] 메시지는 응답 메시지의 일 실시예를 도시한 것이다.

도 7은 본 발명에 의한 디바이스의 일 실시예를 블럭도로 도시한 것이다.

메시지 수신부(700)는 제어 포인트(100)로부터 송신된 참가 메시지, 제어 메시지, 가입 메시지 및 탈퇴 메시지를 수신받는다.

식별자 추출부(710)는 메시지 수신부(700)에서 수신받은 메시지에서 도메인 식별자 또는 제어 포인트 식별자를 추출한다. 여기서, 식별자 추출부(710)는 메시지 수신부(700)에서 참가 메시지를 수신받은 경우 도메인 식별자를 추출하고, 제어 메시지, 가입 메시지 및 탈퇴 메시지를 수신받은 경우 제어 포인트 식별자를 추출한다.

판단부(720)는 식별자 추출부(710)에서 도메인 식별자 또는 제어 포인트 식별자를 추출할 수 있는지 여부를 판단하고, 만일 추출할 수 있다면 식별자 추출부(710)에서 추출된 도메인 식별자 또는 제어 포인트 식별자가 등록목록 저장부(730)에 저장된 도메인 식별자 또는 제어 포인트 식별자와 동일한 것이 있는지 여부를 판단한다.

여기서, 판단부(720)는 식별자 추출부(710)에서 도메인 식별자 또는 제어 포인트 식별자를 추출할 수 있는지 여부는 식별자 추출부(710)에서 추출하려는 도메인 식별자 또는 제어 포인트 식별자에 대한 필드가 메시지 수신부(700)에서 수신된 메시지에 있는지 여부를 기준으로 하여 판단한다. 만일 판단부(720)에서 도메인 식별자 또는 제어 포인트 식별자를 추출할 수 없다면, 메시지 수신부(700)에서 수신된 메시지에 응답하지 않음으로써 처리를 종료한다.

등록목록 저장부(730)는 디바이스(110)가 참가한 도메인의 식별자에 대한 목록을 저장하고, 참가부(740)에서 참가가 허용된 제어 포인트에 대하여 식별자 생성부(750)에서 생성된 제어 포인트 식별자의 목록을 저장하며, 가입부(760)에서 가입이 허용된 제어 포인트에 대한 가입 리스트를 저장한다.

참가부(740)는 식별자 추출부(710)에서 참가 메시지로부터 추출한 도메인 식별자가 등록목록 저장부(730)의 제어 포인트 식별자의 목록에 저장되어 있다고 판단되면, 제어 포인트(100)를 도메인에 참가를 허용한다.

식별자 생성부(745)는 참가부(740)에서 도메인에 참가가 허용된 제어 포인트(100)에 대하여 디바이스(110)를 제어할 수 있는 권한을 나타내는 제어 포인트 식별자를 생성한다. 또한, 식별자 생성부(745)는 생성된 제어 포인트 식별자를 등록목록 저장부(730)에 기입한다.

제어부(750)는 식별자 추출부(710)에서 제어 메시지로부터 추출한 제어 포인트 식별자가 등록목록 저장부(730)에 저장되어 있다고 판단되면, 메시지 수신부(700)에서 수신된 제어 메시지에 의하여 호출된 액션을 수행한다.

가입부(760)는 식별자 추출부(710)에서 가입 메시지로부터 추출한 제어 포인트 식별자가 등록목록 저장부(730)에 저장되어 있다고 판단되면, 등록목록 저장부(730)에 저장된 가입 리스트에 제어 포인트의 식별자를 기입하고 제어 포인트(100)에 송신할 디바이스(110)의 상태 변수값을 생성한다.

탈퇴부(760)는 식별자 추출부(710)에서 탈퇴 메시지로부터 추출한 제어 포인트 식별자가 등록목록 저장부(730)의 제어 포인트 식별자의 목록에 저장되어 있다고 판단되면, 등록목록 저장부(730)에 저장된 제어 포인트 식별자의 목록에서 해당하는 제어 포인트 식별자를 삭제한다.

메시지 송신부(780)는 메시지 수신부(700)에서 수신받은 메시지에 대한 응답 메시지를 제어 포인트(100)에 송신한다. 여기서, 메시지 송신부(780)는 참가부(740)에서 생성된 제어 포인트 식별자를 참가 메시지에 대한 응답 메시지에 포함하여 송신한다. 또한, 메시지 송신부(780)는 제어 메시지, 가입 메시지 또는 탈퇴 메시지에 대한 응답메시지에 제어 포인트 식별자를 포함하여 송신한다.

본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드 디스크, 플로피 디스크, 광데이터 저장 장치 등이 있다.

이러한 본원발명의 이해를 돕기 위하여 도면에 도시된 실시예를 참고로 설명되었으나, 이는 예시적인 것에 불과하며, 당해 분야에서 통상적 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위에 의해 정해져야 할 것이다.

발명의 효과

본 발명에 의한 디바이스의 제어 허용 방법 및 그를 이용한 디바이스에 의하면, 디바이스가 참가한 도메인에 이미 참가한 특정 제어 포인트에게만 제어를 선택적으로 허용함으로써 디바이스가 특정한 제어 포인트에게만 제어받을 수 있다. 이에 의하여 동일한 네트워크에 연결된 제어 포인트이더라도 도메인에 참가하지 않으면 디바이스를 제어할 수 없도록 하는 효과를 거둘 수 있다.

도면의 간단한 설명

도 1a 및 1b는 UPnP 네트워크(120)를 설명하기 위한 개념도를 도시한 것이다.

도 2는 본 발명에 의한 디바이스의 제어 허용 방법 및 그를 이용한 디바이스를 설명하기 위한 개념도를 도시한 것이다.

도 3a는 본 발명에 의한 디바이스의 제어 허용 방법에서 참가(join)의 일 실시예를 흐름도로 도시한 것이다.

도 3b는 본 발명에 의한 디바이스의 제어 허용 방법에서의 참가 메시지의 일 실시예이다.

도 4a는 본 발명에 의한 디바이스의 제어 허용 방법에서 제어(control)의 일 실시예를 흐름도로 도시한 것이다.

도 4b는 본 발명에 의한 디바이스의 제어 허용 방법에서의 제어 메시지의 일 실시예이다.

도 5a는 본 발명에 의한 디바이스의 제어 허용 방법에서 가입(subscribe)의 일 실시예를 흐름도로 도시한 것이다.

도 5b는 본 발명에 의한 디바이스의 제어 허용 방법에서의 가입 메시지의 일 실시예이다.

도 6a는 본 발명에 의한 디바이스의 제어 허용 방법에서 탈퇴(leave)의 일 실시예를 흐름도로 도시한 것이다.

도 6b는 본 발명에 의한 디바이스의 제어 허용 방법에서의 탈퇴 메시지의 일 실시예이다.

도 7은 본 발명에 의한 디바이스의 일 실시예를 블록도로 도시한 것이다.

〈도면의 주요 부호에 대한 간단한 설명〉

700: 메시지 수신부 710: 식별자 추출부

720: 판단부 730: 등록목록 저장부

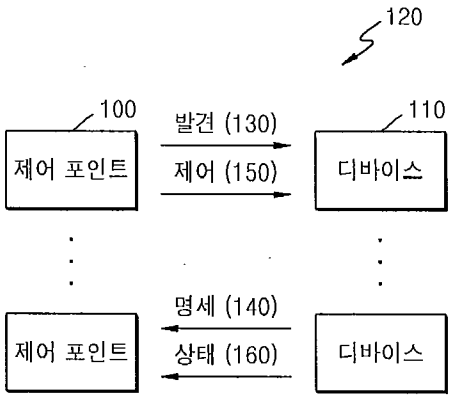
740: 참가부 745: 식별자 생성부

750: 제어부 760: 가입부

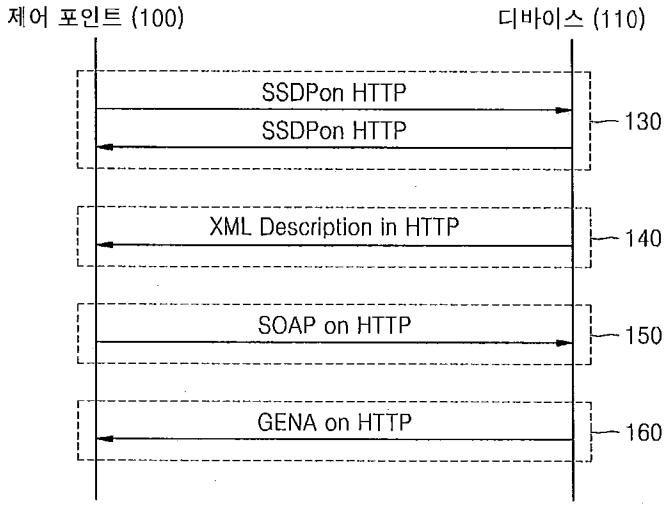
770: 탈퇴부 780: 메시지 송신부

도면

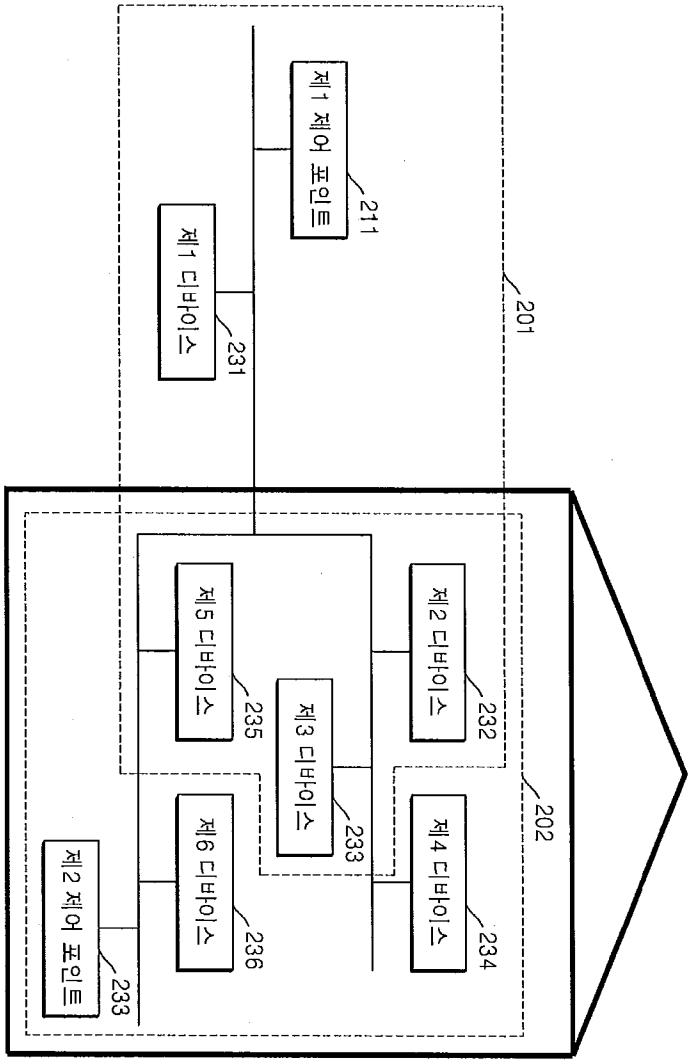
도면1a



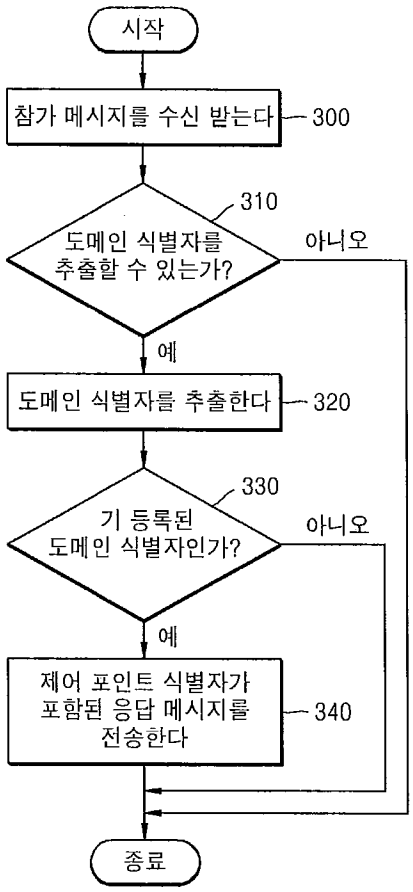
도면1b



도면2


제1 제어 포인트
211
제1 디바이스
231
201
제2 디바이스
232
제5 디바이스
235
제3 디바이스
233
제4 디바이스
234
제6 디바이스
236
202
제2 제어 포인트
233

도면3a



도면3b

[REQUEST]

JOIN *path domain URL* HTTP/1.1

HOST: hostname:portNumber

USER-AGENT: *OS/version* UPnP/1.1 *product/version*

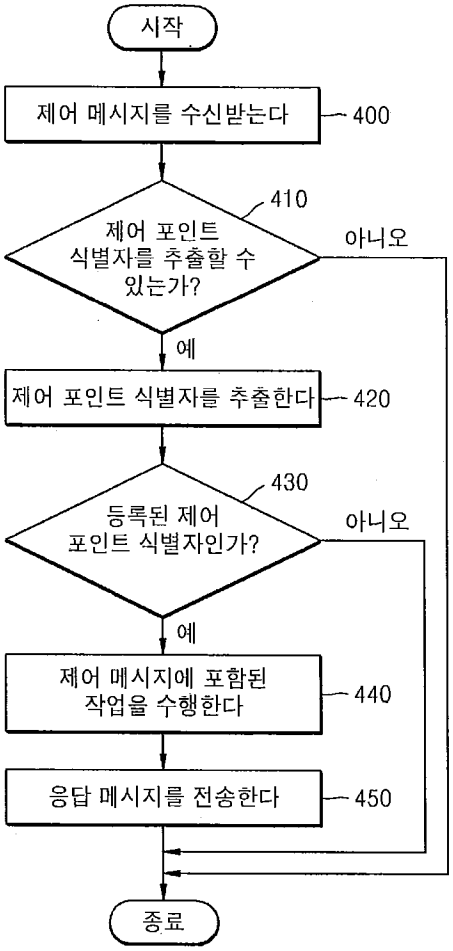
DOMAIN-ID: domain *identifier*

[RESPONSE]

HTTP/1.1 200 OK

CP-ID: *control point identifier*

도면4a


시작
제어 메시지를 수신받는다
400
410
제어 포인트 식별자를 추출할 수 있는가?
아니오
예
제어 포인트 식별자를 추출한다
420
430
등록된 제어 포인트 식별자인가?
아니오
예
제어 메시지에 포함된 작업을 수행한다
440
응답 메시지를 전송한다
450
종료

도면4b

[REQUEST]

POST *path control* URL **HTTP/1.0**

HOST: hostname:portNumber

CONTENT-LENGTH: *bytes in body*

CONTENT-TYPE: text/xml; charset="utf-8"

USER-AGNET: *OS/version* UPnP/1.1 *product/version*

CP-ID: *control point identifier*

SOAPACTION: "urn:schemas-upnp-org:service:*serviceType*:*v#actionName*"

POST *path control* URL **HTTP/1.1**

HOST: hostname:portNumber

Transfer-Encoding: "chunked"

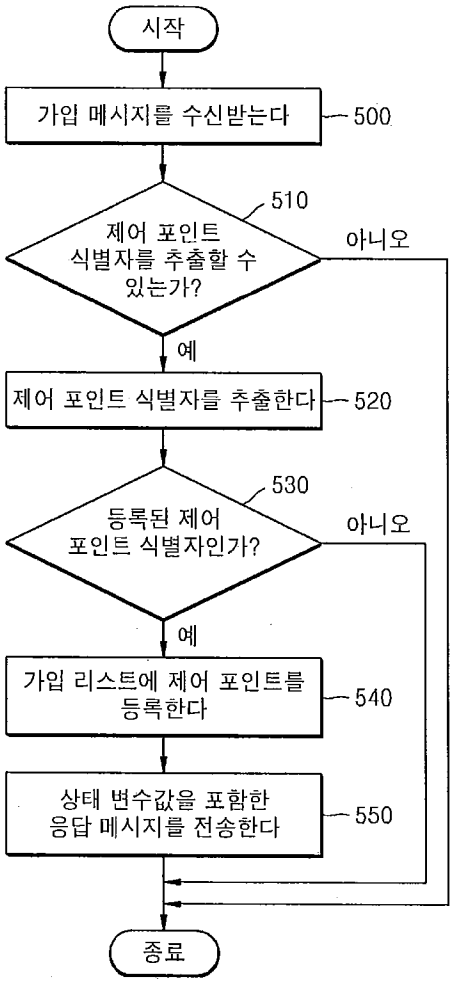
CONTENT-TYPE: text/xml; charset="utf-8"

USER-AGNET: *OS/version* UPnP/1.1 *product/version*

CP-ID: *control point identifier*

SOAPACTION: "urn:schemas-upnp-org:service:*serviceType*:*v#actionName*"

도면5a



도면5b

SUBSCRIBE *publisher path* HTTP/1.1

HOST: *publisher host:publisher port*

USER-AGENT: *OS/version UPnP/1.1 product/version*

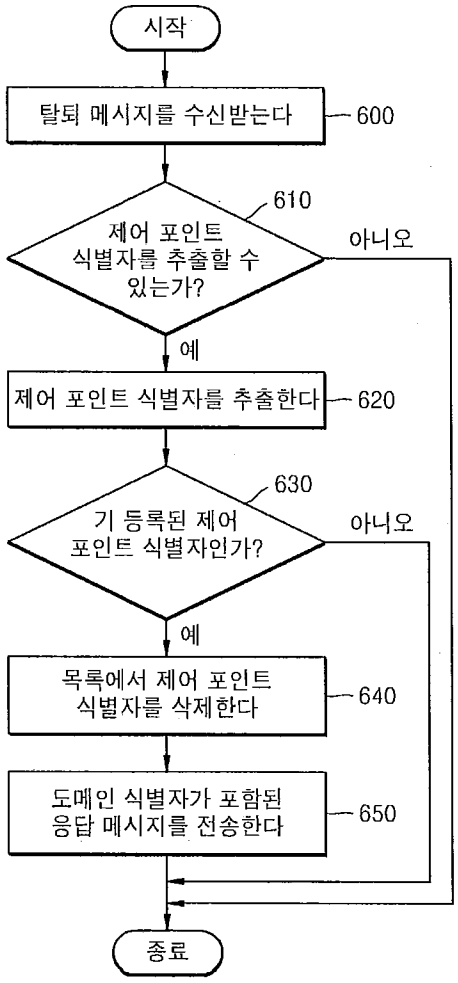
CALLBACK: <*delivery URL*>

NT: upnp:event

TIMEOUT: *Send-requested subscription duration*

CP-ID: *control point identifier*

도면6a



도면6b

[REQUEST]

LEAVE *path domain URL* HTTP/1.1

HOST: hostname:portNumber

USER-AGENT: *OS/version* UPnP/1.1 *product/version*

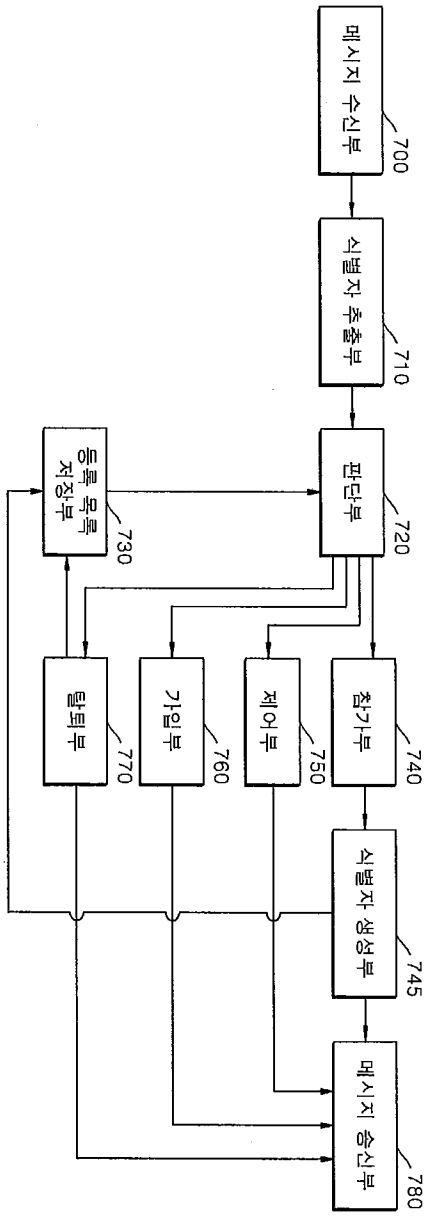
CP-ID: *control point identifier*

[RESPONSE]

HTTP/1.1 200 OK

DOMAIN-ID: *domain identifier*

도면7


메시지 수신부
700
식별자 추출부
710
판단부
720
등록 목록 저장부
730
탈퇴부
770
가입부
760
제어부
750
참가부
740
식별자 생성부
745
메시지 송신부
780

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11) Publication number: 1020050060685 A

(43) Publication date: 22.06.2005

(21) Application number: 1020030092385

(22) Application date: 17.12.2003

(71) Applicant:
- SK TELECOM CO., LTD.

(72) Inventor:
- YANG, JIN WOOK
- YOON, SONG YEE

(51) Int. Cl: H04Q 7/24

(54) METHOD FOR CHECKING TYPE INFORMATION OF A USER TERMINAL, AND ITS SYSTEM, CAPABLE OF CONSTRUCTING AND OFFERING SERVICES APPROPRIATED FOR A DEVICE, A LOCATION, AN AGE OR AN INCLINATION ON A BASIS OF USER INFORMATION COLLECTIVELY MANAGED BY A SERVER WHEN A USER USES A DEVICE WHERE A CORRESPONDING TERMINAL SUCH AS A HANDSET, A ROBOT, A VEHICLE OR A PERSONAL COMPUTER IS MOUNTED BY UTILIZING A TERMINAL CONNECTED TO THE SERVER VIA A NETWORK

(57) Abstract:

PURPOSE: A method for checking type information of a user terminal, and its system are provided to analyze a life pattern according to a user life style, and to offer personally optimized life solutions to various kinds of terminals via user friendly character interfaces when the user uses a device where a terminal like a handset, a robot, a vehicle or a personal computer, connected to a server via a network is mounted.

CONSTITUTION: A system for checking type information of a user terminal comprises a network(50), a device, a personal information management database server(60) and a service content management database server(70). The device, connected to the network(50), can be a handset(10), a robot(20), a

vehicle(30), or a personal computer(40) which has a corresponding agent(10a,20a,30a,40a). The personal information management database server(60), linked with the device, stores personal information on a location, an age or an inclination collected by each agent and offers the personal information. The service content management database server(70), linked with the personal information management database server(60), offers service content, appropriate for each user on a basis of the personal information, to the user via the agent.

Legal Status

Date of request for an examination (20081217)

Notification date of refusal decision (00000000)

Final disposal of an application (registration)

Date of final disposal of an application (20101223)

Patent registration number (1010066730000)

Date of registration (20101230)

Number of opposition against the grant of a patent ( )

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ( )

Date of requesting trial against decision to refuse ( )

Date of extinction of right ( )

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년01월10일
(11) 등록번호 10-1006673
(24) 등록일자 2010년12월30일

(51) Int. Cl.
H04W 8/18 (2009.01) *G06Q 50/00* (2006.01)
(21) 출원번호 10-2003-0092385
(22) 출원일자 2003년12월17일
심사청구일자 2008년12월17일
(65) 공개번호 10-2005-0060685
(43) 공개일자 2005년06월22일
(56) 선행기술조사문헌
KR1020030006717 A*
KR1020030069308 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에스케이 텔레콤주식회사
서울 중구 을지로2가 11번지
(72) 발명자
양진욱
서울특별시서대문구홍제1동홍제아파트1동103호
윤송이
서울특별시서초구반포4동대림빌라A동104호
(74) 대리인
김창달, 특허법인화우

전체 청구항 수 : 총 13 항 심사관 : 문성돈

(54) 사용자의 단말 형태정보 파악방법 및 그 시스템

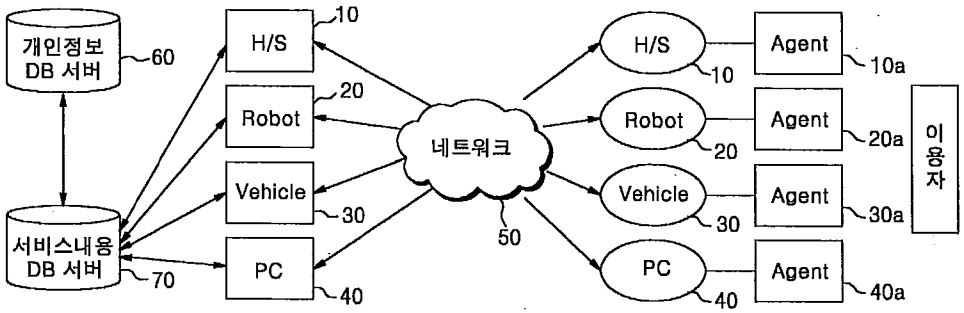
(57) 요 약

본 발명은 사용자의 단말 형태정보 파악방법 및 그 시스템에 관한 것으로서, 고객의 라이프 스타일에 따른 생활 패턴을 분석하여 개인에게 최적화된 라이프 솔루션(Life solution)을 고객에게 친근한 캐릭터 인터페이스(I/F)를 통하여 각종 단말로 서비스를 제공하는 기술에 관한 것이다.

본 발명에 의하면, 네트워크와; 상기 네트워크와 연결되며, 해당 에이전트(agent)가 장착된 소정의 디바이스(Device); 상기 디바이스와 연동되며, 해당 에이전트를 통해 수집된 개인 정보에 대한 데이터베이스를 구축하여 제공하는 개인정보 DB서버; 및 상기 개인정보 DB서버와 연동되어 개인 정보를 바탕으로 각 개인에 적합한 컨텐츠별 서비스 내용을 해당 에이전트를 통해 제공하는 서비스내용 DB서버를 포함하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템을 제시한다.

따라서, 기존의 모바일 인터넷 브라우저 상의 서비스 형태별로 수직 분할된 각 CP의 컨텐츠를 CI 서비스를 통하여 수평 집약적 구조로 형성함으로써 개인에게 최적화된 형태로 서비스를 제공할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

네트워크와;

상기 네트워크와 연결되며, 해당 에이전트(agent)가 장착된 디바이스(Device)로서 핸드셋(H/S), 로봇(Robot) 및 차량(Vehicle) 중 적어도 2개 이상을 포함하는 복수의 서로 다른 디바이스들;

상기 디바이스와 연동되며, 상기 해당 에이전트를 통해 수집된 개인 정보에 대한 데이터베이스를 구축하여 제공하는 개인정보DB서버; 및

상기 개인정보 DB서버와 연동되어 개인 정보를 바탕으로 각 개인에 대한 컨텐츠별 서비스 내용을 상기 해당 에이전트를 통해 제공하는 서비스내용 DB서버를 포함하고,

상기 해당 에이전트를 통해 수집하는 개인정보는 호 이력(call history), 단문메시지(SMS) 및 CI 어플리케이션에 관한 정보인 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 2

청구항 1에 있어서, 상기 디바이스로서 컴퓨터(PC)를 더 포함하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 3

청구항 2에 있어서, 상기 디바이스들 중 핸드셋(H/S), 로봇(Robot), 차량(Vehicle)에 해당되는 에이전트는 무선 LAN 또는 CDMA를 이용하여 접속하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 4

청구항 1에 있어서, 상기 개인정보 DB서버에는 개인의 연령, 취향, 위치에 대한 정보데이터가 구비되는 것을 특징으로하는 사용자의 단말 형태정보 파악 시스템.

청구항 5

지능형 통신단말시스템(CITS)을 이용한 사용자의 단말 형태정보 파악 시스템에 있어서,

지능형 통신(CI) 서비스를 구현하기 위한 고객 사용 패턴을 수집하는 Mobile 플랫폼과;

고객 사용 패턴을 수집함과 더불어 대기모드를 장악해서 고객에게 단말의 개별 서비스를 접근할 수 있는 사용자 인터페이스(UI) 및 접근 경로를 제공하는 CI 어플리케이션;

상기 Mobile 플랫폼과 CI 어플리케이션로부터 수집된 정보를 바탕으로 CI 서비스가 가능하도록 고객의 성향 분석을 위한 센싱(Sensing), 대기모드의 배달 및 실행, 어플리케이션 간의 연계 기능을 하는 CI 매니저; 및

상기 CI 매니저로부터 전송되는 고객의 성향 데이터를 분석하여 고객에게 풀/푸시(Pull/Push) 형으로 서비스를 제공하는 CI Server 플랫폼을 포함하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 6

청구항 5에 있어서, 상기 CI 어플리케이션에서는 개별 어플리케이션을 통째로 호출하는 방식 혹은 어플리케이션, 라이브러리(Library) 형태의 모듈로 호출하는 방식을 이용하여 사용자 인터페이스(UI) 및 접근 경로를 제공하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 7

청구항 5에 있어서, 상기 CI 서비스에서의 센싱(Sensing) 대상에는 Call 발/착신, SMS 발/착신, MMS 발/착신, 단말 Power ON/OFF, Morning Call Alarm, 및 기지국 정보가 포함되는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 8

청구항 5 또는 청구항 7에 있어서, 상기 CI 서비스에서의 센싱(Sensing) 접근방식은 센싱 대상의 히스토리(History)을 단말에 로그(Log)를 남기는 히스토리 로깅(History Logging) 방식과, 단말에 남긴 로그(Log)를 서버로 전송하는 로그 전송(Log Transfer) 방식을 이용하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 9

청구항 8에 있어서, 상기 히스토리 로깅(History Logging) 방식에는 고객의 위치에 대한 로깅을 일정 시간 간격으로 현재 상태를 남기는 시간주기(Time Period) 방식과, 특정한 사건이 있을 때마다 그 시점을 기록하는 방식으로서 사건구동(Event Driven) 방식이 더 포함되는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 10

청구항 8에 있어서, 상기 로그 전송(Log Transfer) 방식에는

서버가 SMS Push를 사용하여 히스토리(History)를 요청할 때 마다 전송하는 서버요청 시점마다 전송하는 방식과;

미리 설정된 시간 간격 마다 축적된 단말 로그(Log)를 서버로 전송하는 일정시간마다 전송하는 방식; 및

특정 사건(위치의 변화, Call History 발생, SMS History 발생) 발생시 마다 서버로 전송하는 방식이 더 포함되는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 11

청구항 5에 있어서, 상기 CI 서비스에서 위치 감지(Location Sensing)를 위한 위치(Location) 정보는 핸드셋(Handset)이 무선통신을 하기 위한 자신의 위치 정보를 활용하며, 기지국 ID 및 GPS 단말일 경우 GPS ID가 위치정보가 되는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 12

청구항 11에 있어서, 상기 위치 감지에 대한 로깅(Logging) 및 로그 전송(Log Transfer)은 특정 지역에 도달했거나 셀(Cell)이 변경 될 때마다 전송하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템.

청구항 13

지능형 통신단말시스템(CITS)을 이용한 사용자 단말 형태정보 파악 방법에 있어서,

핸드셋(H/S), 로봇(Robot) 및 차량(Vehicle) 중 적어도 2개 이상을 포함하는 복수의 서로 다른 디바이스들로부터 호 이력(call history), 단문메시지(SMS) 및 CI 어플리케이션에 관한 정보를 수집하는 제 1단계와,

상기 수집된 정보들로부터 사용자의 생활 패턴을 분석하여 사용자별 생활 패턴 데이터베이스를 구축하는 제 2단계와,

상기 사용자별 생활 패턴 정보에 의거해서 개인화된 서비스를 상기 디바이스에 배달하는 제 3단계와,

상기 디바이스에서 개인화 서비스를 구동하는 제 4단계를 포함하고,

상기 개인화 서비스의 구동은 상기 복수개의 디바이스 중 어느 디바이스에서도 가능한 것을 특징으로 사용자 단말 형태정보 파악 방법.

청구항 14

삭제

청구항 15

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0006] 본 발명은 사용자의 단말 형태정보 파악방법 및 그 시스템에 관한 것이다.보다 상세하게는 고객의 라이프 스타일에 따른 생활 패턴을 분석하여 개인에게 최적화된 라이프 솔루션(Life solution)을 고객에게 친근한 캐릭터 인터페이스(I/F)를 통하여 각종 단말로 서비스를 제공하는 기술에 관한 것이다.

[0007] 최근 모바일 인터넷을 통하여 사용자의 욕구를 충족시킬 수 있는 다양한 컨텐츠, 즉 멀티미디어 컨텐츠(Multimedia contents), 위치서비스 컨텐츠(Location service contents), 상업서비스 컨텐츠(Commerce service contents) 등이 컨텐츠 제공자(CP)에 의해 제작되어 인터넷 사용자들에게 제공되고 있다.

[0008] 그러나, 이러한 서비스 제공방법은 고객의 취향에 따른 서비스 형태별로 서로 다른 사용자 인터페이스(UI) 및 컨텐츠 접근방식이 요구되었다. 즉, 종래의 서비스 제공방식은 고객이 자신이 필요한 정보 또는 컨텐츠 서비스를 모바일 인터넷 상에서 일일이 헤매면서 찾아야 하는 번거로움이 있었다.

[0009] 따라서, 기존의 모바일 인터넷 브라우저 상의 서비스 형태별로 수직 분할된 각종 컨텐츠 및 어플리케이션을 수평 집약적 구조로 형성하여 고객에게 최적화된 서비스 형태로 제공할 필요성이 제기되었다.

발명이 이루고자 하는 기술적 과제

[0010] 본 발명은 상기한 문제점을 해결하기 위한 것으로서 본 발명은 네트워크를 이용하여 서버에 연결된 단말을 활용하여 사용자가 핸드셋(H/S), 로봇(Robot), 차량, PC등 해당 단말이 장착된 장치를 이용할 때 서버에서 일괄 관리되는 사용자에 대한 정보를 바탕으로 디바이스, 위치, 연령, 취향에 적절한 서비스를 구성하여 제공할 수 있도록 하는데 그 목적이 있다.

[0011] 상기한 본 발명의 목적을 달성하기 위한 기술적 사상으로서 본 발명은

[0012] 지능형 통신단말시스템(CITS)을 이용한 사용자의 단말 형태정보 파악 시스템에 있어서,

[0013] 지능형 통신(CI) 서비스를 구현하기 위한 고객 사용 패턴을 수집하는 Mobile 플랫폼과;

[0014] 고객 사용 패턴을 수집함과 더불어 대기모드를 장악해서 고객에게 단말의 개별 서비스를 접근할 수 있는 사용자 인터페이스(UI) 및 접근 경로를 제공하는 CI 어플리케이션;

[0015] 상기 Mobile 플랫폼과 CI 어플리케이션으로부터 수집된 정보를 바탕으로 CI 서비스가 가능하도록 고객의 성향 분석을 위한 센싱(Sensing), 대기모드의 배달 및 실행, 어플리케이션 간의 연계 기능을 하는 CI 매니저; 및

[0016] 상기 CI 매니저로부터 전송되는 고객의 성향 데이터를 분석하여 고객에게 풀/푸시(Pull/Push) 형으로 서비스를 제공하는 CI Server 플랫폼을 포함하는 것을 특징으로 하는 사용자의 단말 형태정보 파악 시스템을 제공한다.

발명의 구성 및 작용

[0017] 이하, 본 발명의 실시 예에 대한 구성 및 그 작용을 첨부한 도면을 참조하면서 상세히 설명하기로 한다.

[0018] 도 1은 본 발명에 따른 사용자의 단말 형태정보 서비스 제공을 위한 개념도이다. 도 2는 본 발명에 적용된 지능형 통신단말시스템(CITS)을 이용한 사용자 단말 형태정보 시스템의 구성도이다.

[0019] 본 발명의 설명에 앞서, CITS(Communication intelligence Terminal System)란 고객의 행동 패턴(Pattern) 정보를 서버로 전송해 주며, 고객에게 필요한 개인화된 서비스를 고객 친화적 방식으로 제공하는 서비스를 말한다.

[0020] 도 1에 도시된 바와 같이, 본 발명에 적용된 서비스 개념을 살펴보면 유무선 통신망으로 구축되는 네트워크(50)와; 상기 네트워크(50)와 연결되며, 해당 에이전트(agent)(10a,20a,30a,40a)가 장착된 핸드셋(H/S)(10), 로봇(Robot)(20), 차량(Vehicle)(30), 컴퓨터(PC)(40)를 구비하는 디바이스(Device); 상기 디바이스와 연동되며, 해당 에이전트를 통해 수집된 위치, 연령, 취향 등에 대한 개인 정보 데이터베이스를 구축하여 제공하는 개인정

보 DB서버(60); 및 상기 개인정보 DB서버(60)와 연동되어 개인 정보를 바탕으로 각 개인에 적합한 컨텐츠별 서비스 내용을 해당 에이전트를 통해 제공하는 서비스내용 DB서버(70)로 구성된다.

[0021] 이 때, 상기 디바이스에서 컴퓨터(PC)를 제외한 핸드셋(H/S), 로봇(Robot), 차량(Vehicle)에 해당되는 에이전트는 무선 LAN 또는 CDMA를 이용하여 접속하게 된다.

[0022] 상기와 같이 구성되는 본 발명의 서비스는 개인정보 DB서버(60)와 서비스내용 DB서버(60)를 활용하여 개인 정보의 수집 및 단말별 서비스를 제공하고, 이를 해당되는 각 에이전트를 통해 각 개인에 적합한 컨텐츠별 서비스를 제공하게 된다.

[0023] 또한, 본 발명에 적용된 지능형 통신단말시스템(CITS)은 도 2에 도시된 바와 같이 모바일 플랫폼(Mobile Platform)(110)과, CI 매니저(CI Manager)(120), CI 어플리케이션(CI Application)(130), 및 CI 서버 플랫폼(CI Server Platform)으로 구성된다.

[0024] 각 구성 요소를 좀 더 상세히 살펴보면, 상기 Mobile 플랫폼(110)은 CI(Communication intelligence) 서비스가 구현될 단말의 플랫폼(Platform) 및 하드웨어(H/W)를 나타낸다.

[0025] 상기 CI 매니저(CIM)(120)는 CI 서비스가 가능하도록 공통분모의 코어(core) 기능들을 가지고 있는 모바일 어플리케이션(Mobile Application)으로 고객의 성향분석을 위한 센싱(Sensing) 기능을 한다.

[0026] 또한, 대기모드 어플리케이션(Application)의 D/L 및 실행, CI 어플리케이션간, 기타 어플리케이션간, OEM 기능간의 연계 기능을 갖는다.

[0027] 상기 CI 어플리케이션(130)은 대기모드에 상주할 수 있는 어플리케이션으로 고객과 직접적인 인터페이스(I/F)를 수행하는 기능을 한다.

[0028] 이 때, 상기 CI 어플리케이션(130)은 상주형 어플리케이션과 비상주형 어플리케이션으로 구분할 수 있으며, 상주형 어플리케이션은 대기모드 장악 할 수 있는 기능이 있고, 비상주형 어플리케이션은 일반 어플리케이션과 같이 대기모드 장악이 불가능 하다.

[0029] 상기 CI Server 플랫폼(CISP)(140)은 CITS가 전해주는 고객의 성향을 분석하여 고객에게 풀/푸시(Pull/Push) 형으로 서비스를 제공하는 서버 군 역할을 한다.

[0030] 도 3은 본 발명에 적용된 지능형 통신단말시스템(CITS)을 이용한 사용자 단말 형태정보 제공과정을 나타낸 흐름도이다.

[0031] 도 3을 살펴보면, 고객 사용 패턴을 수집하는 제 1단계(S110)와; 상기 고객 사용 패턴을 전달하는 제 2단계(S120); 개인화된 서비스를 배달하는 제 3단계(S130); 개인화 서비스를 구동하는 제 4단계(S140); 및 개인화 서비스를 고객 친화적 방식으로 제공하는 제 5단계(S150)로 이루어진다.

[0032] 이 때, 상기 제 1단계에서의 고객사용 패턴 수집 정보에는 호 히스토리(Call history), 단문메시지(SMS), CI 어플리케이션에 대한 정보가 포함되며, 상기 제 3단계에서는 감지(Sensing), 판단(Decision), 행위(Behavior)를 바탕으로 개인화된 서비스를 배달한다.

[0033] 상기와 같이 구성된 CITS 구성간의 서비스 과정을 좀 더 구체적으로 살펴보면 다음과 같다.

[0034] 먼저, CISP(140)는 미리 사용자 패턴(Pattern)을 분석하기 위한 사용/위치 히스토리(Usage/Location History)를 어떤 주기로 저장 및 전송할 지 CITS(140)에 설정 한다.

[0035] 그러면, 사용자(User)가 CITS를 사용하게 된다. 이 때, 그에 따른 단말 히스토리(History)가 폰(Phone)에 남게 된다.

[0036] 상기 설정된 주기별로 CIM(120)은 서버로 Usage/Location History를 CISP(140)로 전송한다.

[0037] 이 때, 상기 CISP(140)는 감지/판단(Sensing/Decision) 과정을 거쳐 사용자(User)에게 어떤 정보를 배달할 지 결정한다.

[0038] 그 후, CITS를 통해 풀/푸시(Pull/Push) 방식으로 고객에게 개인화된 서비스가 제공이 된다. 이러한 서비스 제공은 CI 어플리케이션, 기타 어플리케이션, OEM 어플리케이션이 협업하여 제공된다.

[0039] 도 4는 도 2에 도시된 CI 어플리케이션의 상세 구성도이다.

[0040] 본 발명에 적용된 CITS에서 CI 어플리케이션은 고객과의 직접 대면하여, 모든 단말 기능으로 이어지는 일종의 Mobile 서비스 게이트웨이(Gateway)로서 위치한다.

[0041] 이를 설명하기 전에 도 4를 참조하여 우선 CI 서비스에 적용된 어플리케이션(Application)의 종류를 살펴보기로 한다.

[0042] 먼저, CI Main 어플리케이션은 CI 서비스를 제공하는 메인 어플리케이션(Main Application)으로 대기모드를 장악하여 고객에게 모바일(Mobile) 서비스 G/W로서 역할을 제공한다.

[0043] CI 부가 어플리케이션은 CI 서비스의 일환으로 개발한 단위 서비스를 제공하는 어플리케이션으로 대기모드 장악이 불가능 하다. 예컨대, CI-Game, CI-Music.. 등이 해당된다.

[0044] 기타 어플리케이션은 모바일 플랫폼(Mobile Platform)상에서 구동 되는 CI를 제외한 모든 어플리케이션(Application)을 나타낸다. 예컨대, LBS, MMS.. 등이 해당된다.

[0045] OEM 어플리케이션은 OEM에서 기본적으로 제공하는 어플리케이션(Application)을 나타낸다. 예컨대, Call, SMS 등이 해당된다.

[0046] 상기와 같이, CI Main 어플리케이션은 대기모드를 장악해서 고객에게 단말의 개별 서비스를 접근할 수 있는 UI 및 접근 경로를 제공한다.

[0047] 그리고, 실행 시 CI Main 어플리케이션은 적절한 입력(Input) 값을 주고, 실행 후 적절한 개별 서비스는 적절한 출력(Output) 값을 제공한다. 이 때, 연동하는 방식에 다음과 같이 2가지가 존재한다.

[0048] 첫째, 개별 어플리케이션(Application)을 통째로 호출하는 형태를 갖는다.

[0049] UI는 통일성을 유지하기 힘들고, 실행시점에 CI Main 어플리케이션은 보류(Pending)되어 단말의 UI를 장악하지 못한다. 종료 후 일정한 결과 값만을 CI Main 어플리케이션으로 전달한다. UI의 통일성을 위해서는 통째로 호출되는 어플리케이션은 UI에 대한 구현을 CI UI Guide에 맞게 진행해야 한다.

[0050] 둘째, API, Library형태의 모듈로 호출하는 형태를 갖는다.

[0051] CI Main 어플리케이션이 개별 어플리케이션 및 기능의 일부 모듈을 라이브러리(Library)로 호출하여 사용하는 형태로 기본적으로 UI는 통일되게 유지되고 키(Key) 및 사건(Event)처리는 CI Main 어플리케이션이 처리한다. 이를 위한 기능의 지원을 Mobile 플랫폼/CIM이 제공한다.

[0052] 상기에서와 같이, 본 발명에 의한 CI 서비스는 1. 개인의 성향 및 생활 사이클 패턴(Life cycle Pattern) 분석을 위한 단말의 히스토리(History)를 전송하는 센싱(Sensing) 기능; 2. 고객 패턴(Pattern) 분석에 따른 푸시/풀(Push/Pull) 형태의 서비스를 제공하는 서비스 푸싱(Pushing) 기능; 3. CI서비스는 대기모드 장악을 통해서 단말기능의 G/W로서 타 어플리케이션(Application)을 실행/종료 시 적절한 입/출력을 처리하는 수평 집약적(Horizontal Integration) 기능을 갖게 된다.

[0053] 이어서, 본 발명에 적용된 CI 서비스의 감지(Sensing)(Usage/Location History Gathering) 기능에 대하여 살펴보기로 한다.

[0054] 고객의 사용(Usage) 및 위치(Location)의 파악을 위해 두 가지 방식으로 히스토리(History)를 남기고 두 가지 방식으로 서버에 전송한다. 이러한 모든 방식의 설정은 서버에서 CI를 위한 SMS를 통해서 설정을 한다.

[0055] 이 때, 센싱(Sensing)을 단말에서 원천적으로 봉쇄할 수 있다. 이에 대한 설정/해지는 단말의 특정 메뉴를 통해서 고객이 설정한다.

[0056] 1) 센싱(Sensing) 대상

[0057] 센싱(Sensing) 대상은 다음의 정보를 활용하여 고객의 생활 패턴(Pattern)을 파악한다. 센싱(Sensing) 대상은 아래의 표 1(센싱의 항목)보다 다양한 정보일 수 있다.

표 1

세부	Description	확인/요구사항
Call 발/착신	발/착신 번호, 발/착신 시간 통화 시간	
SMS 발/착신	발/착신 번호, 발/착신 시간	
MMS 발/착신	발/착신 번호, 발/착신 시간	
단말 Power On/Off	단말 Power On/Off 시간 정보 (최대 5개)	
Morning Call Alarm	Morning Call Alarm 설정 정보	OEM 상의 설정정보
기지국 정보	기지국 세기, 기지국 ID : 최대 288개	

[0058]

[0059] 2) 히스토리 로깅(History Logging) 방식

[0060] 상기 히스토리 로깅은 History(Sensing대상)을 단말에 로그(Log)로 남기는 것에 대한 정의하며, 여기에는 시간 주기(Time Period) 방식과 사건구동(Event Driven) 방식이 적용된다.

[0061] 먼저, Time Period 방식은 일정시간을 간격(예컨대, 5분 간격)으로 현재 상태를 남기는 방식으로서 고객의 위치에 대한 로깅이 이에 해당된다.

[0062] 그리고, Event Driven 방식은 특정한 사건이 있을 때마다 그 시점을 기록하는 방식으로서 예컨대, Call Event, MMS Event, 등이 이에 해당된다.

[0063] 이 때, 히스토리 로깅(History Logging) 방식은 특정 사용(Usage) 형태마다 다를 수 있다. 즉, 호 히스토리(Call History)는 사건구동(Event Driven)형태 밖에 없을 것이고, 위치 히스토리(Location History)는 시간주기(Time Period), 사건구동(Event Driven) 둘 다 가능하다.

[0064] 그러므로 CIM-CIS 프로토콜(Protocol) 설계 및 API 설계시, 둘 다 가능한 히스토리(History)일 경우 두 가지 방식을 모두 지원할 수 있도록 설정 프로토콜(Protocol)을 제공해야 한다. 아래는 표 2는 히스토리별 로깅 방식의 차이표를 나타낸 것이다.

표 2

항목	Time Period Logging 가능	Event Driven Logging 가능	비고
Call 착/발신	X	O	
MMS 착/발신	X	O	
SMS 착/발신	X	O	
on/off History	X	O	
Moring Call 설정	O	O	Time Period방식이 가능하나 별 의미가 없음
Application 실행정보	X	O	
Location	O	O	
기타 설정정보	O	O	Time Period방식이 가능하나 별 의미가 없음

[0065]

[0066] 이 때, 상기 시간 주기(Time Period) 방식으로 로깅(Logging)이 가능한 히스토리(History)에 대해서는 시간주기 설정이 가능하도록 프로토콜(Protocol) 구성이 필요하다.

[0067] 3) 로그 전송(Log Transfer) 방식

[0068] 상기 로그 전송방식은 단말에 남긴 로그(Log)를 서버로 전송하는 방법은 3가지 종류가 있다.

[0069] 첫째, 서버요청 시점 마다 전송하는 방식은 서버가 SMS Push를 사용하여 히스토리(History)를 요청할 때 마다 전송하는 방식이고, 둘째 일정시간마다 전송하는 방식은 미리 설정된 시간 간격 마다 축적된 단말 로그(Log)를 서버로 전송하는 방식이며, 셋째 이벤트(Event) 발생시 마다 전송하는 방식은 특정 사건 예컨대 위치의 변화, Call History 발생, SMS History 발생 등 Event 발생시 마다 서버로 전송하는 방식이다.

[0070] 이러한 3가지에 대한 설정을 서버는 SMS Push로 단말에 설정한다. 이는 히스토리(History)별로 설정 할 수 있어야 한다. 예컨대 위치(Location)은 사건(Event)마다 알려주고, 호 히스토리(Call History)는 하루에 한번 올린다는 식으로 설정한다.

[0071] 상기와 같이, 서버요청마다 전송(Transfer)하는 것은 따로 설정하는 것이 아니며, 모든 히스토리(History)에 해당 히스토리(History)별로 동시에 설정 가능하다.

[0072] 4) 위치 감지(Location Sensing)

[0073] 상기의 위치 감지 방식은 위치 포맷(Location Format) 방식과, 로깅(Logging) 및 로그 전송(Log Transfer) 방식으로 나뉘다.

[0074] 위치 포맷에서의 위치(Location) 정보는 핸드셋(Handset)이 무선통신을 하기 위한 자신의 위치 정보를 활용한다. 위치정보는 기지국 ID 및 GPS 단말일 경우 GPS ID가 될 수 있다. 이 모두를 위치(Location) ID라고 한다.

[0075] 로깅(Logging) 및 로그 전송(Log Transfer) 방식은 아래의 사항을 제공한다.

[0076] 첫째, 특정 지역에 도달했을 경우 로깅 및 Transfer 제공은 특정지역에 대한 셋팅(Setting)은 CIS가 단말로 미리 특정 Location ID를 설정해 주고, 단말은 이 지역에 도달했을 때 자신의 위치에 대한 로깅(Logging) 및 전송(Transfer)을 제공한다.

[0077] 둘째, 셀(Cell)이 변경 될 때마다 Logging 및 Transfer 제공 방식은 로깅(Logging)을 셀(Cell) 변경 사건(Event)마다(Handoff 시마다) 남기고, 즉시 알리는 것으로 사건구동 로깅 및 전송(Event Driven Logging & Transferring)을 의미한다.

[0078] 마지막으로, 본 발명에 적용된 서비스 푸시(Push) 및 알람(Alarm) 실행에 대하여 도 5를 참조하여 살펴보기로 한다.

[0079] 도 5에 도시된 바와 같이, 서비스 푸시(PUSH)는 SMS를 통해서 서버에서 단말에 어떤 실행을 요청하는 것으로서, 단말의 CIM이 이러한 SMS Push를 관장하여 해당 어플리케이션에 사건(Event)을 전달한다.

[0080] 그 과정을 살펴보면, CIS(Communication Intelligence Server)는 CITS(Communication Intelligence Terminal System)에 특정 TID xxxxx으로 SMS를 송출한다.

[0081] Mobile 플랫폼은 TID xxxxx이 CIM용 Message임을 알고 이에 대한 Event를 CIM(Communication Intelligence Manager)에 전달한다.

[0082] CIM은 AID 4324324324(가상ID임)인 어플리케이션(Application)에 특정 Parameter= "PAM " 전달한다.

[0083] 이 때, CIS가 CIM에 전달하는 서비스 Push는 크게 두 가지 종류가 있다. 1)즉시 Push는 일회성 Push Message(Event)를 특정 어플리케이션에 즉시 전달하며, 2) 예약 Push는 시작시간이후 Push Message(Event)를 특정 어플리케이션에 전달한다.

[0084] 또한, 주기설정 가능, 주기별 재 실행(주기는 시 분 초 단위로 설정) CIM이 어플리케이션에 전달하는 Push Event(즉시/예약 모두 포함됨)는 단말기의 상태별로 다음과 같이 표 3(푸시 이벤트 전달에 다른 단말상태별 액션)에 도시된 액션(Action)을 취한다.

표 3

단말상태	Action
IDLE	CIM은 해당 Application(Push Message 상의 AID를 가지는)을 실행 시키고 Event를 전달한다.
해당 Application이 실행 중	CIM은 해당 Application에 Event만 전달 (이미 실행 중이므로 재실행 필요 없음)
타 Application또는 OEM 실행 중	OEM Application실행 중(ex전화 중) 또는 타 Application이 실행 중일 경우 CIM은 Anuciator 영역에 CI Push Event가 도착했음을 알림. 해당 실행이 종료 되면 CIM은 해당 Application에 Event 전달

[0085]

발명의 효과

[0086] 이상에서와 같이 본 발명에 의한 사용자의 단말 형태정보 파악방법 및 그 시스템에 따르면 다음과 같은 효과가 있다.

[0087] 첫째, 대기화면 상의 캐릭터 인터페이스(Character I/F)를 통하여 친근하고 대화식(Interactive) 서비스를 제공할 수 있다.

[0088] 둘째, 모바일 인터넷 컨텐츠(Mobile Internet Content)를 고객의 성향 및 패턴(Pattern)에 맞게 배달하여 줄 수 있다.

[0089] 셋째, 기존의 모바일 인터넷 브라우저(Mobile Internet Browser)상의 서비스 형태별로 수직 분할된 각 CP의 컨텐츠를 CI 서비스를 통하여 수평 집약적(Horizontal Integration)하여 개인에게 최적화된 형태로 서비스를 제공할 수 있다.

[0090] 넷째, 고객의 성향 및 외부 환경(날씨, 위치, 시간)을 파악하여 적절한 이벤트 및 서비스를 제공할 수 있다.

도면의 간단한 설명

[0001] 도 1은 본 발명에 따른 사용자의 단말 형태정보 서비스 제공을 위한 개념도이다.

[0002] 도 2는 본 발명에 적용된 지능형 통신단말시스템(CITS)을 이용한 사용자 단말 형태정보 시스템의 구성도이다.

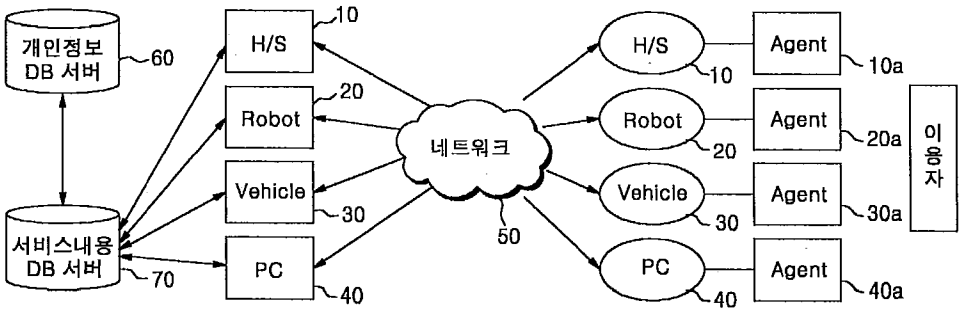
[0003] 도 3은 본 발명에 적용된 지능형 통신단말시스템(CITS)을 이용한 사용자 단말 형태정보 제공과정을 나타낸 흐름도이다.

[0004] 도 4는 도 2에 도시된 CI 어플리케이션의 상세 구성도이다.

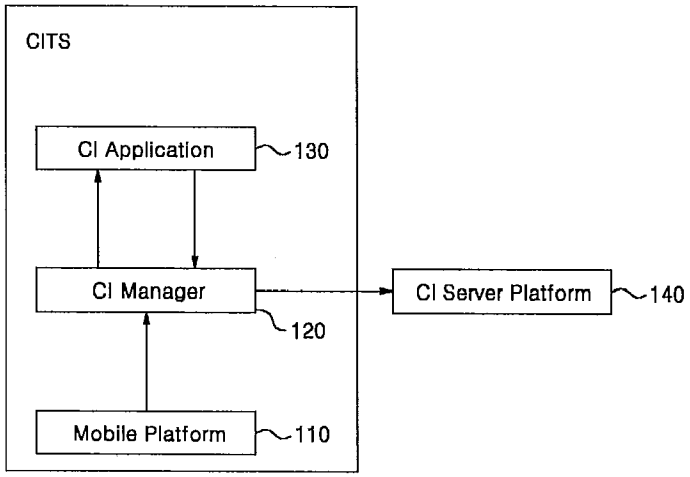
[0005] 도 5는 도 2에 도시된 CITS의 서비스 푸시(Push)에 대한 개념도이다.

도면

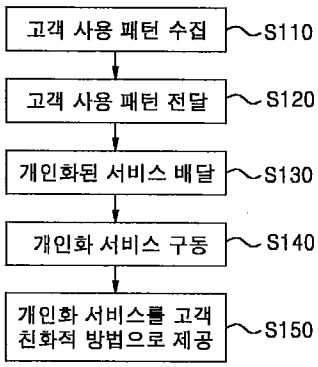
도면1



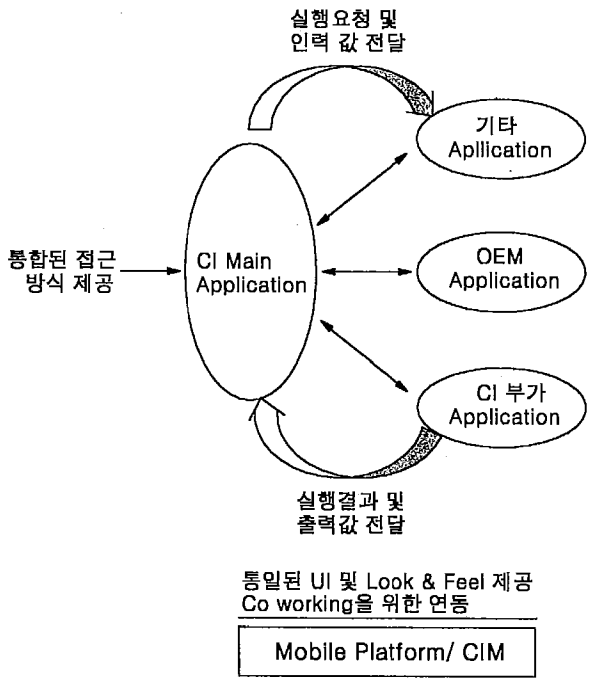
도면2



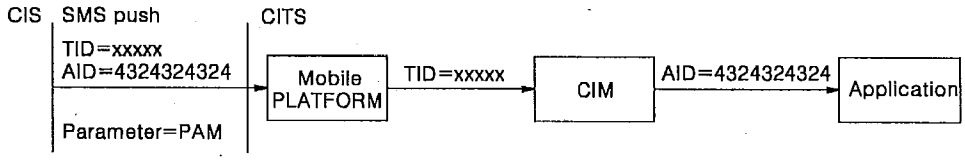
도면3



도면4


실행요청 및
인력 값 전달
기타
Apllication
통합된 접근
방식 제공
CI Main
Application
OEM
Application
CI 부가
Application
실행결과 및
출력값 전달
통일된 UI 및 Look & Feel 제공
Co working을 위한 연동
Mobile Platform/ CIM

도면5


CIS
SMS push
TID=xxxxx
AID=4324324324
Parameter=PAM
CITS
Mobile
PLATFORM
TID=xxxxx
CIM
AID=4324324324
Application

Electronic Acknowledgement Receipt

EFS ID:	12219197
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	05-MAR-2012
Filing Date:	06-JAN-2011
Time Stamp:	03:47:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	March_5_IDS2.pdf	612567 a1a09249258e9569eaf19a1fa6eb8dd8d6b94111	no	4

Warnings:	
Information:	

2	Foreign Reference	npl1fr.pdf	769751 1d5af5ee3bb9e974cb1d3b2084c7e094f1b8a9af	no	16
Warnings:					
Information:					
3	Foreign Reference	npl2fr.pdf	376860 29154adc82f151f9e0f827b4b8c30c3bd81acc1e	no	9
Warnings:					
Information:					
4	Foreign Reference	npl3fr.pdf	579122 016d44e70566b39d347810a119f2f433c8c24e8a	no	12
Warnings:					
Information:					
5	Foreign Reference	npl4fr.pdf	590060 89e99f01541f6f48d8ff7f7a4996255db70e3f1e	no	20
Warnings:					
Information:					
6	Foreign Reference	nplfr5.pdf	472887 129bf6a77631ac1c43f0dfc5f6db5e31bd81c78a	no	13
Warnings:					
Information:					
		Total Files Size (in bytes):	3401247		

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

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	William Grecia
Art Unit	2432
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

	1	Author - Michael Arrington - Movie Labels To Launch New "Open Market" Play Anywhere Scheme As Last Ditch Effort To Save DRM - Publication Source: TechCrunch.com [URL: http://techcrunch.com/2008/08/26/movie-labels-to-launch-new-open-market-play-anywhere-scheme-as-last-ditch-effort-to-save-drm/] - (INTERNET PUBLICATION 8-26-2008)	☐
	2	Author - Mitch Singer - Developing the Digital Market - Publication Source: TechCrunch.com [URL: http://tctechcrunch.files.wordpress.com/2008/08/singer.pdf] - (INTERNET PUBLICATION 8-26-2008)	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	William Grecia
Art Unit	2432
Examiner Name	
Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature		Date (YYYY-MM-DD)	
Name/Print		Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	11839635
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	14-JAN-2012
Filing Date:	06-JAN-2011
Time Stamp:	19:25:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	singer_tc_IDS.pdf	612562 32f78bf1c6dde4415f581b190d0dbb0ecad2a995	no	4

Warnings:	
Information:	

A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

2	Non Patent Literature	singer_techcrunch_2008.pdf	7170006 1f4b13d8fde12064d972818554846be8cb495f00	no	17
Warnings:					
Information:					
3	Non Patent Literature	tcma.pdf	265785 e3fe0789bfbe68ba80b35cd71043d7225ef318e7	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	8048353	

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	Grecia, William
Art Unit	2432
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7610630		2009-10-27	Ming Ji	
	2	7689823		2010-03-30	Sheng Mei Shen	
	3	7702592		2010-04-20	James H. Taylor	
	4	7515710		2009-04-07	Eric W. Grab	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	Grecia, William
	Art Unit	2432
	Examiner Name	
	Attorney Docket Number	

	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	Grecia, William
Art Unit	2432
Examiner Name	
Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2011-11-22
Name/Print	William Grecia	Registration Number	70984

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	11470760
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	22-NOV-2011
Filing Date:	06-JAN-2011
Time Stamp:	21:18:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	nov22_IDS.pdf	612372 8f5aa70ffe57480f5ae63174742768cdebfde11d	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	612372

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 12/985,351

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))	22 minus 20 =	* 2	x 30 =	60	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 125 =	0.00			
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))				225			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	815		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	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
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.

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
12/985,351	01/06/2011	2431	1009		20	3

CONFIRMATION NO. 4165

UPDATED FILING RECEIPT

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

OC00000050209043

Date Mailed: 10/11/2011

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)

William Grecia, Brooklyn, NY;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 12/728,218 03/21/2010 ABN

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.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 01/14/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/985,351**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: Yes
**** SMALL ENTITY ****

Title

PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)

Preliminary Class

713

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).

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	12985351
Filing Date	2011-01-06
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6799165		2008-09-28	Boesjes; Eimar M	
	2	6385596		2002-05-07	Wiser; Philip R	
	3	5907617		1999-05-25	Ronning; Joel A	
	4	5903647		1999-05-11	Ronning; Joel A	
	5	5887060		1999-03-23	Ronning; Joel A	
	6	5883955		1999-03-16	Ronning; Joel A	
	7	5883954		1999-03-16	Ronning; Joel A	
	8	5870543		1999-02-09	Ronning; Joel A	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Author - PRESTON GRALLA - Digital River Launches DRM Solution For Software Publishers - Publication Source: informationweek.com [URL: http://www.informationweek.com/news/18901739] - (INTERNET PUBLICATION DATE: 04-15-2004)	☐
	2	Author - Digital River Corporation - Digital River Announces New Digital Rights Management Service - Publication Source: digitalriver.com [URL: http://www.digitalriver.com/corporate/press_releases/pr_328.shtml] - (INTERNET PUBLICATION DATE: 07-14-2003)	☐
	3	Author - Digital River Corporation - Digital River SoftwarePassport Copyright software - Publication Source: siliconrealms.com [URL: http://www.siliconrealms.com/] - (INTERNET PUBLICATION)	☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	12985351
	Filing Date	2011-01-06
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/william grecia/	Date (YYYY-MM-DD)	2011-06-29
Name/Print	William Grecia	Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	10410373
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	29-JUN-2011
Filing Date:	06-JAN-2011
Time Stamp:	08:40:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	UV_IDS.pdf	612391 32826a1c11e6fe300af91f6264d60c3ee63b5f44	no	5

Warnings:	
Information:	

2	Non Patent Literature	sp.pdf	471973 37c7d5df7f373216aff3e6560c18b8b971163f89	no	2
Warnings:					
Information:					
3	Non Patent Literature	DigitalRiver.pdf	130684 80f76703535fb1d254a6e0cf8e421ed979c99f8c	no	2
Warnings:					
Information:					
4	Non Patent Literature	InformationWeek.pdf	340922 0cbb2c821565294bf8621ba72946ebea16fb2be5	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	1555970		

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/985,351	01/06/2011	William Grecia	

CONFIRMATION NO. 4165

PUBLICATION NOTICE

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

OC00000047402618

Title:PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)

Publication No.US-2011-0099382-A1
Publication Date:04/28/2011

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

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	12985351
Filing Date	01-06-2011
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
		20100299264		11/25/2010	Richard Berger, Mitch Singer	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
								☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	
	Art Unit	
	Examiner Name	
	Attorney Docket Number	

			☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	
	Art Unit	
	Examiner Name	
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

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

Signature		Date (YYYY-MM-DD)	
Name/Print		Registration Number	

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	9586059
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	04-MAR-2011
Filing Date:	06-JAN-2011
Time Stamp:	11:41:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	ids_ms.pdf	188682 46dea41e5b76eff85732cb6df85cc4e68634dfe2	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form

Total Files Size (in bytes):	188682

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/08b(05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of | |

Complete if Known	
Application Number	12/985,351
Filing Date	01-06-2011
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Internet publication: Nook Color LendMe www.barnesandnoble.com/	
		Internet publication: Coral consortium "Scenario" www.coral-interop.org	

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 copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	9413834
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	10-FEB-2011
Filing Date:	06-JAN-2011
Time Stamp:	00:07:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	NPL Documents	Coral_Scenario_rs.pdf	8323062 53d971a83ef90c5b4657f9a82379dbc764596785	no	24

Warnings:	
Information:	

2	Information Disclosure Statement (IDS) Filed (SB/08)	sb0008z.pdf	118283 8da3ac14332ca2719bee7a07a047f5a3e7b85a75	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	NPL Documents	NOOKcolor.pdf	365178 b3c7ae71731456431ecef781f7ad8e8b21a35a39	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8806523		

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/985,351	01/06/2011	William Grecia	

CONFIRMATION NO. 4165

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

FORMALITIES LETTER

OC000000045509064

Date Mailed: 01/21/2011

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Additional claim fees of $**52** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**52** for a small entity
- Total additional claim fee(s) for this application is $**52**
  - $**52** for **2** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/etadesse/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/985,351	01/06/2011	2431	957		20	3

CONFIRMATION NO. 4165

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

FILING RECEIPT

OC000000045509063

Date Mailed: 01/21/2011

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)

William Grecia, Brooklyn, NY;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 12/728,218 03/21/2010

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.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 01/14/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/985,351**

Projected Publication Date: 04/28/2011

Non-Publication Request: No

Early Publication Request: Yes
**** SMALL ENTITY ****

Title

PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)

Preliminary Class

726

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: 12/985,351

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	82		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	270		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	110		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	22 minus 20 =	* 2	x 26 =	52	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 110 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 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))				195			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	709		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	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
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.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
12985351	

Applicant(s) William Grecia

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1					
2		1				
3		1				
4		1				
5		2				
6		1				
7		1				
8		1				
9		1				
10	1					
11		1				
12		1				
13		1				
14		2				
15	1					
16		1				
17		1				
18		1				
19		1				
20		1				
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	3		0		0	
Total Depend	19	↵	0	↵	0	↵
Total Claims	22		0		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

Electronic Patent Application Fee Transmittal

Application Number:	12985351
Filing Date:	06-Jan-2011
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Filer:	William Grecia
Attorney Docket Number:	

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:				
Claims in excess of 20	2202	2	26	52
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**52**

Electronic Acknowledgement Receipt

EFS ID:	9276314
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	21-JAN-2011
Filing Date:	06-JAN-2011
Time Stamp:	07:07:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$52
RAM confirmation Number	7753
Deposit Account	
Authorized User	

File Listing:

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

1	Fee Worksheet (PTO-875)	fee-info.pdf	29811 06340134ba27c2c15b99dde4f1a09080d75e5cb9	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	29811

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

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/08a (05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of | |

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

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 copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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/08b(05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of |

Complete if Known	
Application Number	12/985,351
Filing Date	01/06/2011
First Named Inventor	William Grecia
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Author – WIKIPEDIA.ORG – Steam (software) – Publication Source: wikipedia.org [URL:http://http://en.wikipedia.org/wiki/Steam_(software)	

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 copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	9208253
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	11-JAN-2011
Filing Date:	
Time Stamp:	15:08:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	sb0008steam.pdf	272036 d417edcfd99b0bc997666a0494574e858148f6ab	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	NPL Documents	Steam.pdf	1264897 a365e8a32459c21712dc4f4e34f839746cfcf370	no	30
Warnings:					
Information:					
			Total Files Size (in bytes):	1536933	

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 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE

UTILITY PATENT APPLICATION TRANSMITTAL

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

Attorney Docket No.	
First Inventor	William Grecia
Title	PERSONALIZED DIGITAL MEDIA ACCESS
Express Mail Label No.	

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* 32]
   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* 7]
5. **Oath or Declaration** [*Total Sheets* 4]
   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: Early publication request

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.: 12/728,218

Prior application information: *Examiner* - *Art Unit:* 2431

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 70984 ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/william grecia/	Date	01/04/2011
Name (Print/Type)	William Grecia	Registration No. (Attorney/Agent)	

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/01 (04-09)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	
First Named Inventor	Willaim Grecia
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)

(Title of the Invention)

the application of which

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☒ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (04-09)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Utility or Design Patent Application

Direct all correspondence to:	☒	The address associated with Customer Number:	70984	**OR** ☐	Correspondence address below

Name		
Address		
City	State	Zip
Country	Telephone	Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: *Patent Application Files*. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: *Deposit Accounts and Electronic Funds Transfer Profiles*.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:	☐ A petition has been filed for this unsigned inventor
Given Name (first and middle [if any])	Family Name or Surname
William	Grecia

Inventor's Signature	Date
/william grecia/	01/04/2011

Residence: City	State	Country	Citizenship
Brooklyn	NY	USA	American

Mailing Address			
2885 Sanford Ave SW #13208			
City	State	Zip	Country
Grandville	MI	49418	USA

☐ Additional inventors or a legal representative are being named on the _____ supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7290699		2007-11-06	Reddy; Karimireddy Hari	
	2	7340769		2008-03-04	Baugher; Mark John	
	3	7343014		2008-03-11	Sovio; Sampo	
	4	7386513		2008-06-10	Lao; Guillermo	
	5	7571328		2008-08-04	Baumert; David W	
	6	7624417		2008-11-24	Dua; Robin	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	1	20020010759		2002-01-24	Hitson; Bruce L	
	2	20020157002		2002-10-24	Messerges; Thomas S.	
	3	20030220880		2003-11-27	Lao; Guillermo	
	4	20040024670		2004-02-05	Valenzuela; Edgar	
	5	20040062400		2004-04-01	Sovio; Sampo	
	6	20040162786		2004-08-19	Cross; David B	
	7	20040220878		2004-11-04	Lao; Guillermo	
	8	20050066353		2005-03-24	Fransdonk; Robert	
	9	20050182727		2005-08-18	Robert, Arnaud	
	10	20060173787		2006-08-03	Weber; Daniel	
	11	20060173789		2006-08-03	Baumert; David W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	12	20060259852		2006-11-16	Upendran; Manish	
	13	20060259982		2006-11-16	Upendran; Manish	
	14	20070055887		2007-03-08	Cross; David B	
	15	20070156719		2007-07-05	Upendran; Manish	
	16	20070179854		2007-08-02	Ziv; Aran	
	17	20070180485		2007-08-02	Dua; Robin	
	18	20070250445		2007-10-25	Ache; Marc	
	19	20080027869		2008-01-31	Kalker; Antonius	
	20	20080091606		2008-04-17	Grecia; William	
	21	20080109911		2008-05-08	Tedesco; Megan Lesley	
	22	20080165956		2008-07-10	Zhu; Bin	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	23	20090012805		2009-01-08	Schnell; Patrik	
	24	20090049556		2009-02-19	Vrielink; Koen Hendrik Johan	
	25	20090083541		2009-03-26	Levine; Scott	
	26	20090183010		2009-07-16	Schnell; Patrik	
	27	20090217036		2009-08-27	Irwin; James	
	28	20090254930		2009-10-08	Lo; Charles N	
	29	20090257591		2009-10-15	MITHAL; ASHISH K	
	30	20090265278		2009-10-22	WANG; Xin	
	31	20090299963		2009-12-03	Pippuri; Sami	
	32	20090307078		2009-12-10	Mithal; Ashish K	
	33	20090327702		2009-12-31	Schnell; Patrik	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	34	20090328228		2009-12-31	Schnell; Patrik	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1505530A1	EP			Lao, Guillermo		☐
	2	1564621A1	EP			Robert, Arnaud		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Author - WILLIAM GRECIA - STR3EM Windows Java C++ written code copyright and support documentation - Publication Source: str3em.com [URL: http://www.str3em.com] - (SOFTWARE COPYRIGHT PUBLICATION DATE AND INVENTION REDUCED TO PRACTICE: 09-03-2009)	☐
	2	Author - WILLIAM GRECIA - Next Generation Digital Delivery STR3EM Ecosystem Replaces DVD And Blu-Ray - Publication Source: mi2n.com [URL: http://mi2n.com/press.php3?press_nb=130517] - (INTERNET PUBLICATION DATE: 05-28-2010)	☐
	3	Author - FACEBOOK CORPORATION - Graph API documentation - Publication Source: facebook.com [URL: http://developers.facebook.com/docs/api] - (INTERNET PUBLICATION UPDATE: 04-21-2010)	☐
	4	Author - AMAZON INC - Amazon Web Services API documentation - Publication Source: [URL: http://aws.amazon.com] - (INTERNET PUBLICATION)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	5	Author - RICK MERRITT - Analysis: Hollywood's next digital media gambit - Publication Source: eetimes.com [URL: http://www.eetimes.com/design/audio-design/4005862/Analysis-Hollywood-s-next-digital-media-gambit] - (INTERNET PUBLICATION DATE: 11-02-2008)	☐
	6	Author - ETHAN SMITH - Disney Touts a Way to Ditch the DVD - Publication Source: Wall Street Journal Online [URL: http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703816204574485650026945222.html] - (INTERNET PUBLICATION DATE: 09-21-2009)	☐
	7	Author - Neda Ulaby - Introducing UltraViolet: Buy Your Digital Movie Once, Play It Anywhere? - Publication Source: NPR Online [URL: http://www.npr.org/blogs/monkeysee/2010/07/19/128626624/introducing-ultraviolet-buy-your-movie-once-play-it-anywhere] - (INTERNET PUBLICATION DATE: 07-20-2010)	☐
	8	Author - WILLIAM GRECIA - The Retail Zip Company Releases Secure Electronic Media Format STR3EM To Replace DVD And Blu-ray - Publication Source: mi2n.com [URL: http://mi2n.com/press.php3?press_nb=122843] - (INTERNET PUBLICATION DATE: 09-03-2009)	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

PTO/SB/08a (05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | of

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	William Grecia
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-20030051149	03-13-2003	Robert, Arnaud	
		US-20050182727	08-18-2005	Robert, Arnaud	
		US-20050182931	08-18-2005	Robert, Arnaud	
		US-20050198510	09-08-2005	Robert, Arnaud	
		US-20050216752	09-29-2005	Robert, Arnaud	
		US-20080114992	05-15-2008	Robert, Arnaud	
		US-20080137869	06-12-2008	Robert, Arnaud	
		US-20090086975	04-02-2009	Robert, Arnaud	
		US-20090089884	04-02-2009	Robert, Arnaud	
		US-20090106850	04-23-2009	Robert, Arnaud	
		US-20100027796	03-04-2010	Robert, Arnaud	
		US-20100057527	03-04-2010	Robert, Arnaud	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

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 copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours 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/08b(05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | | of | |

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

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 copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 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/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	1	Author - APPLE CORPORATION - iTunes application copyright - Publication Source: apple.com [URL: www.apple.com/itunes] - (COPYRIGHT PUBLICATION DATE: 01-09-2001)	☐
	2	Author - MICROSOFT CORPORATION - Zune application copyright - Publication Source: zune.net [URL: www.zune.net] - (COPYRIGHT PUBLICATION DATE: 11-14-2006)	☐
	3	Author - NETFLIX CORPORATION - Netflix application copyright - Publication Source: netflix.com [URL: www.netflix.com] - (COPYRIGHT PUBLICATION)	☐
	4	Author - BEST BUY CORPORATION - CinemaNow application copyright - Publication Source: cinemanow.com/ [URL: www.cinemanow.com/] - (COPYRIGHT PUBLICATION)	☐
	5	Author - BEST BUY CORPORATION - Napster application copyright - Publication Source: napster.com/ [URL: www.napster.com/] - (COPYRIGHT PUBLICATION)	☐
	6	Author - GOOGLE CORPORATION - YouTube application copyright - Publication Source: youtube.com/ [URL: www.youtube.com/] - (COPYRIGHT PUBLICATION)	☐
	7	Author - WAL-MART CORPORATION - Vudu application copyright - Publication Source: vudu.com/ [URL: www.vudu.com/] - (COPYRIGHT PUBLICATION)	☐

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	William Grecia
Art Unit	2431
Examiner Name	
Attorney Docket Number	

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

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

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

	1	Author - CONNECTED MEDIA EXPERIENCE ORG- CMX specification - Publication Source: connectedmediaexperience.org [URL: www.connectedmediaexperience.org/technicaloverview.html] - (INTERNET PUBLICATION)	☐
	2	Author - SMPTE ORG - Digital Cinema DCP MXF speifications - Publication Source: smpte.org [URL: www.smpte.org/standards] - (INTERNET PUBLICATION)	☐
	3	Author - WIKIPEDIA ORG - Xbox Live Marketplace and Zune Marketplace - Publication Source: wikipedia.org [URL: http://en.wikipedia.org/wiki/Xbox_Live#Xbox_Live_Marketplace_and_Zune_Marketplace] - (INTERNET PUBLICATION)	☐
	4	Author - DAN FRANKS - First Look: iTunes Digital Copy - Publication Source: macworld.com/ [URL: www.macworld.com/article/131751/2008/01/digitalcopy.html/] - (INTERNET PUBLICATION 01-22-08)	☐
	5	Author - RICH FISCUS - Review - Is DVD Digital Copy worth the trouble? - Publication Source: afterdawn.com/ [URL: www.afterdawn.com/news/article.cfm/2009/11/18/review_is_dvd_digital_copy_worth_the_trouble] - (INTERNET PUBLICATION 11-18-2009)	☐
	6	Author - WIKIPEDIA ORG - Digital rights management - Publication Source: wikipedia.org [URL: http://en.wikipedia.org/wiki/Digital_Rights_Management] - (INTERNET PUBLICATION)	☐
	7	Author - WIKIPEDIA ORG - Application programming interface - Publication Source: wikipedia.org [URL: http://en.wikipedia.org/wiki/Api] - (INTERNET PUBLICATION)	☐
	8	Author - WIKIPEDIA ORG - Steam (content delivery) - Publication Source: wikipedia.org [URL: http://en.wikipedia.org/wiki/Steam_(content_delivery)] - (INTERNET PUBLICATION)	☐
	9	Author - BEN DRAWBAUGH - Disney's KeyChest is not DRM - Publication Source: engadget.com [URL: www.engadget.com/2010/01/10/disneys-keychest-is-not-drm] - (INTERNET PUBLICATION 01-10-2010)	☐
	10	Author - RICHARD LAWLER - DECE & Keychest both laying claim to friendly DRM of the future title - Publication Source: engadget.com [URL: www.engadget.com/2010/01/06/dece-and-keychain-both-laying-claim-to-friendly-drm-of-the-future/] - (INTERNET PUBLICATION 01-06-2010)	☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	William Grecia
	Art Unit	2431
	Examiner Name	
	Attorney Docket Number	

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	William Grecia
Art Unit	
Examiner Name	Unknown
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6611812	08-26-2003	Hurtado; Marco M.	
		US- 7568111	07-28-2009	Alve, Jukka	
		US- 20090164776	06-25-2009	Tuoriniemi; Samuli	
		US- 20080209576	08-28-2008	Nooning; Malcolm H.	
		US- 20100057871	03-04-2010	Kaplan; Gregg	
		US- 6665797	12-16-2003	Keung; Tse Ho	
		US- 5586186	12-17-1996	Yuval; Gideon A.	
		US- 5719938	02-17-1998	Haas; Zygmunt	
		US- 5010571	04-23-1991	Katznelson; Ron D.	
		US- 5247575	09-21-1993	Sprague; Peter J.	
		US- 5267313	11-30-1993	Hirata; Kozo	
		US- 5319705	06-07-1994	Halter; Bernard J.	
		US- 5349642	09-20-1994	Kingdon; Kevin	
		US- 5509074	04-16-1996	Choudhury; Abhijit K.	
		US- 5737416	04-07-1998	Cooper; Thomas Edward	
		US- 7516495	04-07-2009	Shoemaker; Charles H.	
		US- 20050138406	06-23-2005	Cox, Alan	
		US- 7594275	09-22-2009	Zhu; Bin	
		US- 20100043077	02-18-2010	Robert; Arnaud	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

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 copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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.

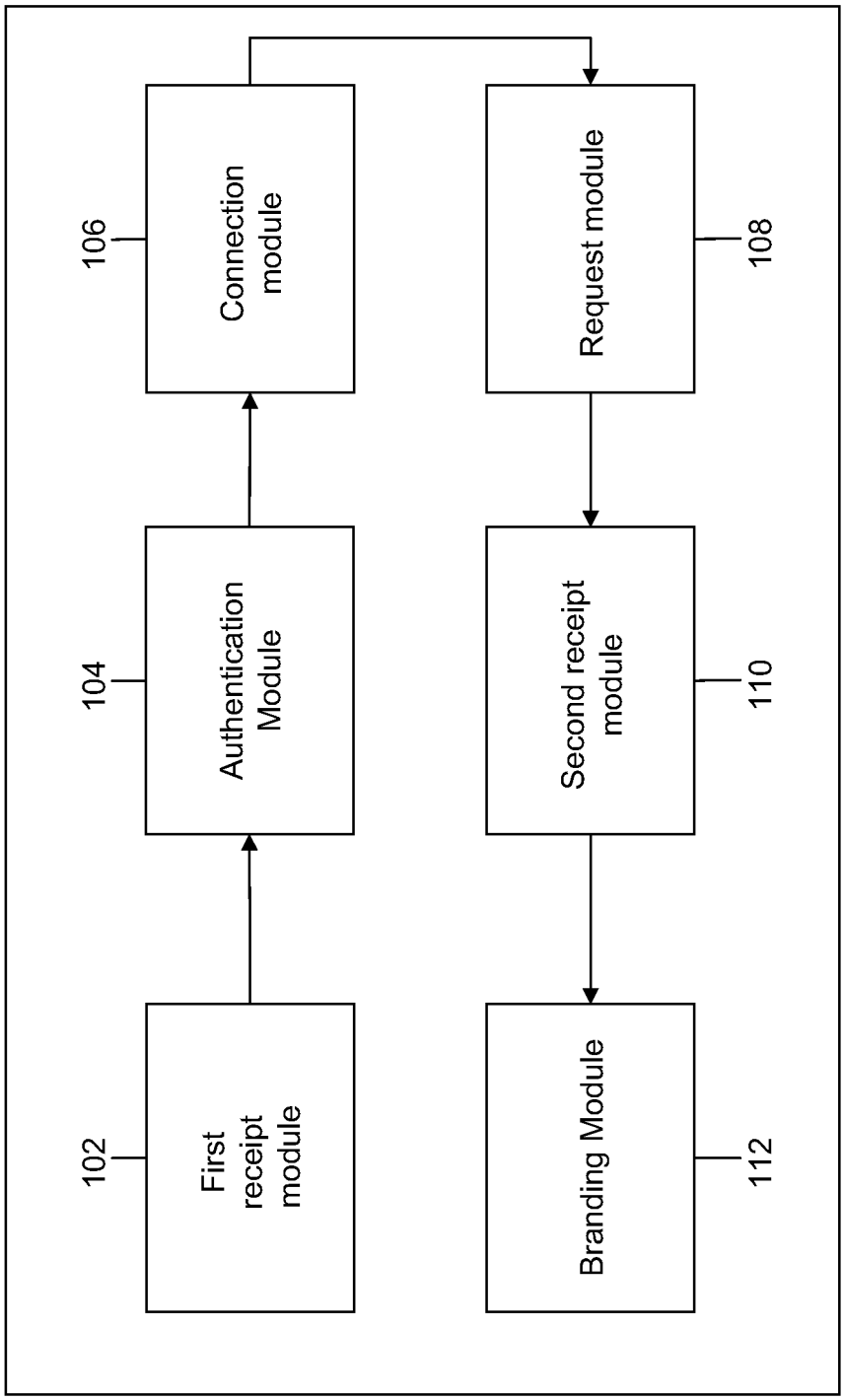

First receipt module
102
Authentication Module
104
Connection module
106
Request module
108
Second receipt module
110
Branding Module
112

FIG.1

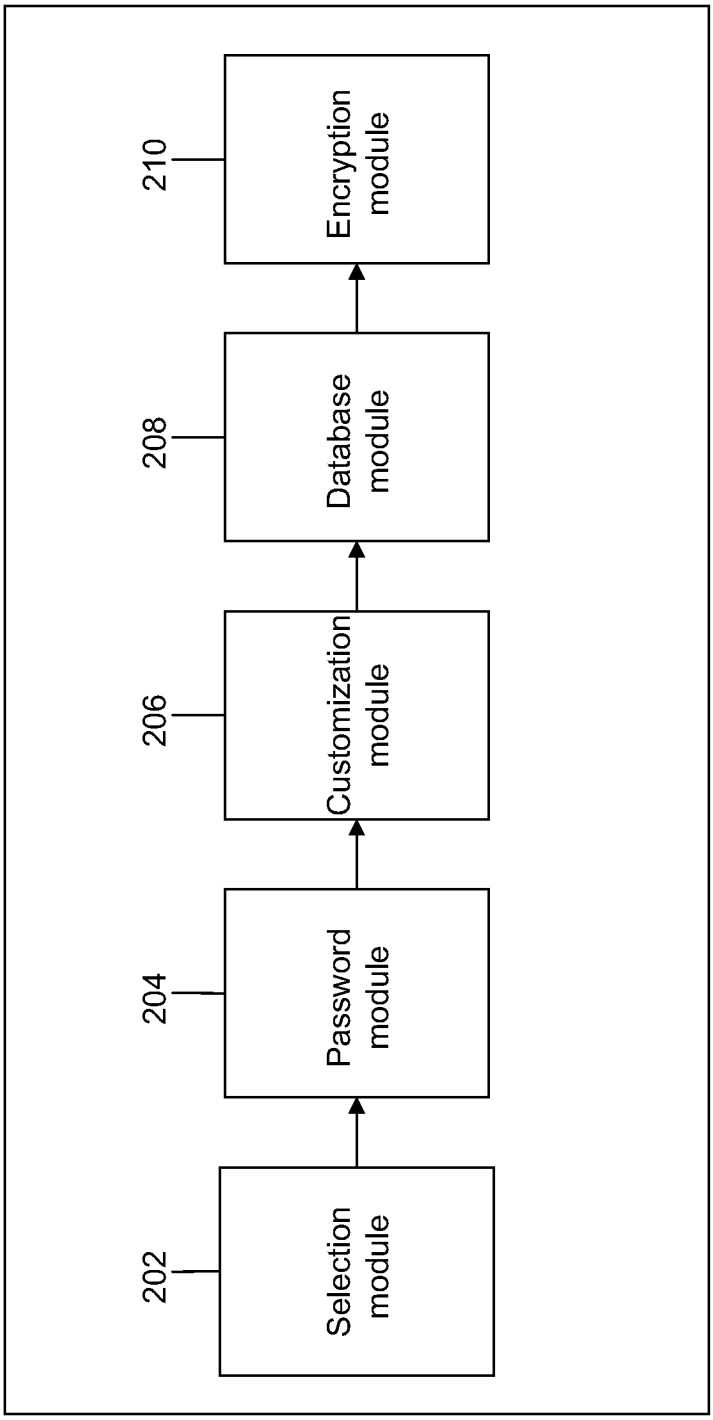

202
Selection module
204
Password module
206
Customization module
208
Database module
210
Encryption module

FIG.2

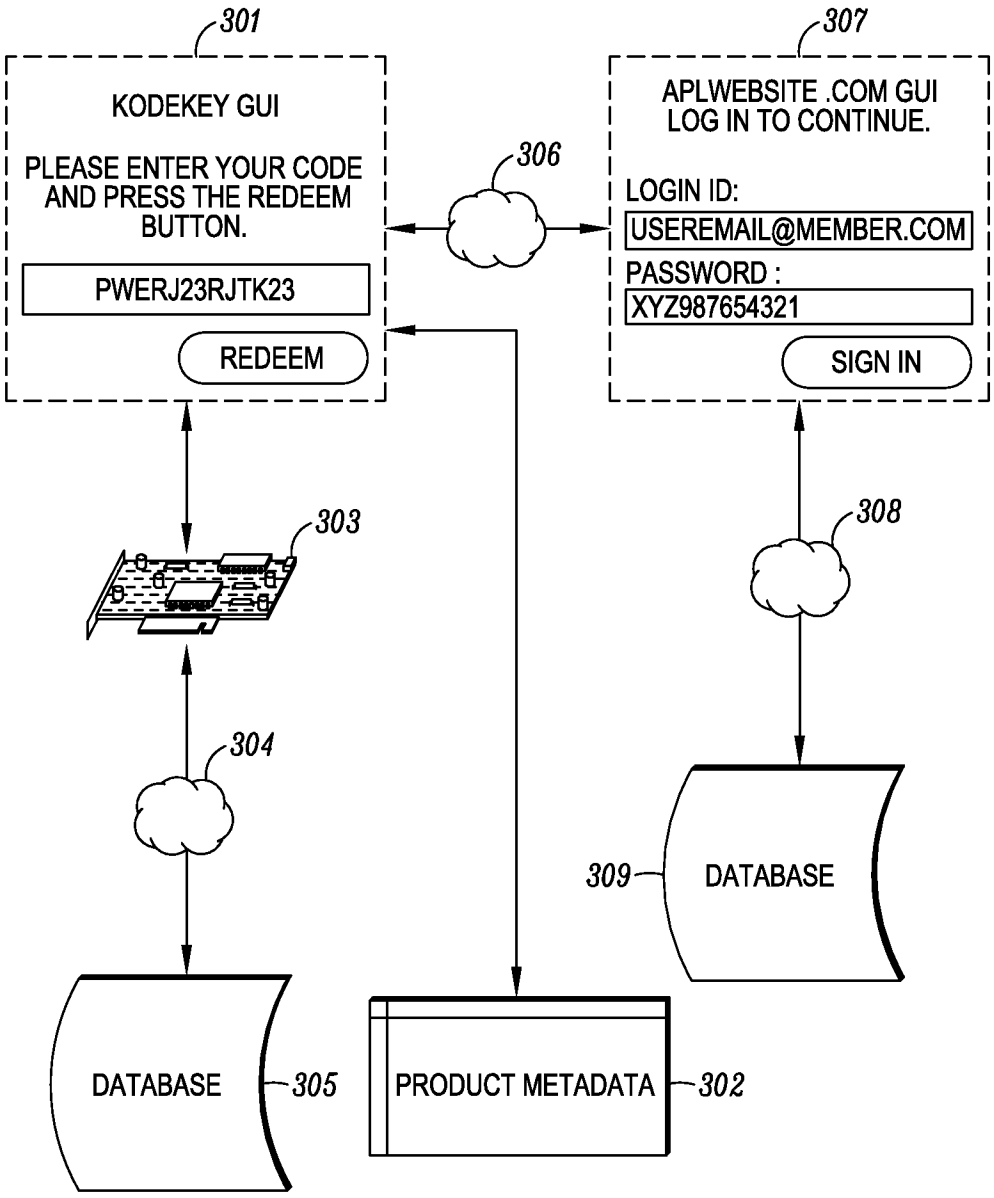

301
KODEKEY GUI
PLEASE ENTER YOUR CODE AND PRESS THE REDEEM BUTTON.
PWERJ23RJTK23
REDEEM
306
307
APLWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
303
304
308
309
DATABASE
DATABASE
305
PRODUCT METADATA
302

FIG. 3

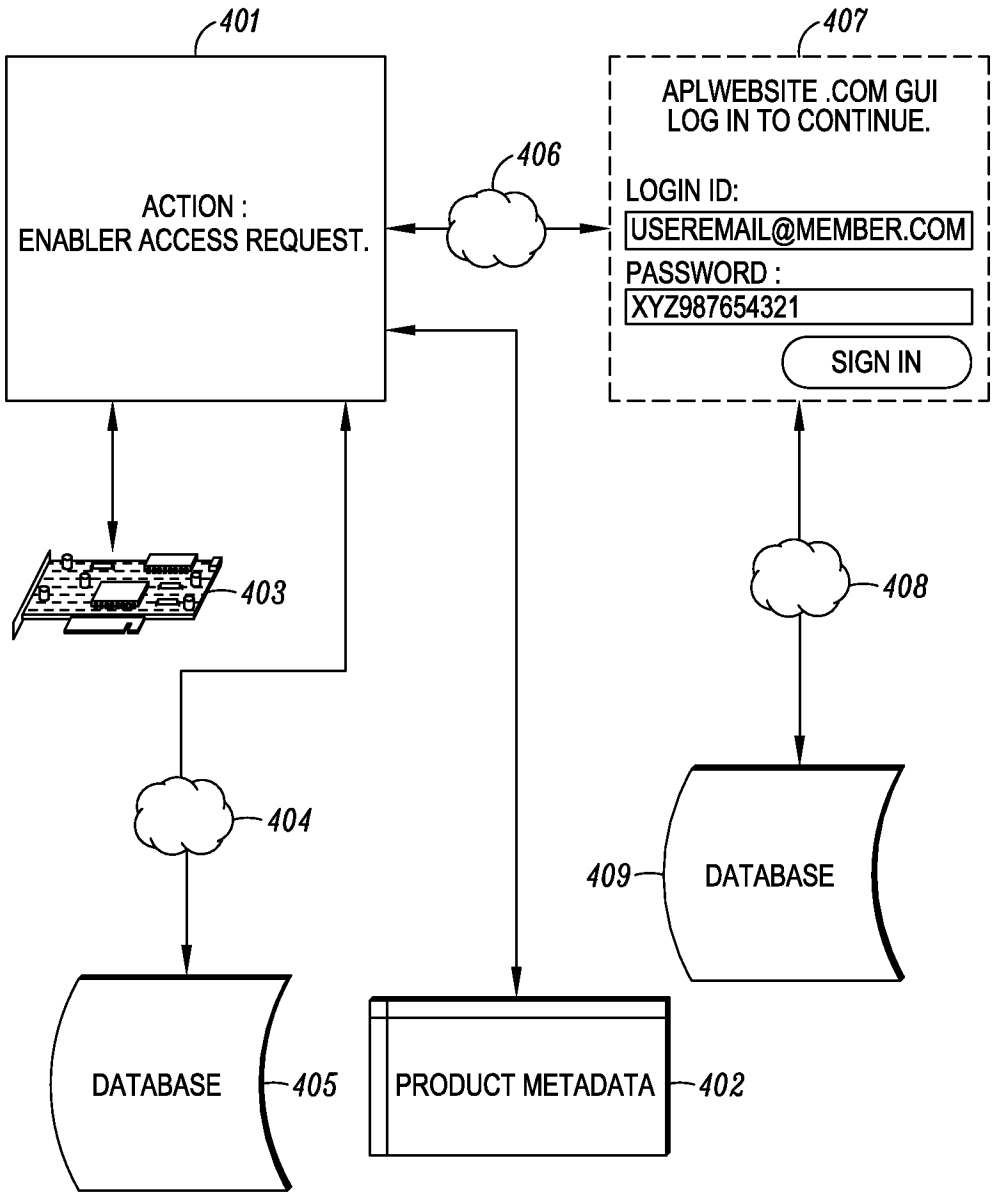

401
407
APLWEBSITE .COM GUI
LOG IN TO CONTINUE.
406
ACTION :
ENABLER ACCESS REQUEST.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
403
408
404
409
DATABASE
DATABASE
405
PRODUCT METADATA
402

FIG. 4

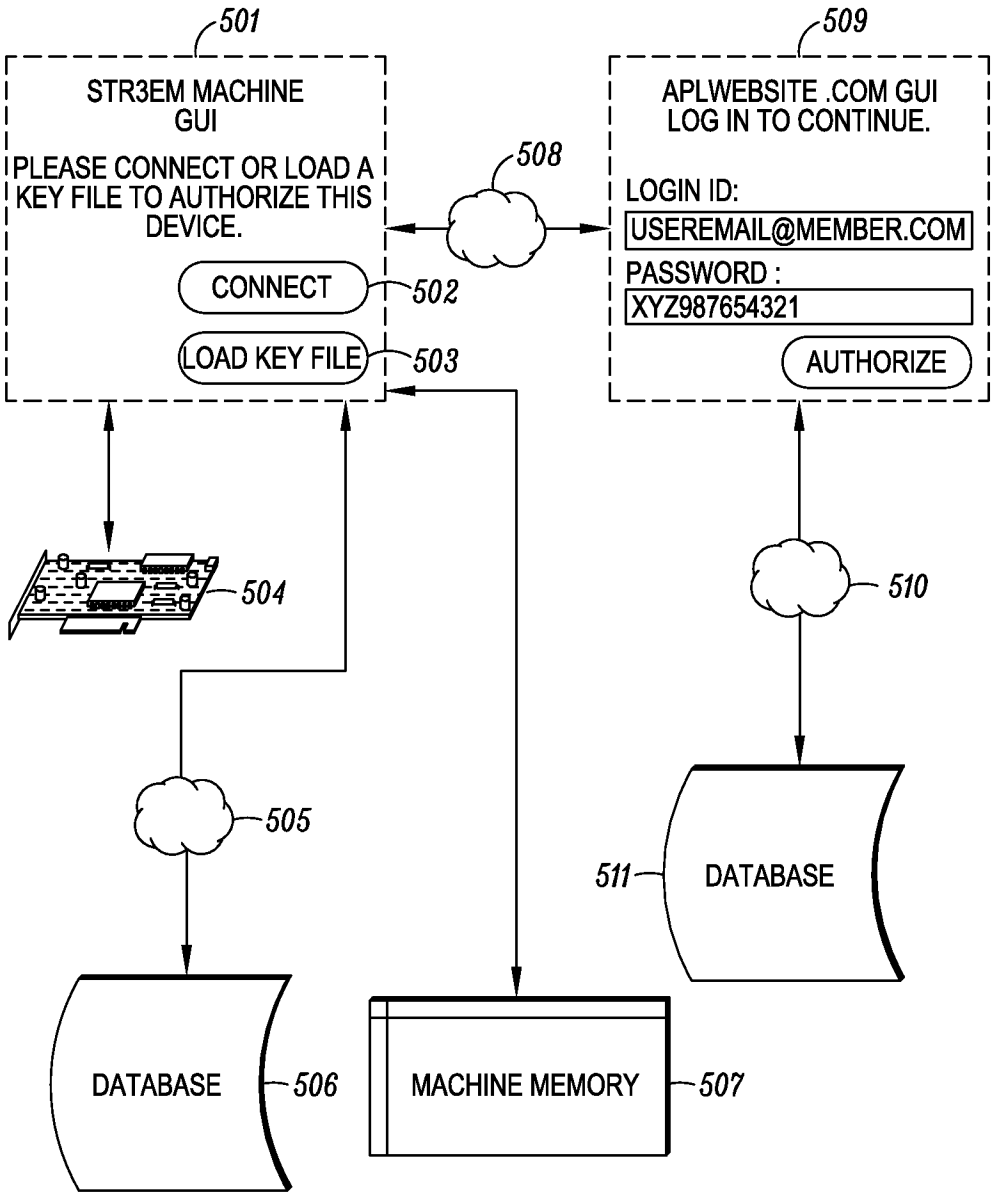

501
STR3EM MACHINE GUI
PLEASE CONNECT OR LOAD A KEY FILE TO AUTHORIZE THIS DEVICE.
CONNECT
502
LOAD KEY FILE
503
508
509
APLWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
AUTHORIZE
504
505
510
511
DATABASE
DATABASE
506
MACHINE MEMORY
507

FIG. 5

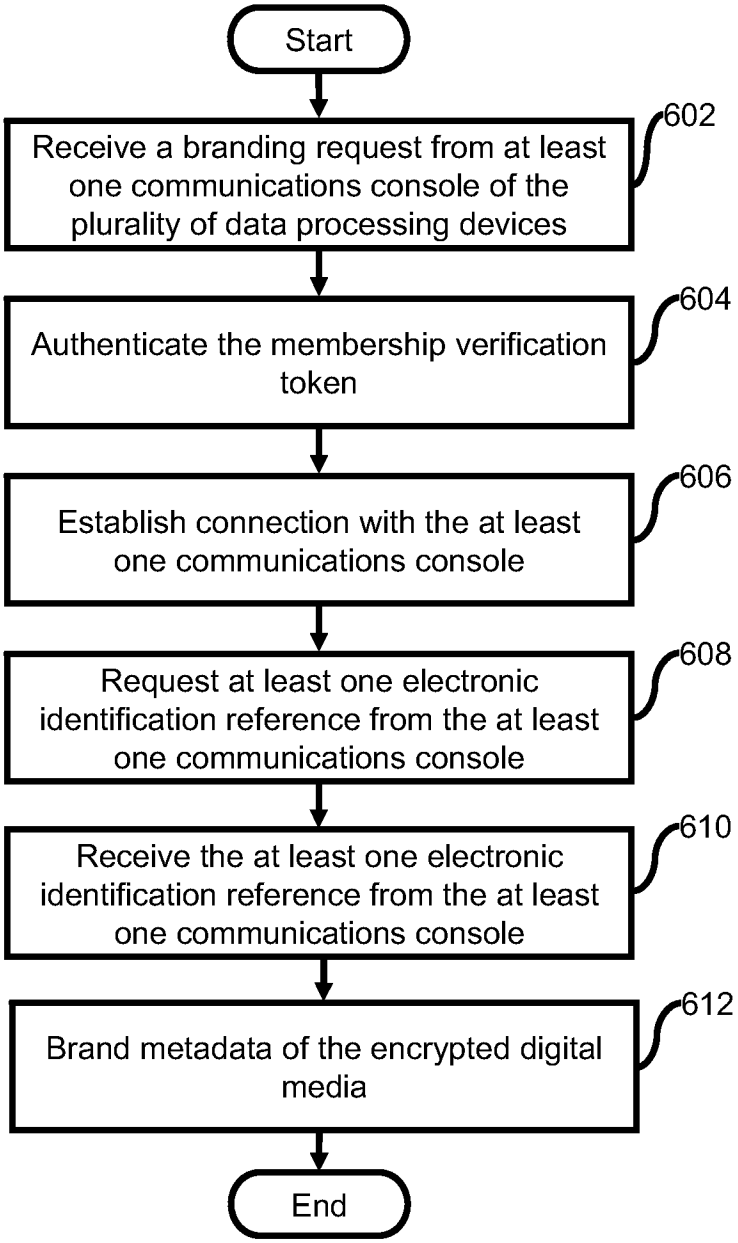

Start
Receive a branding request from at least one communications console of the plurality of data processing devices
602
Authenticate the membership verification token
604
Establish connection with the at least one communications console
606
Request at least one electronic identification reference from the at least one communications console
608
Receive the at least one electronic identification reference from the at least one communications console
610
Brand metadata of the encrypted digital media
612
End

FIG.6

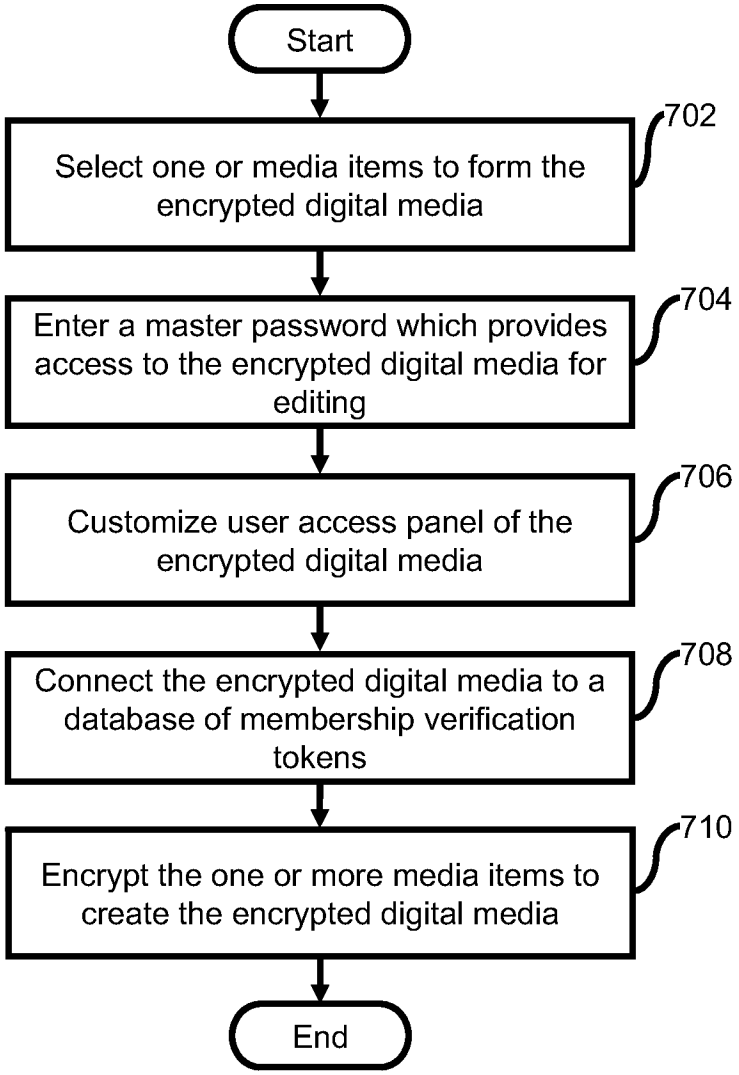

Start
Select one or media items to form the encrypted digital media
702
Enter a master password which provides access to the encrypted digital media for editing
704
Customize user access panel of the encrypted digital media
706
Connect the encrypted digital media to a database of membership verification tokens
708
Encrypt the one or more media items to create the encrypted digital media
710
End

FIG.7

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

(11) EP 1 564 621 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
16.09.2009 Bulletin 2009/38

(51) Int Cl.:
G06F 1/00 *(2006.01)*

(21) Application number: **05100667.4**

(22) Date of filing: **01.02.2005**

(54) Binding content to a domain

Zuweisung von Inhalten zu einer Domain

Association de contenus à un domaine

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR

(30) Priority: **13.02.2004 US 778743**

(43) Date of publication of application:
17.08.2005 Bulletin 2005/33

(73) Proprietor: **MICROSOFT CORPORATION**
Redmond, WA 98052 (US)

(72) Inventors:
- **Robert, Arnaud,**
  c/o Microsoft Corporation
  Redmond,
  Washington 98052 (US)
- **Knowlton, Chadd B.,**
  c/o Microsoft Corporation
  Redmond, WA 98052 (US)
- **Alkove, James A.**
  98052, Redmond (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser
Anwaltssozietät
Leopoldstrasse 4
80802 München (DE)

(56) References cited:
WO-A-03/098931

- **HEUVEL VAN DEN S A F A ET AL: "Secure Content Management in Authorised Domains" INTERNATIONAL BROADCASTING CONVENTION, 15 September 2002 (2002-09-15), pages 467-474, XP002273504**

EP 1 564 621 B1

Description

BACKGROUND OF THE INVENTION

1. The Field of the Invention

[0001] The present invention generally relates to digital rights management. More specifically, the present invention relates to digital rights management within a domain.

2. Background and Related Art

[0002] Due in part to concerns over the distribution of copyrighted digital content (such as digital audio, digital video, digital text, digital data, digital multimedia, etc.) to users for consumption, digital rights management (DRM) has become highly desirable. Typical modes of distribution of such content include tangible devices such as magnetic (floppy) disk, magnetic tape, optical (compact) disk, etc., and intangible media such as electronic bulletin boards, electronic networks, the Internet, etc. Upon being received by the user, such users consumes the content by rendering, playing or otherwise interacting with the digital content with the aid of an appropriate rendering device such as a media player, personal computer, or the like.

[0003] Typically, a content provider, or rights-owner, such as an author, publisher, broadcaster, etc. (hereinafter "content owner"), wishes to distribute such digital content to a user or a recipient in exchange for a license fee or some other consideration. Usually, content owners wish to restrict what the user can do with such distributed digital content. For example, the content owner may restrict the user from copying and re-distributing such content to a second user. Traditionally, content owners have used DRM to bind content to a specific device.

[0004] Figure 1 illustrates an example of a DRM system 100, which allows a content owner to bind content to a specific device. In general, the licensing process is initiated by the content owner encrypting content and packaging and distributing the content to consumers via the Internet, CD, or other conventional means. Consumers may then receive a license for consuming the content in accordance with the business rules defined by the content owner. As noted above, traditionally these rules have required that the content be bound to a specific device. For example, the following describes how a license may be used to bind content to a specific device in accordance with a typical DRM model.

[0005] A content owner usually encrypts and packages the content in accordance with any number of well known processes. Typically, however, the content will be packaged to include the encrypted content and a header portion that includes information to assist a device in consuming the content. Further, the packaged content may use a license acquisition URL to point to a location where a license may be acquired. Moreover, there is a number of other optional and important data which may be included within the packaged file, e.g., private signing key used to sign the content header, license key seed used to generate the key that is shared between content owner and license issuer, etc.

[0006] The content 105 may be sent to a content distributor 140 and placed on a web or file server or streaming server for distribution. Devices 130 receiving the content may then be directed to the license acquisition URL that is embedded within the header (or other areas) of the file to acquire the appropriate license 125 for consuming content 105. Before license 125 can be requested and distributed by license issuer 115, the content owner sends to the license issuer 115 the business rules and sharing of secrets 110, which typically include the seed, public key and the business rules by which a license 125 will be granted. The rules 110 define how and under what conditions licenses may be distributed to users. For example, the rules may allow for the distribution of digital content to be played only a limited number of times, only for a certain total time, only on a certain type of machine, only on a certain type of media player, only by a certain type of user, etc. In any event, the license issuer 115 should be trusted in order to ensure that licenses 125 are issued in accordance with the appropriate business rules or requirements 110 as specified by the content owner.

[0007] Device 130 may obtain the content 105 from the content distributor 140 after paying such consideration 135 as defined by the content owner when the content 105 is sent to the content distributor 140. As previously mentioned, in order to play the encrypted content 105 the device 130 must first obtain a license 125 from the license issuer 115. Device 130 may use the license acquisition URL within the header of the encrypted content 105 to determine who the license issuer 115 is in order to make a request 120 for a license 125. A request process may then be initiated which includes exchanging the content identification, information about the client computer 130 and other optional information. Based on the information received, the license issuer 115 responds with an appropriate license 125 allowing the device 130 to consume the encrypted content 105.

[0008] This license will typically include the encrypted key to decrypt the content, the specified usage rights, information about the device 130, and other information. As previously mentioned, in order to tightly control the consumption of the content 105 the license is bound to particular device or client computer 130 (e.g., the license is valid only for device 130 and content 105), and therefore the content usually can be consumed only by the specific device 130.

[0009] With competing interests of consumers, which desire the ability to consume the content on any number of devices (e.g., a desktop computer, a laptop computer, a handheld device, devices within a car or home audio/visual system/network), various mechanisms have been created to extend licenses for consuming content to a set of devices that share both content and license. Shar-

ing the same content and license on any of several devices more closely approximates the user experience for tangible media, such as a CD, which may be played on any of several devices or even loaned to another. Current solutions for extending a license to a set of devices, however, rely on individual peer devices to enforce the criteria for sharing licenses and content.

[0010] Figure 2 illustrates an example implementation of distributing content and a license within a network 200 that includes multiple devices. Initially, device 205 requests and obtains content 210 and license 220 in accordance with a procedure similar to the one described above with regard to Figure 1. Content 210 is encrypted, and license 220 binds license 220 to content 210 through a key identifier (K_ID) that is specific to content 210. Rather than binding the license to a particular device, however, license 220 includes a device ecosystem or network identification (N_ID) which may be now distributed to other devices via device 205 (or other devices within the network 200) thereby allowing content 210 to be bound to those devices within the network 200. For example, network device 225 may request from device 205 the content 210 and the license 220 for consumption. Provided that device 225 has a N_ID that matches the N_ID within license 220, device 225 is able to use license 220 to consume content 210. Similarly, device 230 may obtain the license 220 and content 210 from device 205, and subsequently distributed the license 220 and content 210 to device 235. If device 235 has obtained the appropriate N_ID the content 210 may be consumed in accordance with license 220 and in accordance with the business rules defined therein.

[0011] One of the problems associated with the aforementioned distribution of content within a network is that there is no central network service to ensure that network membership criteria are not abused. For example, a network may be limited to a specific number of devices, say four. This limitation is intended to provide a reasonable restriction on the size of the domain, given a particular license agreement. One way that the limitation on the number of device could be circumvented is to share the four licenses among a much larger group of devices. To illustrate how this might occur, consider content that is twelve minutes in length, which therefore could be played five times an hour, 120 times a day, 840 times a week, and so forth. The four device limit introduces a factor of four, meaning that the content theoretically can be played 20 times an hour, 480 times a day, 3,360 times a week, and so forth.

[0012] Of course, no matter how much four consumers like the content, as a practical matter, they will not play the content 3,360 times a week. However, it is possible for other devices to make use of the 3,360 potential plays of the content each week. In order to play the content, a device must be part of (i.e., a member of) a licensed network, but after the content is played (or at time when the content is not being played) there may not be a significant reason for a device to remain as a network member. As a result, a device may join a network for the sole purpose of playing the content and then unjoin after the content has been consumed. This process of joining and unjoining effective allows a four device domain to share licensed content among a much larger group of devices. In this example, the number of device could theoretically be as large as 3,360 over the course of a single week, which is probably a much larger group of devices than was contemplated when the four-device domain license was issued for the content. At first, sharing domain membership in this way may appear analogous to sharing a physical CD, which seems reasonable and in some aspects is desirable. However, there are practical limits on how many times a physical medium, such as a CD, can be shared over time, which simply do not manifest themselves in the context of an electronic or digital medium, such as a computer network.

[0013] Current network technology, such as network 200 in Figure 2, have not accounted for how frequently devices enter and leave the network. At least in part, this may be attributed to the lack of a centralized network service that for enforcing network membership criteria. A set of devices like network 200 also have failed to manage, and in some cases purposefully so, for the proximity of devices that make up a network. Again, analogizing to a physical media paradigm, sharing a CD typically involves at least intermittent proximity.

[0014] WO 03/098931 relates to a system and method of controlling access to a content item in a domain. Initially (in the factory), for a device, a domain_ID will be set to the device_ID, so that any individual device then could be considered as an authorized domain (AD) with a size of one device, and the device is automatically the domain originator for that AD. After a network connection to a new device has been established, authentication of the new device by the device to which it is connected is involved. If this authentication is successful, the new device becomes part of the authorized domain. An authorized domain is identified by means of a unique domain_ID. This identifier is then stored in every device that is a member of the domain. Further, digital rights associated with content inside an authorized domain are typically received together with the content as it enters the authorized domain

BRIEF SUMMARY OF THE INVENTION

[0015] It is the object of the invention to provide an improved digital rights management within a domain.

[0016] This object is solved by the present invention as claimed in the independent claims.

[0017] Preferred embodiments are defined by the dependent claims.

[0018] In accordance with exemplary embodiments of the present invention, the above-identified deficiencies and drawbacks of current digital rights management systems (DRMs) are overcome. For example, the present invention provides a rights management system that pro-

tects content from being consumed by unauthorized devices. In particular, the present invention provides for methods, systems and computer program products for enforcing digital rights within the confines of the content license used when consuming content within a domain through the validation of domain membership criteria.

[0019] Example embodiments provide for a receiving a request to create a domain, whereupon a domain identification is created that allows a content provider to uniquely bind content licenses to a domain. The content licenses include usage rights that define how content associated with the licenses may be consumed by one or more members of the domain. Thereafter, or simultaneously, the centralized domain service may receive a request from a requestor to become a member of the domain. The centralized domain service can enforce digital rights by validating membership criteria including at least one of a domain proximity check for validating that a requestor is in close proximity to the domain, a total number of requestors, or the frequency that the requests have been made by various requestors to join the domain and unjoin from the domain. Upon validation of the membership criteria, a domain certificate that includes the created domain identification is sent to the requestor.

[0020] Other example embodiments of the present invention provide for a domain identification that is sent to the requestor expires within a time period set by the centralized domain service. Thereafter, a renewal request may be received by the centralized domain service to extend the domain identification expiration time period.

[0021] In further example embodiments provide that the requestor receives a token from a domain manager, which created the domain, to send to the centralized domain service for validating that the requestor is in close proximity to the domain manager. For example, the token may include information about the time it took the requestor to receive the token, the number of intermediary nodes that the token traveled across before the requestor received the token, etc.

[0022] Additional features and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention, The features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] In order to describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0024] Figure 1 illustrates an example of a typical digital rights management system that binds content to a particular device through the distribution of a license that is device specific;

[0025] Figure 2 illustrates an example of a typical distribution of content within a domain;

[0026] Figure 3 illustrates how protected content and licenses are distributed within a domain using a centralized domain service in accordance with example embodiments of the present invention;

[0027] Figure 4 illustrates a centralized domain service and the location of a domain manager within such service in accordance with example embodiments of the present invention;

[0028] Figure 5 shows example acts and steps for methods of enforcing digital rights within a domain by validating membership criteria; and

[0029] Figure 6 illustrates an example system that provides a suitable operating environment for the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0030] The present invention extends to methods, systems, and computer program products for enforcing digital rights within a domain. The embodiments of the present invention may comprise a special purpose or general-purpose computer including various computer hardware, as discussed in greater detail below.

[0031] The present invention provides for a domain that allows more flexible content usage across a variety of devices while preventing mass re-distribution of content to, *e.g.*, the Internet. Example embodiments provide for a central domain service that is an authority capable of granting and creating the existence of a domain in accordance with certain rules, set forth or agreed to by the content provider and frequency based on business rules defined by the content owner. Content providers will require certain attributes or restrictions called member criteria for domains. For example, the membership criteria may specify the number of devices that can join a domain, the expiration of a domain (*e.g.*, a predetermined fixed time period) or individual licenses within a domain, the proximity or how close a device must be to other devices within the domain, the rate at which devices are allowed to join and unjoin, etc.

[0032] Although the consumer may choose a content provider as a function of the attributes offered, content providers and owners generally dictate at least some of the domain membership criteria consumers should meet in order to access content controlled by the providers.

Some content providers may elect to have membership criteria validated on several different centralized domain services for various purposes. For example, the content provider and/or consumers may choose a central domain service based on such things as proximity, speed, bandwidth, reliability, cost, etc. In addition, the content provider may offer varying criteria through different domain services as a function of the consideration given by the consumer. For example, a content provider may offer a consumer more devices within a domain for additional money paid by the consumer, and can therefore direct the consumer to the appropriate domain service based on the desired attributes. In any event, because of the varying domain services available, domain services are uniquely identifiable, and domains are uniquely identifiable within the scope of their domain service.

[0033] Figure 3 illustrates the distribution of content and licenses throughout a domain 300 that is controlled by a central domain service 305. Example embodiments provide for a domain manager 385 that initiates a request 320 for creating a domain 300 capable of binding content to the domain through the use of a domain identification (D_JD). Accordingly, domain manager 385 establishes a connection to the centralized domain service 305 through, *e.g.*, the Internet 315 and requests 320 a D_ID. It is noted that although Figure 3 illustrates the centralized domain service 305 as a cloud server, the centralized domain server could be a device or limited group of devices, as described in greater detail below. Accordingly, the illustration of the centralized domain service 305 as a cloud server is for illustrative purposes only and is not meant to limit or otherwise narrow the scope of the invention.

[0034] In any event, upon receipt of the request 320 for a D_ID, the central domain service 305 may grant a domain certificate 330 to the domain manager 385 of the newly created domain 300. The domain certificate 330 includes (among other information) the D_ID, which as described in greater detail below uniquely identifies (at least within the central domain service 305) the domain 300 and binds the licenses associated therewith to that particular domain 300.

[0035] Thereafter, devices associated with the domain 300 can become members by requesting 340 D_ID from the central domain service 305. For example, membership requestor 365 that now wishes to join the domain 300 will need to obtain a similar certificate 340 as received by the domain manager 385 that includes, among other things, the D_ID. Accordingly, membership requestor 365 will need to make a request 340 for the D_ID to the central domain service 305. The request 340 for the D_ID should contain, among other things, device specific information in order to bind the D_ID to the device making the request, which ensures that D_ID cannot be transferred to and used by other devices. Upon receipt of the request 340 for the D_ID, the central domain service 305 will validate that member criteria 310 defined by content provider 370 are satisfied before a certificate 345 can be issued.

[0036] In accordance with example embodiments, one of the member criteria 310 that the central domain service 305 may need to verify or validate in order to allow a device to become a member of the domain 300 is known as a "proximity" check. This criterion establishes that the device 365 making the request 340 for the D_ID is not too far removed from the domain 300. In order to satisfy this criterion, membership requestor 365 should first request to become a member 335 of the domain and make such request to domain manager 385. Domain manager 385 can then send, e.g., a token 370 to the membership requestor 365.

[0037] When membership requestor 365 now makes the request 340 for the D_ID from the central domain service 305 via, *e.g.*, the Internet 315, it 365 may include the token 370 in the request 340. The central domain service 305 will use the token 370 to ensure that membership requestor 365 is "proximally" close to domain manager 385 in accordance with the business rules defined for creating such domain 300. Such validation or verification may be in the form of determining the time that it took the token to travel from the domain manager 385 to membership requestor 365, the roundtrip time (e.g., where the domain manager 385 is part of the centralized domain service 305), the number of hops or intermediary nodes that the token traveled between domain manager 385 and membership requestor 365, etc. Of course, other well-known means of determining proximity may also be used in the validation process.

[0038] Other example embodiments provide that other membership criteria 310 may include a restriction on the number of memberships that are available. For example, the content owner may restrict the number of devices that can be in a domain at any one particular time. Alternatively, or in conjunction, the membership criteria 310 may restrict the types of devices based on the functionality of such device. For example, a first count limit may apply to devises capable of storing the content or to devices capable of distributing the content outside the domain. A second count limit may apply to devises capable of rendering the content or those devices cable of acquisitioning the content, *i.e.*, capable of brining content into the domain. Of course any number of device attributes or other considerations might be used to limit the device count, and therefore the above features for limiting the number of devices are used for illustrative purposes only and are not meant to limit or otherwise narrow the scope of the invention.

[0039] In further example embodiments, the centralized domain service may enforce digital rights by validating the velocity that membership requestors 365 join and unjoin the domain. In particular, centralized domain service 305 will check to see the frequency that one or more requests 340 have been made by various requestors 365 to join the domain and unjoin from the domain. This helps prevent large numbers of users from sharing a small number of licenses. For example, embodiments allow for

devices to join and unjoin from the domain, but may only allow for a specified number of devices to be members at any one particular time. Accordingly, without the velocity control, users could continually join and unjoin from the domain as needed to allow an overly broad number of users to become members of the domain, which would potentially circumvent the intended number of device restriction set by the content owner.

[0040] It should be noted that any number of member criteria 310 can be validated in accordance with business rules and models set forth by content owners. Accordingly, the above-identified examples of member criteria 310 are used for illustrative purposes only and are otherwise not intended to limit the present invention to just those criteria 310.

[0041] In any event, once centralized domain server 305 has validated member criteria 310 a certificate 345 can be issued to member requestor 365, which includes the D_ID that binds license 355 to the domain 300. As previously mentioned, the certificate (and thus the D_ID within the certificate) should be devices specific in order to ensure that the D_ID cannot be freely transferred between devices.

[0042] Once the membership requestor 365 has obtained the appropriate D_ID, the device 365 will be able to request 380 content and licenses from a content/license provider 370 in accordance with a similar process as that previously described regarding typical domain rights management (DRM) services. It should be noted that any device within the domain, including the domain manager 385, can obtain the content 350 and the license 355 from the content/license provider 370. In any event, the device making the request (365 in this case) should provide the D_ID within the request 380 to the content/license provider 370. The content/license provider 370 may then verify 375 the D_ID with the central domain service 305. Upon verification, the content/license provider 370 may send content 350 and license 355 to the device 365. The content is encoded and includes a key identification (K_ID), which is also included in the license 355 in order to bind the encrypted content 350 to the license 355. Further, license 355 includes the D_ID, which now binds the license 355 to the domain 300 as well as the content 350.

[0043] As discussed above, because the content is bound to the license 355, which is also bound to the D_ID, and because D_IDs are machine specific, and therefore non-transferable, the content 350 and the license 355 associated with the domain may now be freely transferred among the devices of the domain without concern of wide distribution. In other words, other devices, *e.g.*, 360, without the appropriate D_ID are unable to consume the content even if they receive content 350 and license 355 from a subsequent device, *e.g.*, 365. In order for such a device 360 to be able to consume content 350 it must go through a similar process for requesting a D_ID as previously described.

[0044] In another example embodiment, a time period expiration and renewal feature may be placed on the D_ID, certificate 345 associated with the D_ID, or both. Accordingly, in this embodiment, when the centralized domain service 305 issues the certificate 345, the time period expiration feature disables the use of the license 355, and thus consumption of content 350 when the predetermined time period has ended. Although the term "time period" is used, it is not necessarily limited to a time dependency. For example, time period is used to also include the number of times that content may be consumed, a time period to consume only small sample of the full content, an hour, day, week or any other such time restriction, etc. Accordingly, time period is used as a general term and reference only.

[0045] In any event, as mentioned above, the present invention also includes a renewal feature. Accordingly, upon expiration of the time period, i.e., when the content has been consumed a particular number of times, for a duration of time, etc., the device can make a request for renewal of D_ID or certificate. The request should be made to the central domain service 305, which can again validate membership criteria 310 and either issue another temporary or permanent certificate/D_ID.

[0046] Also related to the expiration feature, the present invention provides for a revocation of a domain ID or a specific certificate. Accordingly, the central domain service may revoke the entire domain by revoking the D_ID, or can revoke a single users (or multiple users) right to continue to be a part of the domain membership.

[0047] It is important to note that a domain manager may reside on a particular device, be spread amongst multiple devices of the domain or exist on the domain service itself depending upon the device capabilities and the trust chain between the domain service and the devices. Figure 4 illustrates various examples of where a domain manager may reside within the domain service 400 in accordance with example embodiments. As shown, domain manager 420 may reside within domain 1 (440) and service both device 1 (430) and device 2 (435). Alternatively, the domain manager 420 may be spread to multiple devices as illustrated in domain 2 (470), wherein domain manager 1 (420a) resides on device 1 (450) and domain manager 2 (420b) exits in device 2 (460). Still yet other embodiments provide that the domain manager 420 may sit on central domain service 405 as illustrated in domain 3 (490). The domain manager 420 may then service device 1 (480) and device 2 (475) within domain 3 (490).

[0048] Regardless of where the domain manager resides within a domain, devices are uniquely identifiable to the domain manager, and domains are uniquely identifiable to the domain service. Further, the present invention provides that any device can act as the domain service and/or the domain manager and the domain manager can validate membership criteria. For example, in the case where the domain manager is included in the centralized domain service, the creation or initialization of the domain (e.g., the receipt of the private/public key pair,

domain identifier, etc.) may be obtained from another centralized domain service. All other membership criteria, however, such as proximity check, limitations on total number of devices, limitations of types of devices, velocity for joining and unjoining, etc. can be performed by the domain manager.

[0049] Further example embodiments provide that the validation of membership criteria can be spread across a limited number of devices. For example, one device could be the central domain service with limited management capabilities, eg., just the domain creation. In such a case, other devices within the domain may be self-managing. In such a case, the content licenses could contain restrictions with respect to playback that could include, e.g., a number of devices or a list of devices that can join the domain. Accordingly, one device could only send domain certificate, license, content, or any combination thereof, to another device if the latter is on the list or according to some other criteria.

[0050] Other example embodiments provide that the domain service can revoke a domain and a domain manager can revoke a member device. Further, a domain manager is capable of managing more than one domain at a time. Moreover, the domain may be self-managed, in that it does not require a permanent administrator to maintain it.

[0051] Still yet other embodiments of the present invention provide that the device may become a member of more than one domain. Typically, however, if a device acquires a second domain identification, the first domain identification or previous domain identifications are temporarily disabled. Accordingly, even though a device may contain more than one domain identification, the device is bound to only one particular domain at any given time.

[0052] The present invention may also be described in terms of methods comprising functional steps and/or non-functional acts. The following is a description of acts and steps that may be performed in practicing the present invention. Usually, functional steps describe the invention in terms of results that are accomplished, whereas non-functional acts describe more specific actions for achieving particular results. Although the functional steps and non-functional acts may be described or claimed in a particular order, the present invention is not necessarily limited to any particular ordering or combination of acts and/or steps.

[0053] Figure 5 illustrates example steps and acts used in a rights management system that protects content from being consumed by unauthorized devices. Methods and computer program products for implementing such methods enforce digital rights within the confines of a content license used when consuming content within a domain by validating domain membership criteria. For example, a step for binding 530 content licenses to a domain may include the act of receiving 510 a request to create a domain. Further, the step for binding 530 may include the act of creating 520 a domain identification that allows a content provider to uniquely bind content licenses to a domain. The content licenses will comprise the usage rights that define how content associated with the license may be consumed by members of the domain.

[0054] A step for validating 560 domain membership criteria may include the act of receiving 540 a request, by a requestor, to become a member of the domain. The request may be received at the centralized domain service and may include a way of validating the proximity of the requestor within the domain. For example, the requestor could request a token from a domain manager, which requested the creation of the domain, and subsequently send the token to the centralized domain service for validating that the requestor is in close proximity to the domain. The token may include information about the time it took the requestor to receive the token, round trip time (e.g., in the case where the domain manager is included in the centralized domain service), or the number of intermediary nodes that the token traveled across before the requestor received the token, or both.

[0055] The step for validating 560 domain membership criteria may also include the enforcement 550 of digital rights at the centralized domain service by validating the at least one of a total number of requestors or the frequency that one or more requests have been made by various requestors to join the domain or unjoin from the domain, or both. Upon validation of the domain membership criteria, the centralized domain service may send a domain certificate that includes the created domain identification to the requestor.

[0056] The domain identification may include an expiration time period sent by the centralized domain service in accordance with rules established by the content owner. Subsequently, the centralized domain service may receive a renewal request to extend the domain identification expiration time period. Other embodiments also provide that the centralized domain service may revoke the domain identification or domain membership for one or more members of a particular domain.

[0057] Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media that can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium.

Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

[0058] Figure 6 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by computers in network environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of the program code means for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps.

[0059] Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination of hardwired or wireless links) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0060] With reference to Figure 6, an example system for implementing the invention includes a general purpose computing device in the form of a conventional computer 620, including a processing unit 621, a system memory 622, and a system bus 623 that couples various system components including the system memory 622 to the processing unit 621. The system bus 623 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 624 and random access memory (RAM) 625. A basic input/output system (BIOS) 626, containing the basic routines that help transfer information between elements within the computer 620, such as during start-up, may be stored in ROM 624.

[0061] The computer 620 may also include a magnetic hard disk drive 627 for reading from and writing to a magnetic hard disk 639, a magnetic disk drive 628 for reading from or writing to a removable magnetic disk 629, and an optical disc drive 630 for reading from or writing to removable optical disc 631 such as a CD-ROM or other optical media. The magnetic hard disk drive 627, magnetic disk drive 628, and optical disc drive 630 are connected to the system bus 623 by a hard disk drive interface 632, a magnetic disk drive-interface 633, and an optical drive interface 634, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer-executable instructions, data structures, program modules and other data for the computer 620. Although the exemplary environment described herein employs a magnetic hard disk 639, a removable magnetic disk 629 and a removable optical disc 631, other types of computer readable media for storing data can be used, including magnetic cassettes, flash memory cards, digital versatile discs, Bernoulli cartridges, RAMs, ROMs, and the like.

[0062] Program code means comprising one or more program modules may be stored on the hard disk 639, magnetic disk 629, optical disc 631, ROM 624 or RAM 625, including an operating system 635, one or more application programs 636, other program modules 637, and program data 638. A user may enter commands and information into the computer 620 through keyboard 640, pointing device 642, or other input devices (not shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 621 through a serial port interface 646 coupled to system bus 623. Alternatively, the input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 847 or another display device is also connected to system bus 623 via an interface, such as video adapter 648. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

[0063] The computer 620 may operate in a networked environment using logical connections to one or more remote computers, such as remote computers 649a and 649b. Remote computers 649a and 649b may each be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically include many or all of the elements described above relative to the computer 620, although only memory storage devices 650a and 650b and their associated application programs 636a and 636b have been illustrated in Figure 6. The logical connections depicted in Figure 6 include a local area network (LAN) 651 and a wide area network (WAN) 652 that are presented here by way of example and not limitation. Such networking environments are commonplace in office-wide or enterprise-wide computer networks, intranets and the Internet.

[0064] When used in a LAN networking environment, the computer 620 is connected to the local network 651 through a network interface or adapter 653. When used in a WAN networking environment, the computer 620 may include a modem 654, a wireless link, or other means

for establishing communications over the wide area network 652, such as the Internet. The modem 654, which may be internal or external, is connected to the system bus 623 via the serial port interface 646. In a networked environment, program modules depicted relative to the computer 620, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing communications over wide area network 652 may be used.

[0065] The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description.

Claims

1. A method in a rights management system that protects content (350) from being consumed by unauthorized devices (360), the method of enforcing digital rights within the confines of a content license used when consuming content within a domain by validating domain membership criteria, the method comprising acts of:

   receiving (510), at a centralized domain service (305, 405), a request (320) to create a domain (440, 470, 490);
   creating (520) a domain identification that allows a content provider (370) to include the domain identification in a content license (355) to uniquely bind content licenses to a domain, the content licenses comprising one or more usage rights that define how content associated with the licenses may be consumed by one or more members (365, 430, 435, 450, 460, 475, 480) of the domain;
   requesting, by the requestor, a token (370) from a domain manager (385, 420), which requested the creation of the domain, to send to the centralized domain service for validating that the requestor is in close proximity to the domain manager, the token including information about the time it took the requestor to receive the token, or the number of intermediary nodes that the token traveled across before the requestor received the token, or both;
   receiving (540), at the centralized domain service, a request (340) including the token, to become a member of the domain by a requestor;
   enforcing (550) digital rights by validating, at the centralized domain service, domain membership criteria (310) including a domain proximity check for validating that the requestor is in close proximity to the domain; and
   upon validation of the domain membership criteria, sending a domain certificate (345) that includes the created domain identification to the requestor.

2. The method of claim 1, wherein the domain identification expires within a time period set by the centralized domain service.

3. The method of claim 2, further comprising the acts of:

   receiving, at the centralized domain service, a renewal request to extend the domain identification expiration time period.

4. The method of claim 1, wherein the domain membership criteria further includes at least one of a total number of requestors or the frequency of requests made by one or more requestors to join the domain and unjoin from the domain.

5. The method of claim 1, wherein the centralized domain service includes the domain manager, and wherein the domain manager requested the creation of the domain from a centralized domain server, which created the domain identification.

6. The method of claim 1, wherein the requestor becomes a domain manager, and wherein a device requests a token from the requestor.

7. The method of claim 1, wherein the requestor becomes a member of a second domain.

8. The method of claim 1, wherein the domain manager receives one or more requests for tokens for a second domain.

9. The method of claim 1, wherein the centralized domain service revokes the domain identification.

10. The method of claim 1, wherein validating comprises validating the domain membership criteria when receiving the request by the requestor and before allowing the domain certificate to be sent to the requestor, wherein the domain identification further includes a time stamp that expires the domain identification within a time period set by the centralized domain service.

11. The method of claim 10, further comprising the acts of:

    receiving, at the centralized domain service, a renewal request to extend the domain identification expiration time period.

12. The method of claim 10, wherein the domain membership criteria further includes at least one of a total number of requestors or the frequency of requests made by one or more requestors to join the domain and unjoin from the domain.

13. The method of claim 12, wherein the centralized domain service includes the domain manager.

14. The method of claim 12, wherein the requestor becomes a domain manager, and wherein a device requests a token from the requestor.

15. The method of claim 12, wherein the requestor becomes a member of a second domain.

16. The method of claim 12, wherein the domain manager receives a request for one or more tokens for a second domain.

17. The method of claim 10, wherein the centralized domain service revokes the domain identification.

18. A computer program product in a rights management system that protects content (350) from being consumed by unauthorized devices (360), the computer program product comprising one or more computer readable media carrying computer executable instructions that implement a method of enforcing digital rights within the confines of a content license used when consuming content within a domain by validating domain membership criteria, the method comprising acts of:

receiving (510), at a centralized domain service (305, 405), a request (320) to create a domain (440, 470, 490);
creating (520) a domain identification that allows a content provider (370) to include the domain identification in a content license (355) to uniquely bind content licenses to a domain, the content licenses comprising one or more usage rights that define how content associated with the licenses may be consumed by one or more members (365, 430, 435, 450, 460, 475, 480) of the domain;
requesting, by the requestor, a token (370) from a domain manager (385, 420), which requested the creation of the domain, to send to the centralized domain service for validating that the requestor is in close proximity to the domain manager, the token including information about the time it took the requestor to receive the token, or the number of intermediary nodes that the token traveled across before the requestor received the token, or both;
receiving (540), at the centralized domain service, a request (340) including the token, to become a member of the domain by a requestor;
enforcing (550) digital rights by validating, at the centralized domain service, domain membership criteria (310) including a domain proximity check for validating that a requestor is in close proximity to the domain; and
upon validation of the domain membership criteria, sending a domain certificate (345) that includes the created domain identification to the requestor.

19. The computer program product of claim 18, wherein the domain identification includes a time stamp that expires the domain identification within a time period set by the centralized domain service.

20. The computer program product of claim 19, further comprising the acts of:

receiving, at the centralized domain service, a renewal request to extend the domain identification expiration time period.

21. The computer program product of claim 18, wherein the domain membership criteria further includes at least one of a total number of requestors or the frequency of requests made by one or more requestors to join the domain and unjoin from the domain.

22. The computer program product of claim 18, wherein the centralized domain service includes the domain manager.

23. The computer program product of claim 18, wherein the requestor becomes a domain manager, and wherein a device requests a token from the requestor.

24. The computer program product of claim 18, wherein the requestor becomes a member of a second domain.

25. The computer program product of claim 18, wherein the domain manager receives one or more requests for tokens for a second domain.

26. The computer program product of claim 18, wherein the centralized domain service revokes the domain identification.

27. The computer program product of claim 21, wherein validating comprises validating the domain membership criteria when receiving the request by the requestor and before allowing the domain certificate to be sent to the requester.

28. The computer program product of claim 27, wherein the domain identification expires within a time period

set by the centralized domain service.

29. The computer program product of claim 28, further comprising the acts of:

receiving, at the centralized domain service, a renewal request to extend the domain identification expiration time period.

30. The computer program product of claim 27, wherein the centralized domain service includes the domain manager, and wherein the domain manager requested the creation of the domain from a centralized domain server, which created the domain identification.

31. The computer program product of claim 27, wherein the requestor becomes a domain manager, and wherein a device requests a token from the requestor.

32. The computer program product of claim 27, wherein the requestor becomes a member of a second domain.

33. The computer program product of claim 27, wherein the domain manager receives one or more requests for tokens for a second domain.

34. The computer program product of claim 27, wherein the centralized domain service revokes the domain identification.

Patentansprüche

1. Verfahren in einem Rechteverwaltungssystem, das einen Inhalt (350) vor einer Verwendung durch nicht autorisierte Vorrichtungen (360) schützt, wobei das Verfahren dazu dient, digitale Rechte innerhalb der Grenzen einer Inhaltslizenz geltend zu machen, die eingesetzt wird, wenn ein Inhalt innerhalb einer Domäne verwendet wird, indem Domänen-Mitgliedschaftskriterien bestätigt werden, und das Verfahren die folgenden Vorgänge umfasst:

Empfangen (510) einer Anforderung (320), eine Domäne (440, 470, 490) zu schaffen, bei einem zentralen Domänen-Dienst (305, 405);
Schaffen (520) einer Domänen-Identifikation, die es einem Inhaltsanbieter (content provider) (370) erlaubt, die Domänen-Kennung in eine Inhaltslizenz (355) zu integrieren, um so Inhaltslizenzen eindeutig an eine Domäne zu binden, wobei die Inhaltslizenzen ein oder mehrere Nutzungsrecht/e umfassen, das/die definiert/definieren, wie ein mit den Lizenzen zusammenhängender Inhalt von einem oder mehreren Mitgliedern (365, 430, 435, 450, 460, 475, 480) der Domäne verwendet werden kann;
Anfordern eines Token (370) von einem Domänen-Manager (385, 420) durch den Anfordernden, der die Schaffung der Domäne angefordert hat, zum Senden zu dem zentralen Domänen-Dienst, um zu bestätigen, dass sich der Anfordernde in enger Nähe zu dem Domänen-Manager befindet, wobei das Token Informationen über die Zeit, die bis zum Empfangen des Token durch den Anfordernden benötigt wurde, oder die Anzahl von Zwischenknoten, die das Token durchlief, bevor der Anfordernde das Token empfing, oder beide enthält;
Empfangen (540) einer das Token einschließenden Anforderung (340) des Anfordernden, ein Mitglied der Domäne zu werden, an dem zentralen Domänen-Dienst;
Geltendmachen (550) digitaler Rechte durch Bestätigen von Domänen-Mitgliedschaftskriterien (310) an dem zentralen Domänen-Dienst, die eine Prüfung der Nähe zur Domäne einschließen, um zu bestätigen, dass sich der Anfordernde in enger Nähe zu der Domäne befindet; und
nach Bestätigung der Domänen-Mitgliedschaftskriterien Senden eines Domänen-Zertifikats (345), das die erzeugte Domänen-Kennung enthält, zu dem Anfordernden.

2. Verfahren nach Anspruch 1, wobei die Domänen-Kennung innerhalb eines Zeitraums abläuft, der durch den zentralen Domänen-Dienst festgelegt wird.

3. Verfahren nach Anspruch 2, das des Weiteren die folgenden Vorgänge umfasst:

Empfangen einer Erneuerungsanforderung zum Verlängern des Ablaufzeitraums für die Domänen-Kennung bei dem zentralen Domänen-Dienst.

4. Verfahren nach Anspruch 1, wobei die Domänen-Mitgliedschaftskriterien des Weiteren wenigstens eine Gesamtzahl von Anfordernden oder die Häufigkeit einschließen, mit der Anforderungen zum Beitreten zu der Domäne und Verlassen der Domäne durch einen oder mehrere Anfordernde/n gestellt werden.

5. Verfahren nach Anspruch 1, wobei der zentrale Domänen-Dienst den Domänen-Manager einschließt, und der Domänen-Manager die Schaffung der Domäne von einem zentralen Domänen-Server angefordert hat, der die Domänen-Kennung erzeugt hat.

6. Verfahren nach Anspruch 1, wobei der Anfordernde zu einem Domänen-Manager wird und eine Vorrich-

tung ein Token von dem Anfordernden anfordert.

7. Verfahren nach Anspruch 1, wobei der Anfordernde ein Mitglied einer zweiten Domäne wird.

8. Verfahren nach Anspruch 1, wobei der Domänen-Manager eine oder mehrere Anforderung/en von Token für eine zweite Domäne empfängt.

9. Verfahren nach Anspruch 1, wobei der zentrale Domänen-Dienst die Domänen-Kennung zurückzieht.

10. Verfahren nach Anspruch 1, wobei Bestätigen umfasst, dass die Domänen-Mitgliedschaft bestätigt wird, wenn die Anforderung des Anfordernden empfangen wird und bevor zugelassen wird, dass das Domänen-Zertifikat zu dem Anfordernden gesendet wird, und die Domänen-Kennung des Weiteren einen Zeitstempel enthält, durch den die Domänen-Kennung innerhalb eines Zeitraums abläuft, der durch den zentralen Domänen-Dienst festgelegt wird.

11. Verfahren nach Anspruch 10, das des Weiteren die folgenden Vorgänge umfasst:

    Empfangen einer Erneuerungsanforderung zum Verlängern des Ablaufzeitraums für die Domänen-Kennung bei dem zentralen Domänen-Dienst.

12. Verfahren nach Anspruch 10, wobei die Domänen-Mitgliedschaftskriterien des Weiteren wenigstens eine Gesamtzahl von Anfordernden oder die Häufigkeit einschließen, mit der Anforderungen zum Beitreten zu der Domäne und Verlassen der Domäne durch einen oder mehrere Anfordernde/n gestellt werden.

13. Verfahren nach Anspruch 12, wobei der zentrale Domänen-Dienst den Domänen-Manager einschließt.

14. Verfahren nach Anspruch 12, wobei der Anfordernde zu einem Domänen-Manager wird und eine Vorrichtung ein Token von dem Anfordernden anfordert.

15. Verfahren nach Anspruch 12, wobei der Anfordernde ein Mitglied einer zweiten Domäne wird.

16. Verfahren nach Anspruch 12, wobei der Domänen-Manager eine Anforderung eines oder mehrerer Token für eine zweite Domäne empfängt.

17. Verfahren nach Anspruch 10, wobei der zentrale Domänen-Dienst die Domänen-Kennung zurückzieht.

18. Computerprogrammerzeugnis in einem Rechteverwaltungssystem, das einen Inhalt (350) vor einer Verwendung durch nicht autorisierte Vorrichtungen (360) schützt, wobei das Computerprogrammerzeugnis ein oder mehrere computerlesbare Medien umfasst, die durch Computer ausführbare Befehle aufweisen, die ein Verfahren implementieren, mit dem digitale Rechte innerhalb der Grenzen einer Inhaltslizenz geltend gemacht werden, die eingesetzt wird, wenn ein Inhalt innerhalb einer Domäne verwendet wird, indem Domänen-Mitgliedschaftskriterien bestätigt werden, wobei das Verfahren die folgenden Vorgänge umfasst:

    Empfangen (510) einer Anforderung (320), eine Domäne (440, 470, 490) zu schaffen, bei einem zentralen Domänen-Dienst (305, 405);
    Schaffen (520) einer Domänen-Identifikation, die es einem Inhaltsanbieter (content provider) (370) erlaubt, die Domänen-Kennung in eine Inhaltslizenz (355) zu integrieren, um so Inhaltslizenzen eindeutig an eine Domäne zu binden, wobei die Inhaltslizenzen ein oder mehrere Nutzungsrecht/e umfassen, das/die definiert/definieren, wie mit den Lizenzen zusammenhängender Inhalt in einem oder mehreren Mitgliedern (365, 430, 435, 450, 460, 475, 480) der Domäne verwendet werden kann;
    Anfordern eines Token (370) von einem Domänen-Manager (385, 420) durch den Anfordernden, der die Schaffung der Domäne angefordert hat, zum Senden zu dem zentralen Domänen-Dienst, um zu bestätigen, dass sich der Anfordernde in enger Nähe zu dem Domänen-Manager befindet, wobei das Token Informationen über die Zeit, die bis zum Empfangen des Token durch den Anfordernden benötigt wurde, oder die Anzahl von Zwischenknoten, die das Token durchlief, bevor der Anfordernde das Token empfing, oder beide enthält;
    Empfangen (540) einer das Token einschließenden Anforderung (340) des Anfordernden, ein Mitglied der Domäne zu werden, an dem zentralen Domänen-Dienst;
    Geltendmachen (550) digitaler Rechte durch Bestätigen von Domänen-Mitgliedschaftskriterien (310) an dem zentralen Domänen-Dienst, die eine Prüfung der Nähe zur Domäne einschließen, um zu bestätigen, dass sich der Anfordernde in enger Nähe zu der Domäne befindet; und
    nach Bestätigung der Domänen-Mitgliedschaftskriterien Senden eines Domänen-Zertifikats (345), das die erzeugte Domänen-Kennung enthält, zu dem Anfordernden.

19. Computerprogrammerzeugnis nach Anspruch 18, wobei die Domänen-Kennung einen Zeitstempel enthält, durch den die Domänen-Kennung innerhalb eines Zeitraums abläuft, der durch den zentralen Do-

mänen-Dienst festgelegt wird.

20. Computerprogrammerzeugnis nach Anspruch 19, das des Weiteren die folgenden Vorgänge umfasst:

Empfangen einer Erneuerungsanforderung zum Verlängern des Ablaufzeitraums der Domänen-Kennung bei dem zentralen Domänen-Dienst.

21. Computerprogrammerzeugnis nach Anspruch 18, wobei die Domänen-Mitgliedschaftskriterien des Weiteren wenigstens eine Gesamtzahl von Anfordernden oder die Häufigkeit einschließen, mit der Anforderungen zum Beitreten der Domäne und Verlassen der Domäne durch einen oder mehrere Anfordernde/n gestellt werden.

22. Computerprogrammerzeugnis nach Anspruch 18, wobei der zentrale Domänen-Dienst den Domänen-Manager einschließt.

23. Computerprogrammerzeugnis nach Anspruch 18, wobei der Anfordernde zu einem Domänen-Manager wird und eine Vorrichtung ein Token von dem Anfordernden anfordert.

24. Computerprogrammerzeugnis nach Anspruch 18, wobei der Anfordernde ein Mitglied einer zweiten Domäne wird.

25. Computerprogrammerzeugnis nach Anspruch 18, wobei der Domänen-Manager eine oder mehrere Anforderung/en von Token für eine zweite Domäne empfängt.

26. Computerprogrammerzeugnis nach Anspruch 18, wobei der zentrale Domänen-Dienst die Domänen-Kennung zurückzieht.

27. Computerprogrammerzeugnis nach Anspruch 21, wobei Bestätigen umfasst, dass die Domänen-Mitgliedschaftskriterien bestätigt werden, wenn die Anforderung des Anfordernden empfangen wird und bevor zugelassen wird, dass das Domänen-Zertifikat zu dem Anfordernden gesendet wird.

28. Computerprogrammerzeugnis nach Anspruch 27, wobei die Domänen-Kennung innerhalb eines Zeitraums abläuft, der durch den zentralen Domänen-Dienst festgelegt wird.

29. Computerprogrammerzeugnis nach Anspruch 28, das des Weiteren die folgenden Vorgänge umfasst.

Empfangen einer Erneuerungsanforderung zum Verlängern des Ablaufzeitraums der Domänen-Kennung bei dem zentralen Domänen-Dienst.

30. Computerprogrammerzeugnis nach Anspruch 27, wobei der zentrale Domänen-Dienst den Domänen-Manager einschließt und der Domänen-Manager die Schaffung der Domäne von einem zentralen Domänen-Server angefordert hat, der die Domänen-Kennung erzeugt hat.

31. Computerprogrammerzeugnis nach Anspruch 27, wobei der Anfordernde zu einem Domänen-Manager wird und eine Vorrichtung ein Token von dem Anfordernden anfordert.

32. Computerprogrammerzeugnis nach Anspruch 27, wobei der Anfordernde ein Mitglied einer zweiten Domäne wird.

33. Computerprogrammerzeugnis nach Anspruch 27, wobei der Domänen-Manager eine oder mehrere Anforderungen von Token für eine zweite Domäne empfängt.

34. Computerprogrammerzeugnis nach Anspruch 27, wobei der zentrale Domänen-Dienst die Domänen-Kennung zurückzieht.

Revendications

1. Procédé intégré dans un système de gestion de droits, destiné à protéger un contenu (350) vis-à-vis d'une exploitation par des dispositifs non autorisés (360), le procédé étant destiné à appliquer des droits numériques dans les limites d'une licence de contenu utilisée lors de l'exploitation d'un contenu appartenant à un domaine, en validant des critères d'appartenance à un domaine, le procédé comportant :

de réception (510), au niveau d'un service de domaines centralisé (305, 405), d'une demande (320) de création d'un domaine (440, 470, 490) ; de création (520) d'une identification de domaine qui permet à un fournisseur de contenus (370) d'inclure l'identification de domaine dans une licence de contenu (355) pour lier de manière unique les licences de contenu à un domaine, les licences de contenu comportant un ou plusieurs droits d'utilisation qui définissent les modalités d'exploitation des contenus associés aux licences par un ou plusieurs membres (365, 430, 435, 450, 460, 475, 480) du domaine ; de demande, par l'intermédiaire du demandeur, d'un jeton (370) auprès d'un gestionnaire de domaine (385, 420), qui a demandé la création du domaine, d'envoyer au service de domaines centralisé pour valider que le demandeur se trouve à proximité du gestionnaire de domaine,

le jeton contenant des informations concernant le temps nécessaire au demandeur pour recevoir le jeton, ou le nombre de noeuds intermédiaires parcourus par le jeton avant sa réception par le demandeur, ou les deux ;
de réception (540), au niveau du service de domaines centralisé, d'une demande (340) contenant le jeton, effectuée par le demandeur pour devenir un membre du domaine ;
d'application (550) des droits numériques en validant, au niveau du service de domaines centralisé, des critères d'appartenance au domaine (310) comportant une vérification de proximité vis-à-vis du domaine pour valider que le demandeur se trouve à proximité du domaine ; et
après validation des critères d'appartenance au domaine, d'adressage au demandeur d'un certificat de domaine (345) qui inclut l'identification du domaine créé.

2. Procédé selon la revendication 1, dans lequel l'identification de domaine expire au-delà d'un délai fixé par le service de domaines centralisé.

3. Procédé selon la revendication 2, comportant en outre:

la réception, au niveau du service de domaines centralisé, d'une demande de renouvellement pour étendre le délai d'expiration d'identification de domaine.

4. Procédé selon la revendication 1, dans lequel le critère d'appartenance au domaine comporte en outre au moins l'un d'un nombre total de demandeurs ou la fréquence des demandes pour rejoindre le domaine ou quitter le domaine, effectuées par un ou plusieurs demandeurs.

5. Procédé selon la revendication 1, dans lequel le service de domaines centralisé inclut le gestionnaire de domaine, dans lequel le gestionnaire de domaine a demandé la création du domaine à partir d'un serveur de domaines centralisé qui a créé l'identification de domaine.

6. Procédé selon la revendication 1, dans lequel le demandeur devient un gestionnaire de domaine et dans lequel un dispositif demande un jeton auprès du demandeur.

7. Procédé selon la revendication 1, dans lequel le demandeur devient un membre d'un second domaine.

8. Procédé selon la revendication 1, dans lequel le gestionnaire de domaine reçoit une ou plusieurs demandes de jeton pour un second domaine.

9. Procédé selon la revendication 1, dans lequel le service de domaines centralisé révoque l'identification de domaine.

10. Procédé selon la revendication 1, dans lequel la validation comporte la validation des critères d'appartenance à un domaine à réception de la demande par le demandeur et avant d'autoriser l'envoi du certificat de domaine au demandeur, dans lequel l'identification de domaine comporte en outre un horodatage d'expiration de l'identification de domaine dans un délai fixé par le service de domaines centralisé.

11. Procédé selon la revendication 10, comportant en outre:

la réception, au niveau du service de domaines centralisé, d'une demande de renouvellement pour étendre le délai d'expiration d'identification de domaine.

12. Procédé selon la revendication 10, dans lequel les critères d'appartenance au domaine comportent en outre au moins l'un d'un nombre total de demandeurs ou la fréquence de demandes effectuées par un ou plusieurs demandeurs pour rejoindre le domaine ou quitter le domaine.

13. Procédé selon la revendication 12, dans lequel le service de domaines centralisé inclut le gestionnaire de domaine.

14. Procédé selon la revendication 12, dans lequel le demandeur devient un gestionnaire de domaine et dans lequel un dispositif demande un jeton auprès du demandeur.

15. Procédé selon la revendication 12, dans lequel le demandeur devient un membre d'un second domaine.

16. Procédé selon la revendication 12, dans lequel le gestionnaire de domaine reçoit une demande pour un ou plusieurs jetons concernant un second domaine.

17. Procédé selon la revendication 10, dans lequel le service de domaines centralisé révoque l'identification de domaine.

18. Produit de programme informatique intégré dans un système de gestion de droits, destiné à protéger un contenu (350) vis-à-vis d'une exploitation par des dispositifs non autorisés (360), le produit de programme informatique comportant un ou plusieurs supports lisibles par ordinateur, contenant des instructions exécutables par ordinateur, permettant de mettre en oeuvre un procédé destiné à appliquer des

droits numériques dans les limites d'une licence de contenu utilisée lors de l'exploitation d'un contenu appartenant à un domaine en validant des critères d'appartenance à un domaine, le procédé comportant:

la réception (510), au niveau d'un service de domaines centralisé (305, 405), d'une demande (320) de création d'un domaine (440, 470, 490) ;
la création (520) d'une identification de domaine qui permet à un fournisseur de contenus (370) d'inclure l'identification de domaine dans une licence de contenu (355) pour lier de manière unique les licences de contenu à un domaine, les licences de contenu comportant un ou plusieurs droits d'utilisation qui définissent les modalités d'exploitation de contenus associés aux licences par un ou plusieurs membres (365, 430, 435, 450, 460, 475, 480) du domaine ;
la demande, par l'intermédiaire du demandeur, d'un jeton (370) auprès d'un gestionnaire de domaine (385, 420), qui a demandé la création du domaine, d'envoyer au service de domaines centralisé pour valider que le demandeur se trouve à proximité du gestionnaire de domaine, le jeton contenant des informations concernant le temps nécessaire au demandeur pour recevoir le jeton, ou le nombre de noeuds intermédiaires parcourus par le jeton avant sa réception par le demandeur, ou les deux ;
la réception (540), au niveau du service de domaines centralisé, d'une demande (340) contenant le jeton, effectuée par le demandeur pour devenir un membre du domaine ;
l'application (550) des droits numériques en validant, au niveau du service de domaines centralisé, des critères d'appartenance au domaine (310) comportant une vérification de proximité vis-à-vis du domaine pour valider que le demandeur se trouve à proximité du domaine ; et
après validation des critères d'appartenance au domaine, l'émission d'un certificat de domaine (345) qui inclut l'identification du domaine créé vis-à-vis du demandeur.

19. Produit de programme informatique selon la revendication 18, dans lequel l'identification de domaine inclut un horodatage d'expiration de l'identification de domaine dans un délai fixé par le service de domaines centralisé.

20. Produit de programme informatique selon la revendication 19, comportant en outre :

la réception, au niveau du service de domaines centralisé, d'une demande de renouvellement pour étendre le délai d'expiration d'identification de domaine.

21. Produit de programme informatique selon la revendication 18, dans lequel les critères d'appartenance au domaine comportent en outre au moins l'un d'un nombre total de demandeurs ou la fréquence des demandes pour rejoindre le domaine ou quitter le domaine effectuées par un ou plusieurs demandeurs.

22. Produit de programme informatique selon la revendication 18, dans lequel le service de domaines centralisé inclut le gestionnaire de domaine.

23. Produit de programme informatique selon la revendication 18, dans lequel le demandeur devient un gestionnaire de domaine et dans lequel un dispositif demande un jeton auprès du demandeur.

24. Produit de programme informatique selon la revendication 18, dans lequel le demandeur devient un membre d'un second domaine.

25. Produit de programme informatique selon la revendication 18, dans lequel le gestionnaire de domaine reçoit une ou plusieurs demandes de jeton pour un second domaine.

26. Produit de programme informatique selon la revendication 18, dans lequel le service de domaines centralisé révoque l'identification de domaine.

27. Produit de programme informatique selon la revendication 21, dans lequel la validation comporte la validation des critères d'appartenance au domaine à réception de la demande par le demandeur et avant d'autoriser l'envoi du certificat de domaine au demandeur.

28. Produit de programme informatique selon la revendication 27, dans lequel l'identification de domaine expire dans un délai fixé par le service de domaines centralisé.

29. Produit de programme informatique selon la revendication 28, comportant en outre :

la réception, au niveau du service de domaines centralisé, d'une demande de renouvellement pour étendre le délai d'expiration d'identification de domaine.

30. Produit de programme informatique selon la revendication 27, dans lequel le service de domaines centralisé inclut le gestionnaire de domaine, et dans lequel le gestionnaire de domaine a demandé la création du domaine à partir d'un serveur de domaines centralisé, qui a créé l'identification de domaine.

31. Produit de programme informatique selon la reven-

dication 27, dans lequel le demandeur devient un gestionnaire de domaine et dans lequel un dispositif demande un jeton auprès du demandeur.

32. Produit de programme informatique selon la revendication 27, dans lequel le demandeur devient un membre d'un second domaine.

33. Produit de programme informatique selon la revendication 27, dans lequel le gestionnaire de domaine reçoit une ou plusieurs demandes de jeton pour un second domaine.

34. Produit de programme informatique selon la revendication 27, dans lequel le service de domaines centralisé révoque l'identification de domaine.

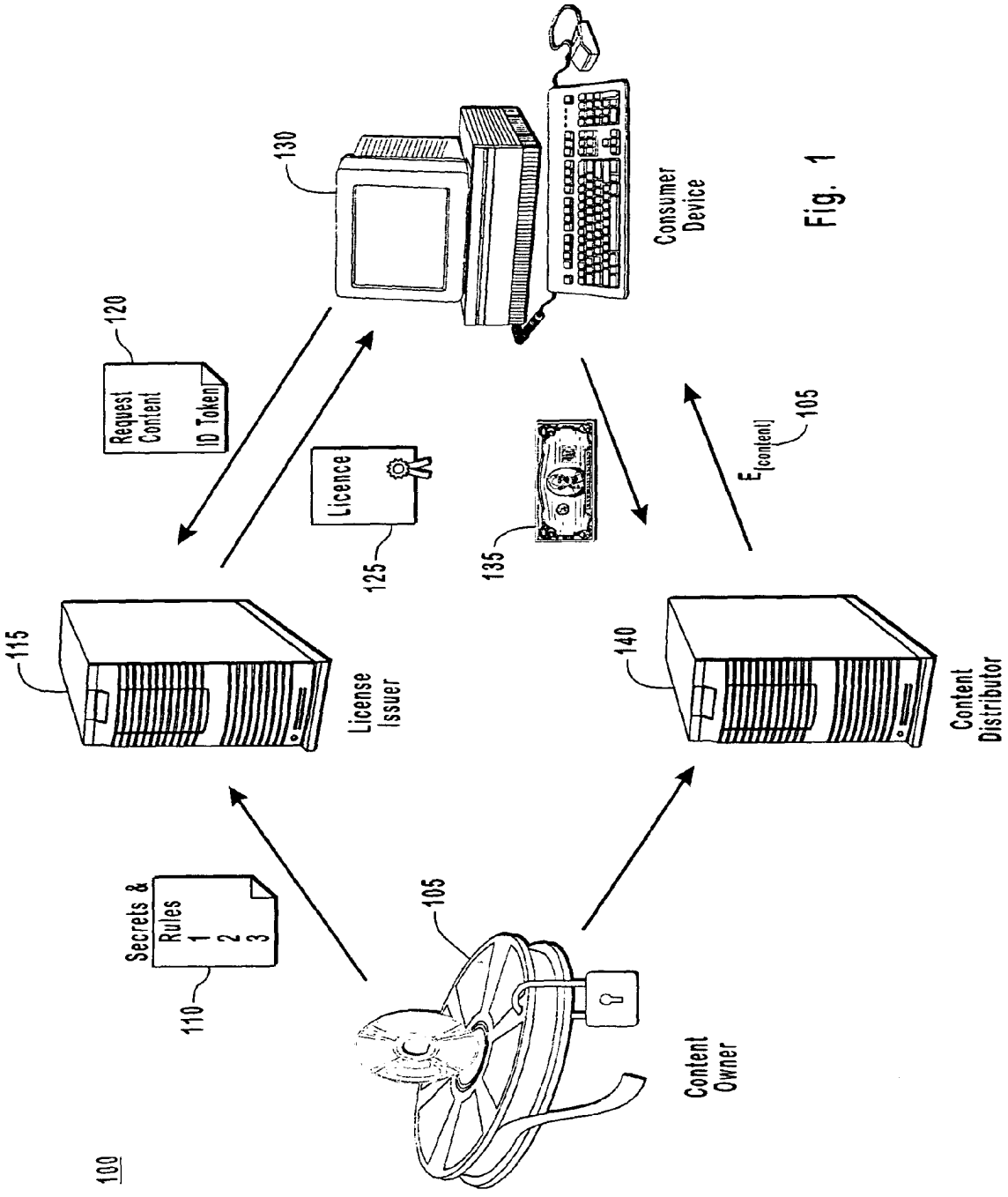

100
Secrets & Rules 1 2 3
110
105
Content Owner
License Issuer
115
Request Content ID Token
120
Licence
125
130
Consumer Device
135
$E_{[content]}$
105
140
Content Distributor

Fig. 1

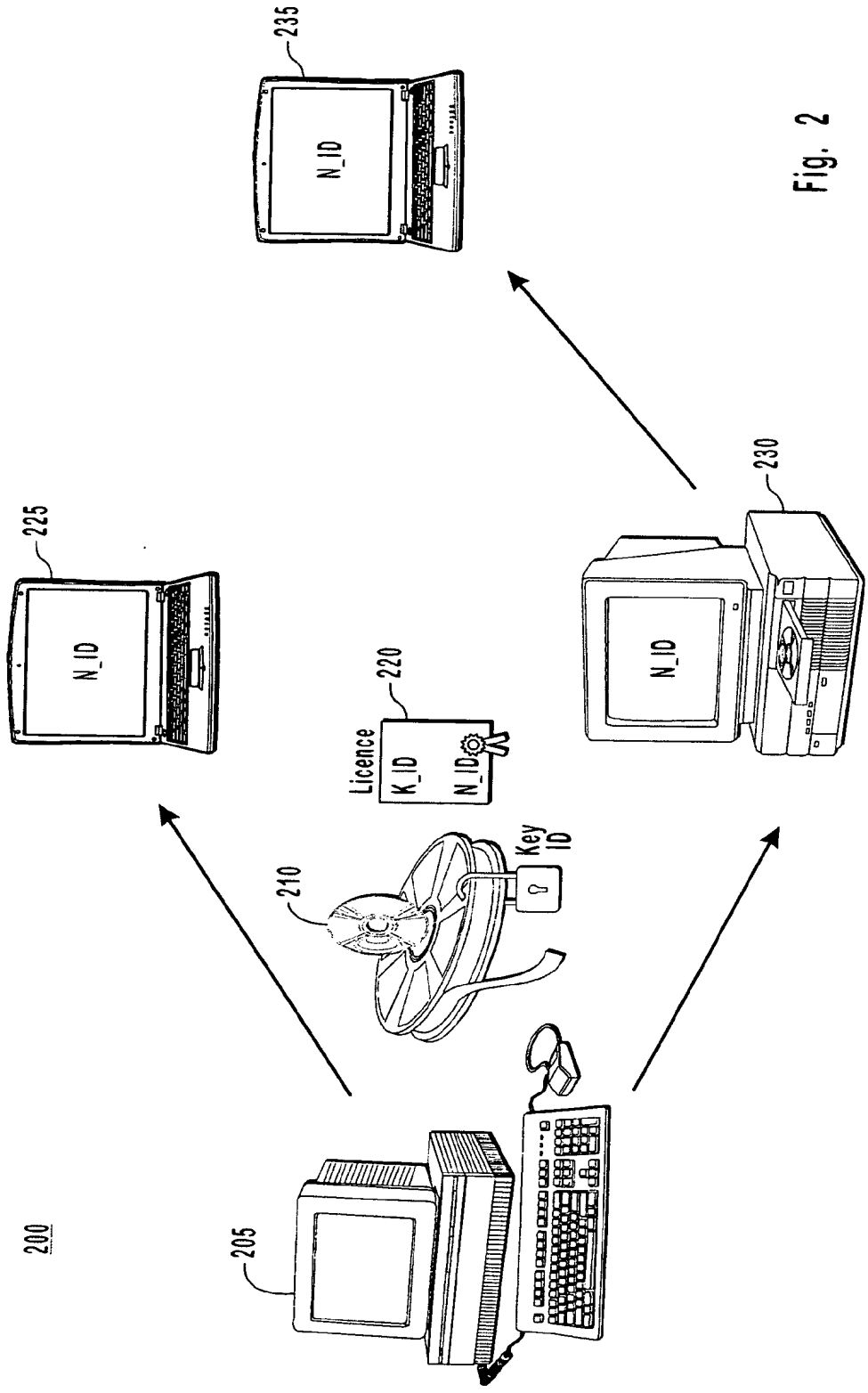


Fig. 2

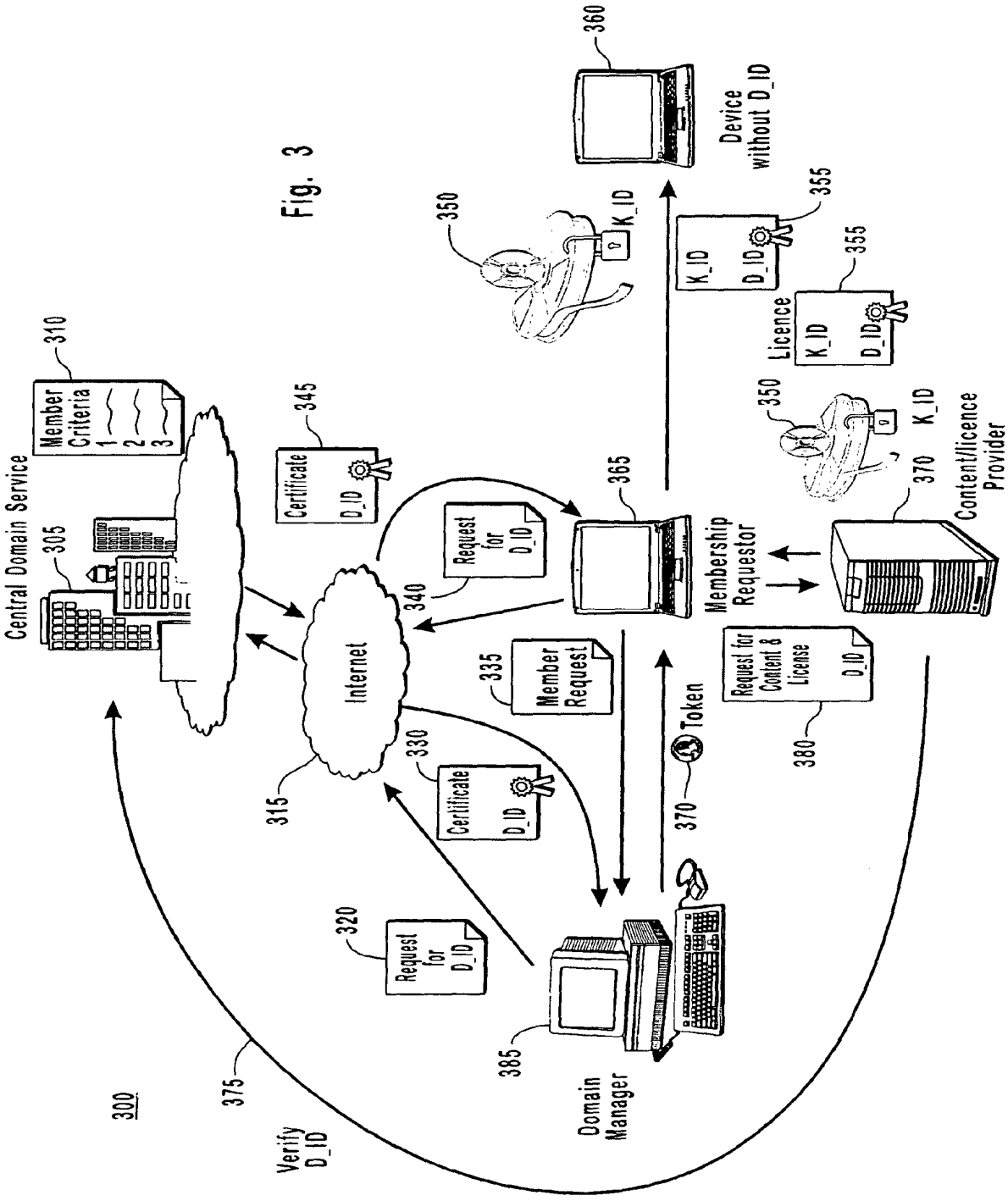

300
Central Domain Service
305
Member Criteria
1
2
3
310
Internet
315
Certificate
D_ID
345
Request for D_ID
340
Certificate
D_ID
330
Request for D_ID
320
Member Request
335
Token
370
Request for Content & License
D_ID
380
Domain Manager
385
Verify D_ID
375
Membership Requestor
365
Content/licence Provider
370
K_ID
350
Licence
K_ID
D_ID
355
K_ID
D_ID
355
Device without D_ID
360

Fig. 3

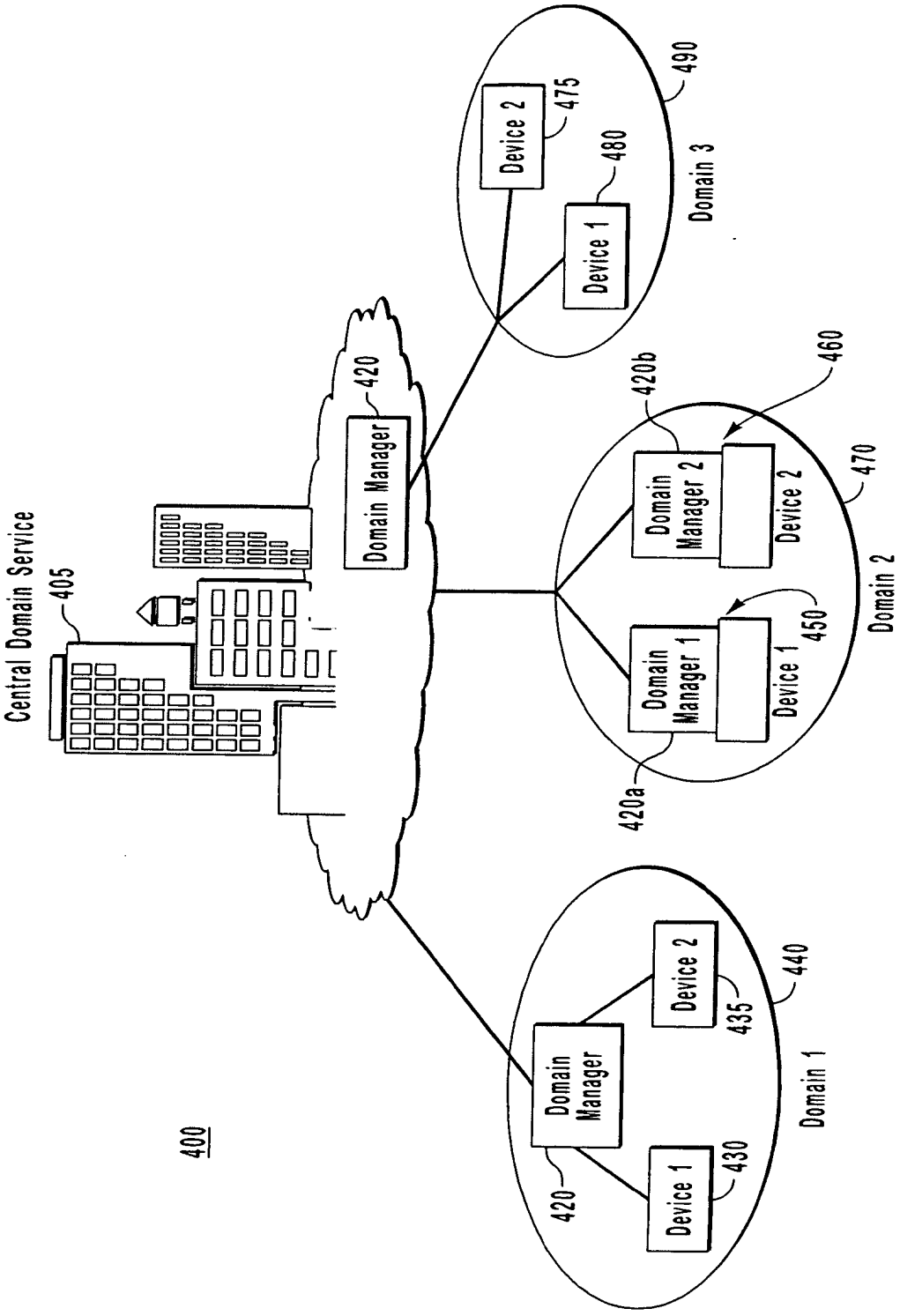

400
Central Domain Service
405
Domain Manager
420
Device 2
475
Device 1
480
490
Domain 3
420b
460
Domain Manager 2
Device 2
470
Domain 2
Domain Manager 1
Device 1
450
420a
Domain Manager
Device 2
435
440
Domain 1
420
Device 1
430

Fig. 4

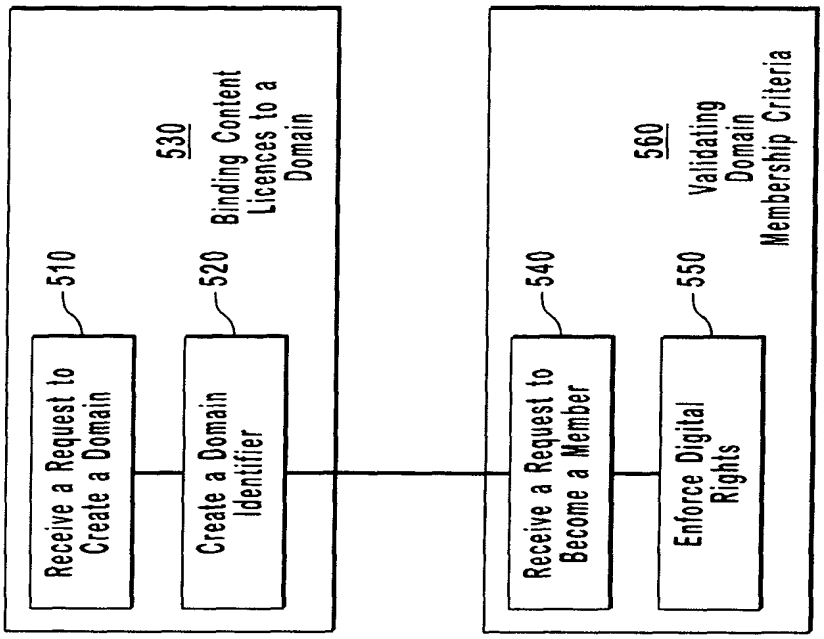

510
Receive a Request to Create a Domain
520
Create a Domain Identifier
530
Binding Content Licences to a Domain
540
Receive a Request to Become a Member
550
Enforce Digital Rights
560
Validating Domain Membership Criteria

Fig. 5

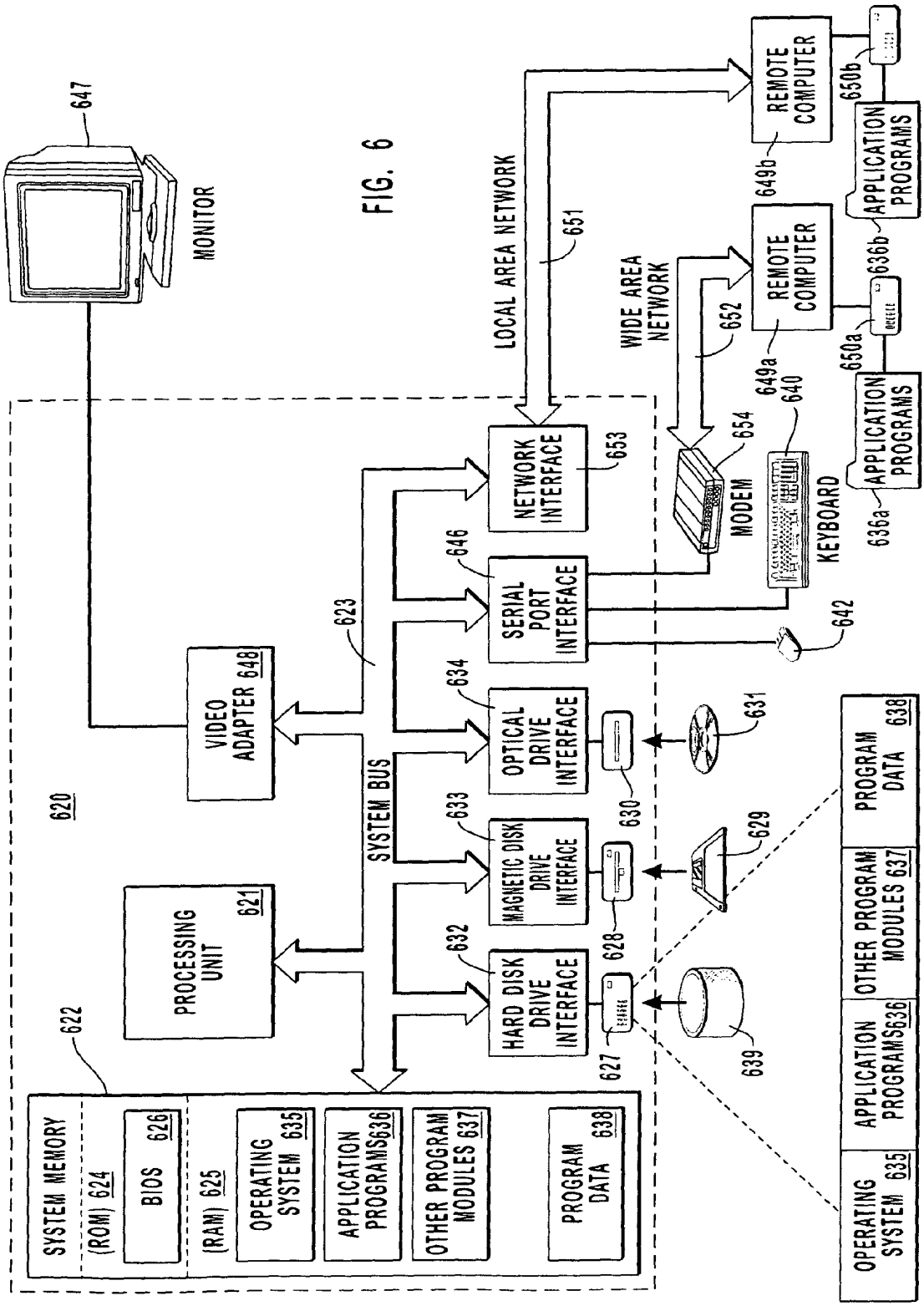

647
MONITOR
620
VIDEO ADAPTER 648
623
SYSTEM BUS
PROCESSING UNIT 621
622
SYSTEM MEMORY
(ROM) 624
BIOS 626
(RAM) 625
OPERATING SYSTEM 635
APPLICATION PROGRAMS 636
OTHER PROGRAM MODULES 637
PROGRAM DATA 638
HARD DISK DRIVE INTERFACE 632
MAGNETIC DISK DRIVE INTERFACE 633
OPTICAL DRIVE INTERFACE 634
SERIAL PORT INTERFACE 646
NETWORK INTERFACE 653
LOCAL AREA NETWORK 651
WIDE AREA NETWORK 652
MODEM 654
KEYBOARD 640
649a
649b
REMOTE COMPUTER
650a
650b
636a
636b
APPLICATION PROGRAMS
627
628
630
631
639
629
642
OPERATING SYSTEM 635
APPLICATION PROGRAMS 636
OTHER PROGRAM MODULES 637
PROGRAM DATA 638

FIG. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 03098931 A **[0014]**

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

(11) EP 1 505 530 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.02.2005 Bulletin 2005/06

(51) Int Cl.[7]: **G06F 17/60**

(21) Application number: **04022578.1**

(22) Date of filing: **27.02.2003**

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

(30) Priority: **27.02.2002 US 359667 P**
03.06.2002 US 159272

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
03716191.6 / 1 483 714

(71) Applicant: **ContentGuard Holdings, Inc.**
Wilmington, Delaware 19803 (US)

(72) Inventors:
- **Lao, Guillermo**
  Torrance CA 90503 (US)
- **Ham, Manuel**
  Downey CA 90241 (US)
- **Chen, Eddie J.**
  Ranchos Palos Verdes CA 90275 (US)
- **Demartini, Thomas**
  Culver City CA (US)
- **Gilliam, Charles P.**
  Darien CT 06820 (US)
- **Raley, Michael**
  Downey CA 90242 (US)
- **Tadayon, Bijan**
  Germantown MD 20876 (US)
- **Wang, Xin**
  Torrance CA 90503 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

Remarks:
This application was filed on 22 - 09 - 2004 as a divisional application to the application mentioned under INID code 62.

(54) Networked services licensing system and method

(57) A method, system, and computer program product for controlling consumption of a networked service (119) in accordance with rights expression information (127) associated with the networked service (119) and specifying a manner of use of the networked service (119), including determining the rights expression information (127) associated with the networked service (119), the rights expression information (127) indicating a manner of use of the networked service (119); and controlling consumption of the networked service (119) based on the rights expression information (127).

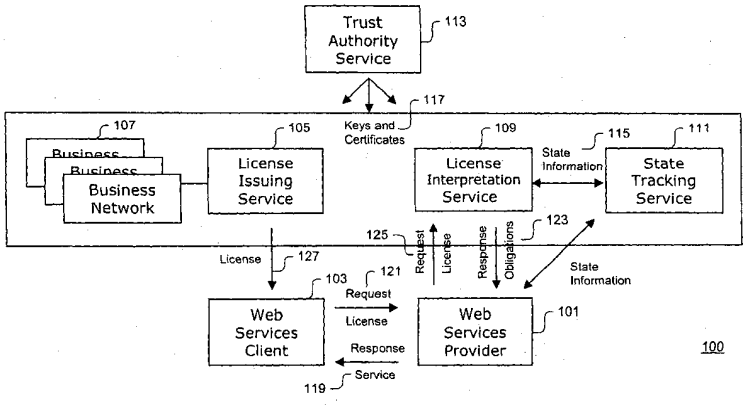


FIG. 1

EP 1 505 530 A1

Description

CROSS REFERENCE TO RELATED DOCUMENTS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] This invention generally relates to networked communications systems, and more particularly to a system and method for licensing of networked services, such as Web services, and the like.

Description of Related Art

[0002] Recently, networked services technologies, such as Web services technologies, are introducing at a rapid pace the capability to access various services over the Internet in an interoperable and automated manner. As enterprises make their content (such as software) and services available as networked services, there exists a need to control their indiscriminate access and use. The typical method of access control has been one where an identity or credentials about an identity are matched against a set of policies that are managed locally by the provider of the service. One example is when a user enters a user name and password to access some resource in a Web service. This method of access control is widely used in computer systems and is primarily about protecting "my" services against unauthorized use. In other words, access to a service typically is solely based on an identity of a user requesting access to the service.

[0003] With a desire to manage or restrict access, proliferate and commercialize services, there exist scenarios where computational environments are merely intermediaries and typically cannot decide on their own security policies. An example of such intermediaries includes hosting and replicating devices used in outsourcing and bandwidth management scenarios. However, in such environments, it is difficult to propagate and manage central security policies. Accordingly, there is still a need for systems and methods for licensing of networked services, such as Web services.

SUMMARY OF THE INVENTION

[0004] The above and other needs are addressed by exemplary embodiments of the present invention, which provide an improved system and method for licensing of networked services, such as Web services, and the like.

[0005] Accordingly, in an exemplary embodiment, there is provided an improved method for controlling consumption of a distributed network service in accordance with rights expression information associated with the distributed network service and specifying a manner of use of the distributed network service. The method includes determining the rights expression information associated with the distributed network service, the rights expression information indicating a manner of use of the distributed network service; and controlling consumption of the distributed network service based on the rights expression information.

[0006] According to another exemplary embodiment, there is provided an improved computer system for controlling consumption of a distributed network service in accordance with rights expression information associated with the distributed network service and specifying a manner of use of the distributed network service. The computer system includes a distributed network services provider configured to provide the distributed network service; a client of the provider configured to consume the distributed network service; a license issuing server configured to determine the rights expression information associated with the distributed network service, the rights expression information indicating a manner of use of the distributed network service; and a license issuing server configured to control consumption of the distributed network service based on the rights expression information.

[0007] According to a further exemplary embodiment, there is provided an improved computer-readable medium carrying one or more sequences of one or more instructions for controlling consumption of a distributed network service in accordance with rights expression information associated with the distributed network service and specifying a manner of use of the distributed network service. The one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of determining the rights expression information associated with the distributed network service, the rights expression information indicating a manner of use of the distributed network service; and controlling consumption of the distributed network service based on the rights expression information.

[0008] According to a still further exemplary embodiment, there is provided an improved system for controlling consumption of a distributed network service in accordance with rights expression information associated with the distributed network service and specifying a manner of use of the distributed network service, including means for determining the rights expression information associated with the distributed network service, the rights expression information

indicating a manner of use of the distributed network service; and means for controlling consumption of the distributed network service based on the rights expression information.

[0009] Still other aspects, features, and advantages of the present invention are readily apparent from the following detailed description, simply by illustrating a number of exemplary embodiments and implementations, including the best mode contemplated for carrying out the present invention. The present invention is also capable of other and different embodiments, and its several details can be modified in various respects, all without departing from the spirit and scope of the present invention. Accordingly, the drawings and descriptions are to be regarded as illustrative in nature, and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[0011] FIG. 1. is a schematic illustration of an exemplary Networked Services Licensing System, according to an exemplary embodiment;

[0012] FIG. 2 is a schematic illustration of exemplary interactions between a Web Services Provider, and a Web Services Client of the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0013] FIG. 3 is a schematic illustration of exemplary interactions between one or more Business Networks, and a License Issuing and/or Generation Service of the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0014] FIG. 4 is a schematic illustration of exemplary interactions between a Web Service Provider, and a License Interpretation Service of the Networked Services Licensing System, according to an exemplary embodiment;

[0015] FIG. 5 is a schematic illustration of exemplary interactions between a Web Service Provider, a License Interpretation Service, and a State Tracking Service of the Networked Services Licensing System, according to an exemplary embodiment;

[0016] FIG. 6 illustrates an exemplary workflow for when a Web Services Client knows, in advance, that a license is to be included in a message for service initiation in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0017] FIG. 7 illustrates an exemplary workflow for when a Web Services Client knows, via a service description language file, that a license is to be included in a message for a service initiation in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0018] FIG. 8 illustrates an exemplary workflow for when a Web Services Client knows, via a service description language file, that a license is to be is to be obtained from a License Generation Service of the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0019] FIG. 9 illustrates an exemplary workflow for when a Web Services Client does not know that a license is to be employed for gaining access to a service in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0020] FIG. 10 illustrates an exemplary workflow for when a Web Services Client attempts to gain access to a service without a license, is informed that the license is to be employed, and obtains the license for gaining access to a service in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0021] FIG. 11 illustrates an exemplary workflow for when an Enterprise out-sources license generation for gaining access to a service in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0022] FIG. 12 illustrates an exemplary workflow for when a plurality of Enterprises out-source license generation for gaining access to a service in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0023] FIG. 13 illustrates an exemplary method for license generation, based on license templates, that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0024] FIG. 14 illustrates an exemplary method for license generation, based on an authorizing license, that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0025] FIG. 15 illustrates an exemplary method for license generation, based on an exemplary a license prototype, that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0026] FIG. 16 illustrates an exemplary method for license generation, from scratch, that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0027] FIG. 17 illustrates an exemplary workflow for license validation that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0028] FIG. 18 illustrates exemplary workflows for license interpretation and state tracking that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiments;

[0029] FIG. 19. illustrates an exemplary workflow for specifying a license that can be used in the Networked Services

Licensing System of FIG. 1, according to an exemplary embodiment;

[0030] FIG. 20 illustrates an exemplary workflow for interpreting a license that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0031] FIG. 21 illustrates an exemplary workflow for controlling consumption of a service that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment;

[0032] FIG. 22 illustrates an exemplary workflow for issuing licenses by a third, party that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment; and

[0033] FIG. 23 illustrates an exemplary workflow for syndication of a service that can be used in the Networked Services Licensing System of FIG. 1, according to an exemplary embodiment.

DETAILED DESCRIPTION OF THE INVENTION

[0034] A system and method for licensing of networked services, such as Web services, and the like, are described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It is apparent to one skilled in the art, however, that the present invention can be practiced without these specific details or with equivalent arrangements. In some instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

[0035] Generally, a more flexible method for access control can be developed through technologies, referred to as Digital Rights Management (DRM) herein, wherein access to a resource is controlled by a license, wherein the license can be encoded in a rights language. The exemplary embodiments described herein, advantageously, leverage DRM system components to address issues related to the licensing of networked services, such as Web services. Accordingly, the exemplary embodiments can employ authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, document protection components, and the like, of a Digital Rights Management system, for example, as further described in commonly assigned U.S. Patents No. 5,530,235, No. 5,629,980, No. 5,634,012, No. 5,638,443, No. 5,715,403, No. 6,233,684, and No. 6,236,971, the entire disclosures of all of which are hereby incorporated by reference herein.

[0036] The use of a rights expression, for example, in the form of a license used to define usage rights for specifying a permitted manner of use, such as consumption, and the like, of a service, advantageously, switches the control, the responsibility for control, and the like, from the computing environment to the rightful owner of the service. Such usage rights can be associated with one or more conditions, such as payment, and the like, that can be a prerequisite for exercising the specified manner of use of the service. A rights expression language, such as extensible Rights Markup Language (XrML), and the like, for example, including predefined syntax and semantics, can be employed to express the usage rights. Consume, consuming, consumption, and the like, of the service, for example, can include access to or use of the service, access to or use of parts or devices of the service, access to or use of results of the service, receiving or rendering content of the service, executing software of the service, and the like.

[0037] In the above model, according to the exemplary embodiments, access control typically is about deploying "my" services "out-there," while at the same time issuing rights to users of such services to control access to the services. By contrast, other methods and systems for access control primarily are focused on protecting "my" services against use by others.

[0038] According to the exemplary embodiments, DRM is employed in a networked services environment, such as a Web services environment, for example, by leveraging components of the DRM system, such as license generation, license interpretation, and the like. In addition, the exemplary embodiments provide a system and method for authorization for networked services, for example, through a license expressed in a rights language. Further, the exemplary embodiments are directed how a license can be generated, used, processed, and the like, by the various entities of the networked services ecosystem to reach an authorization decision that allows access by a client, devices, services, and the like, to the networked services. In general, a requester of for a service presents a license in order to get access to the service.

[0039] Accordingly, the exemplary embodiments, advantageously, enable more flexible business models. For example, a service can be deployed "anywhere," and the control to access the service can be centralized and determined by the owner of the service. The points of deployment typically do not have to worry about establishing local security policies, as this becomes unnecessary. In addition, the model of "distributed access management" of the exemplary embodiments, advantageously, can be applied in the syndication of networked services, such as Web services, for example, including multiple layers of participants.

[0040] Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views, and more particularly to FIG. 1 thereof, there is illustrated an exemplary Networked Services Licensing System 100 that can be used in connection with the described exemplary embodiments for licensing of networked services, such as Web services, and the like. In FIG. 1, the Networked Services Licensing System 100,

for example, includes a Web Services Provider 101, a Web Services Client 103, a License Generation and Issuing Service 105 and that can interface with one or more Business Networks 107, a License Generation, Validation and/or Interpretation Service 109 for relaying a license 127, a State Tracking Service 111 for relaying state information 115, and a Trust Authority Service 113 for relaying keys and/or certificates 117. The services 105-111, advantageously, can be configured as a middle-tier or layer that can be plugged-in between the Trust Authority Service 113, and the Web Services Provider 101 and the Web Services Client 103. Advantageously, existing Web services systems can be modified to practice the exemplary embodiments based on such middle layer configuration.

[0041] A rights language, such as extensible Rights Markup Language (XrML), extensible Access Control Markup Language (XACML), Open Digital Rights Language (ODRL), and the like, can be used to specify a rights expression, rights expression information, and the like, for example, in the form of the license 127. However, the license 127 can be specified in any suitable manner. In addition, the license 127 can be based on a pre-defined specification, template, prototype, and the like, that can be associated with the Web service, according to further exemplary embodiments. Accordingly, the process of specifying the license 127 can include any suitable process for associating rights, conditions, and the like, with access to services, such as Web services.

[0042] An exemplary workflow for the Networked Services Licensing System 100 can include a user operating within the Web Services Client 103 environment being issued the license 127 by the License Issuing Service 105 for accessing a service of the Web Services Provider 101. When the user wishes to use a service 119 provided by the Web Services Provider 101, the user can make a request 121 for the service 119 from the Web Services Provider 101 along with the issued license 127. When associated conditions (for example, obligations 123), such as the collection of a fee, the authentication of the user, and the like, are satisfied based on a license interpretation request 125, as verified, for example, by the License Interpretation Service 109, and the State Tracking Service 111, the user can be allowed access to the service 119 of the Web Services Provider 101 in accordance with a manner of use specified in the license 127.

[0043] Advantageously, the license 127 can specify any suitable usage rights associated with the service 119. The interpretation and enforcement of the usage rights are further described in commonly assigned U.S. Patents No. 5,530,235, No. 5,629,980, No. 5,634,012, No. 5,638,443, No. 5,715,403, No. 6,233,684, and No. 6,236,971, for example. The steps above can take place sequentially or approximately simultaneously or in various orders.

[0044] FIG. 1 illustrates exemplary participants in a generalized Web service model, where the access to services and/or content is specified by a license expressed in a rights language, such as XrML, and the like. Advantageously, the use of a rights language to define access fits the Web services paradigm of distributed policies and access points because a rights language can capture both the rights and the context on which those rights can be exercised. The context can include information, an identification, and the like, of the client that is authorized to exercise the rights, the associated resources and conditions that have to be met in order to exercise the rights.

[0045] The top and bottom layers of FIG. 1 can be used to contrast a typical model for providing Web services, wherein the Web Services Provider 101 controls access through simple processes, such as user-name and password, and local policy evaluation. By contrast, according to the exemplary embodiments, the middle layer is involved in defining processes and/or determining authorization for access the service 119 provided by the Web Services Provider 101. This middle layer can be referred to as a "rights layer."

[0046] Advantageously, tasks related to determining authorization to the service 119, authentication, accounting, and the like, can be managed, outsourced, handled, and the like, by the specialized services provided by the middle layer. In this way, the Web Services Provider 101 can enjoy the luxury of focusing solely on the business logic of the service 119, while outsourcing other activities, such as the processing of payments, the maintaining of customer databases, and the like, that typically would be employed in a more monolithic e-commerce model. Accordingly, the Web Services Provider 101 processes the rights expression in the form of the license 127 that is presented by the Web Services Client 103 in order to determine what services to provide and how to provide such services. According to an exemplary embodiment, the license interpretation, the state information tracking, for example, such as how many times the service 119 has been rendered, which can be the accounting part, and the like, can be outsourced to third party providers.

[0047] The exemplary embodiments, thus, provide the authorizing of the access to the service 119, for example, via the generation of the license 127. By contrast, other Web services systems and methods typically control access by remembering a client's identity and by requesting a credential, such as user-name and password. In the exemplary embodiments, however, such credentials are augmented in the form of the license 127. The issuing of the license 127 can be accomplished by the rights layer, but can include processes performed by the Web Services Provider 101. The rights layer can include the Business Network(s) 107, such as a partner that bought the service 119 and is now allowing its customer base access to the service 119. Thus, anyone with a business arrangement with the Web Services Provider 101 can be capable of issuing the license 127, according to further exemplary embodiments.

[0048] The interaction of the Web Service Client 103 with the Web Services Provider 101 can involve various mechanisms and transactions, such as a request for service, a financial transaction, a rendering of the service 119, and the like. For example, of the Web Service Client 103 can contact the Web Services Provider 101 and request some type

of service 119. The access to the service 119 also can include various transactions, such as access, rendering, execution of code, send-back of data, collecting payment, and the like. Accordingly, the access to the service 119 can include any suitable interactions and/or results between the Web Service Client 103 and the Web Services Provider 101.

[0049] The Networked Services Licensing System 100 is of an exemplary nature and can be implemented in numerous other arrangements. For example, a clearinghouse (not shown) can be used to process payment transactions and verify payment prior to the Issuing Service 105 issuing the license 127. Moreover, the various processes and transactions can be performed, for example, via online and/or offline environments and/or combinations thereof, according to further exemplary embodiments. Accordingly, the various devices and/or components of the Networked Services Licensing System 100 can, but need not, communicate directly with one another and information can be exchanged in any suitable manner, such as by physically moving media between the devices the various devices and/or components of the Networked Services Licensing System 100.

[0050] The devices and subsystems of the Networked Services Licensing System 100 of FIG. 1 can communicate, for example, over one or more communications networks (not shown), and can include, for example, any suitable servers, workstations, personal computers (PCs), laptop computers, PDAs, Internet appliances, set top boxes, modems, handheld devices, telephones, cellular telephones, wireless devices, other devices, and the like, capable of performing the processes of the exemplary embodiments. The devices and subsystems can communicate with each other using any suitable protocol and can be implemented using a general-purpose computer system, for example. One or more interface mechanisms can be used in the Networked Services Licensing System 100, for example, including Internet access, telecommunications in any suitable form, such as voice, modem, and the like, wireless communications media, and the like. Accordingly, such communications network(s) can include, for example, wireless communications networks, cellular communications networks, satellite communications networks, Public Switched Telephone Networks (PSTNs), Packet Data Networks (PDNs), the Intemet, intranets, and the like. In addition, such communications network(s) can be the same or different networks.

[0051] As noted above, it is to be understood that the Networked Services Licensing System 100 of FIG. 1 is for exemplary purposes, as many variations of the specific hardware used to implement the exemplary embodiments are possible. For example, the functionality of the devices and the subsystems of the Networked Services Licensing System 100 can be implemented via one or more programmed computer systems or devices. To implement such variations as well as other variations, a single computer system can be programmed to perform the special purpose functions of one or more of the devices and subsystems of the Networked Services Licensing System 100. On the other hand, two or more programmed computer systems or devices can be substituted for any one of the devices and subsystems of the Networked Services Licensing System 100. Accordingly, principles and advantages of distributed processing, such as redundancy, replication, and the like, also can be implemented, as desired, to increase the robustness and performance of the Networked Services Licensing System 100, for example.

[0052] The components of the Networked Services Licensing System 100, for example, including the license 127, the Web Services Provider 101, the Web Services Client 103, the License Generation and/or Issuing Service 105, the License Validation and/or Interpretation Service 109, the State Tracking Service 111, and the Trust Authority Service 113, according to various embodiments, will now be further described.

[0053] The license 127, for example, can be based on rights language-based functions, such as XrML functions, and the like, in the exemplary embodiments. The Web Services Client 103 can present the license 127 to the Web Services Provider 101, when the Web Services Client 103 requests the service 119. The license 127, for example, can convey the rights and conditions governing the rendering of services, such the service 119, the manner of use of the services, and the like. In addition, the license 127, for example, can convey the context in which transactions between the Services Client 103 and the Web Services Provider 101 can take place, and the like.

[0054] Accordingly, the license 127 can convey information, for example, including the service 119, parts of the service 119, a principal to whom the license 127 has been granted, the rights that are granted, the conditions under which the service 119 can be accessed, obligations that the Web Services Provider 101 and/or the Web Services Client 103 may have to perform while allowing access to a protected resource of the service 119, trust domains, for example, including the issuer of the license 127 and/or the authority under which the license 127 has been issued, information to leverage or utilize security mechanisms, such as signatures and/or encryption mechanisms, any other suitable information, which can be mandatory and/or optionally employed by the Networked Services Licensing System 100, and the like.

[0055] An exemplary license 127, for example, written in XrML, is shown below that conveys, for example, a right to access the service 119 offered by the Web Services Provider 101, "www.foo.com/quoteService," and that has been granted to a holder of a specific cryptographic key, such as the principal, and the like, by the issuer, represented by another key value.

```
<license>
    <grant>
        <keyholder>
```

```
                    ...
                </keyhoder>
                <ws:execute />
                <serviceReference>
                    <foo: location uri= www.foo.com/quoteServicc/>
                </serviceReference>
            </grant>
        <issuer>
            <dsig:keyValue>
                ...
            </dsig:keyValue>
        </license>
```

[0056] The identification of the service 119 can be encoded in the license 127. Such encoding can be used to indicate that the license 127 refers to the service 119 in question. Additionally, any suitable granular identification of the service 119 in question can be specified. For example, the license 127 can describe that the license 127 pertains to a portion of the service 119, a certain Application Programming Interfaces (APIs) exposed by the service 119, and the like. Alternatively, the license 127 also can identify the service 119 including a set of services. For example, the service 119 can be described as "any service that originates from www.foo.com." Further, the service 119 identified can include any suitable combination of the models described above.

[0057] The principal specified in the license 127 can be used to verify the identity of the requester of the service 119, for example, a user of the service 119, such as the Web Services Client 103. The principal, thus, can be used to authenticate the requester of the service 119. Typically, the requester may have to present some form of credential at the time of the request 121, and such credential can verified against the identity of, for example, the principal specified in the license 127. The credential presented can employ various mechanisms, such as digital certificates, including a key, a security token, and the like.

[0058] The principal also can be specified, identified, and the like, in various ways. For example, the principal can be a specific principal, such as the holder of a cryptographic key, and the like. The principal also can specified as "anyone," such as "anyone in the universe," and the like. The principal also can be specified as a member of a set of principals, such as "any client that is a member of company ABC," and the like. Thus, depending on how the principal is specified, one or more credentials may be employed to fully resolve, match, and the like, the identity of the principal. The process to match credentials can include, for example, any suitable technology, traditional, proprietary or new, that can be used to authenticate a principal specified in a license.

[0059] The rights specified in the license 127 can be the granted or allowed "operations," that is, the manner of use, that the recipient of the grant, such as a principal, and the like, can exercise on the service 119, such as a Web service, and the like. Such operations can take various forms, such as "accessing the information on a Web service," "executing the software residing in a Web service," "retrieving some data that has been generated by a Web service," and the like.

[0060] The license 127 can include one or more conditions associated with a right to access the service 119. The conditions that can be specified in the license 127 and that may have to be satisfied in order to exercise the manner of use. For example, the conditions can include temporal conditions, such as a validity period, quantity conditions, such as the number of times the service can be accessed, payment conditions, accounting conditions, such as having the transaction tracked and recorded, and the like. Thus, conditions can include any suitable restrictions, parameters, obligations, states, and the like, that may have to be to be met before, during, after, in order to exercise the right.

[0061] The trust domain that can be specified in the license 127 can relate to the identity of the issuer of the license 127. For example, when the Web Services Provider 101 accepts the license 127 from the Web Services Client 103, the Web Services Provider 101 may have to determine if the Web Services Provider 101 can trust the information included in the license 127. In an exemplary embodiment, the entity that issued the license 127 can be identified by the issuer of the license 127.

[0062] The license 127 can employ, for example, security technologies in order to safeguard the information included in the license 127. For example, the Web Services Provider 101 can employ mechanisms to determine if the issuer of the license can be trusted, to determine if the license has not been tampered with, and the like. Thus, digital signatures technologies, and the like, can be employed to ensure the integrity of the license 127, and encryption technologies, and the like, can be used to keep certain information in the license 127 confidential.

[0063] FIG. 2 is a schematic illustration of exemplary interactions between the Web Services Provider 101 and the Web Services Client 103 of the Networked Services Licensing System 100, according to an exemplary embodiment. As shown in FIG. 2, the license 127 can be conveyed, transmitted, and the like, by the Web Services Client 103 to the Web Services Provider 101 when making the request 121 for the service 119. The Web Services Provider 101 then can render the service 119 based on rights, conditions, and the like, specified in the license 127. For example, the Web Services Client 103 and the Web Services Provider 101 can arrange before-hand that the license 127 is to be

transmitted in a data stream including the service request 121, based on a license protocol that includes the process of negotiating and/or submitting the license 127, and the like.

[0064] According to the exemplary embodiments, the Web Services Provider 101 typically focuses on providing the service 119. In addition, since authorization and/or commerce-related tasks can be managed elsewhere, as proposed in the exemplary embodiments, then tasks, such as the managing payments, the maintaining customers databases, and the like, can be eliminated. Advantageously, this allows the Web Services Provider 101 to more efficiently focus on providing the service 119.

[0065] The Web Services Provider 101 also can handle the service requests 121. Mechanisms to handle the service requests 121 can include, for example, proprietary mechanisms, standard mechanisms, such as Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL), other messaging protocols, and the like. However, any suitable mechanisms that can handle and/or process a service request can be employed.

[0066] In addition, the Web Services Provider 101 can employ a license protocol. Such protocol can include, for example, any suitable open or proprietary licensing mechanisms, a prior agreement to embed the license 127 in the request 121, a protocol that determines the need for the license 127, sending the requester to a site to obtain the license 127, and the like.

[0067] The Web Services Provider 101, thus, consumes and/or accepts the license 127 that has been conveyed by the Web Services Client 103 for gaining access to the service 119. After determining that the license 127 can be trusted, the Web Services Provider 101 can render the service 119, for example, based on rights and/or conditions specified in the license 127. If the license 127 is deemed invalid or untrustworthy, the Web Services Provider 101, for example, may not provide and/or render the service 119, and can generate an error message, for example, indicating that access to the service 119 is denied. Further, the Web Services Provider 101 may have to satisfy, as a condition of the license 127, obligations that result from the rendering the service 119, such as tracking of a state, and the like, and that can be specified in the license 127.

[0068] According to the exemplary embodiments, the Web Services Client 103 typically is the consumer device of the service 119, that is, the user device. The Web Services Client 103 can determine how to access the service 119, for example, via manual processes, through various technologies, such as Universal Description Discovery and Integration Standard (UDDI) registries, WSDL definitions, and the like. The Web Services Client 103 can present, convey, transmit, and the like, the license 127 to the Web Services Provider 101, for example, at the time of service request 121 or at a different time, in order to access the service 119.

[0069] In addition, the Web Services Client 103 can be aware that the license 127 can be employed in order to access the service 119. In other words, the Web Services Client 103 understands that access to the service 119 can entail the possession of the license 127, knows where to obtain the license 127, and the like. Such processes can be accomplished by a license protocol, wherein the request 121 for service 119 is followed by a response indicating that certain credentials, for example, such as the license 127, are employed for gaining access to the service 119. Such processing can be accomplished, for example, by manual processes, such as via agreements, for example, wherein the Web Services Provider 101 informs the Web Services Client 103 that a license is employed for accessing the service 119, and the like. Thus, Web Services Client 103 consumes the service 119, for example, executes code, renders content, and the like, after the Web Services Provider 101 has accepted the license 127.

[0070] In an exemplary embodiment, the Web Services Provider 101 also can be a Web Services Client, such as when the Web Services Provider 101 is a client of another Web service, and the like. Thus, the modes of operation of the exemplary embodiments are not so limited, but rather include other possible permutations of the exemplary. In a further exemplary embodiment, for example, the Web Services Client 103 might use a third party to present the license 127 and the presenter of the license 127 need not be the consumer of the service 119. In this exemplary embodiment, the Web Services Client 103 can provide, for example, additional information indicating that the license 127 can be presented by a third party.

[0071] The exemplary embodiments can include a lifecycle for rights, referred to as the "rights lifecycle." For example, the rights lifecycle can begin with the creation of the license 127, which can be used to associate some rights and/or conditions with some resource, such as the service 119. The license 127 then can be issued to the Web Services Client 103 who would then use the license 127 to obtain the service 119. Eventually, the license 127 is consumed by the Web Services Provider 101, for example, during the rendering of the service 119, completing the rights lifecycle.

[0072] In a typical DRM system, the issuing of a licenses typically is controlled by a single and/or centralized entity. Such entity typically is responsible for the computational tasks of issuing the license, which can include creating the license, validating the license, signing the license, and license recovery. Similarly, in a typical access control system, the authorization assertions are generated by a centralized entity, where security policies are defined and managed. By contrast, in an exemplary embodiment, the generation of the license 127 can be logically separated from the issuing of the license 127. Typically, the license 127 generation includes the computational functions to create the license 127, such as creating an XrML file, and the like, constructing the elements, storing the license in a database, and the like. The license issuing can be the actual authorization of the rights that are granted in the license 127, for example,

including digitally signing the license 127 and/or attesting that the rights conveyed in the license 127 are authorized by the issuer, and the like.

[0073] According to the exemplary embodiments, the License Generation Service 105, a task, and the like, can provide additional services, such as data backup, license version control, upgrades, license revocation, and the like. Advantageously, such services can add further value, to the valued added by the process of generating the license 127.

[0074] The tasks of generating and issuing the license 127 can be performed by a single application, and/or system. However, the separation of authority between license 127 generation and the license 127 issuing, advantageously, supports various exemplary business embodiments. For example, this approach allows a business entity the option to outsource the data intensive part of generating the license 127, and to focus on the authority part of signing and issuing the license 127. This approach, advantageously, enables a single service that can generate and issue licenses 127 on behalf of different business entities, as will now be discussed.

[0075] FIG. 3 is a schematic illustration of exemplary interactions between one or more of the Business Networks 107 and the License Issuing and/or Generation Service 105 of the Networked Services Licensing System 100, according to an exemplary embodiment. In FIG. 3, the authority to issue licenses 127 can be conveyed in the form of the license 305 to issue licenses 127, referred to as a "distribution" license, and as shown in FIG. 3. Accordingly, the distribution license 305 grants the right to issue one or more of the licenses 127. The distribution license 305 also can specify a manner of use that can be granted and conditions, such as the maximum number of licenses 127 that the License Generation Service 105 can issue, and the like. The distribution license 305 also can be used to attest that the issuer of the license 127 has the authority to issue the licenses 127, and can be referenced when the issuer's signature is not recognized, but the signature of the issuer of the distribution license 305 is recognized.

[0076] In other words, the presence of distribution licenses 305 establishes a trust model, wherein signatures in the licenses 127 can be checked, for example, during license 127 interpretation, up the chain of distribution until a signature, signatures, and the like, are recognized, trusted, and the like. Such a model fits well in the exemplary embodiments, where an owner of a service can grant the right, in the form of a license, to issue licenses to business partners, for example, after some contract or business arrangements.

[0077] For example, an exemplary workflow for license generation and issuing, can include business partner 301 (Business Entity A), and business partner 303 (Business entity B). In this example, the Business Entity A owns and operates a Web service, and Business Entity B wishes to bundle the Web service as part of a product line of Business Entity B. Accordingly, the Business Entity A issues the distribution license 305 to the Business Entity B granting the Business Entity B the right to issue the licenses 127 to the customers, for example, the Web Services Client 103, of the Business Entity B, for example, to access the Web service provided by the Business Entity A. The Business Entity B issues the licenses 127 to the customers, for example, by utilizing the License Issuing Service 105 to generate the license 127. When the Web Services Client 103 accesses the Web service provided by the Business Entity A, the license 127 is presented and the Web service can check the authority of the license 127 by recognizing that the Business Entity B was granted the right to issue such licenses 127.

[0078] Accordingly, the License Generation Service 105, for example, can perform the computational process of generating an unsigned license 309, the distribution license 305, and/or the license 127 based on a request 307, and including schema validation, and the like. In addition, the License Generation Service 105 can provide a generalized interface to handle the service requests 307, for example, requests for licenses 127, 305 and/or 309. The License Generation Service 105 typically does not sign the license 127, but, according to a further exemplary embodiment, the License Generation Service 105 can sign the licenses 127 on behalf of a license 127 issuer, such as the Business Entity B. Further, the License Generation Service 105 can provide, for example, data management functions; such as the back-up issued licenses, the re-issue of licenses, reporting functions, and the like.

[0079] FIG. 4 is a schematic illustration of exemplary interactions between the Web Service Provider 101 and the License Interpretation Service 109 of the Networked Services Licensing System 100, according to an exemplary embodiment. For example, in order to consume the service 119, such as allowing execution of code of the Web Services Provider 101, rendering encrypted and/or protected content of the Web Services Provider 101, and the like, the license 127 can be validated, and then interpreted based on the interpretation request 125 to determine if rights, conditions, such as obligations 123, specified therein allow such operation. The capabilities for validating and/or interpreting the license 127 can be built into the Web Services Provider 101 and/or a rendering application. However, according to further exemplary embodiments, such capabilities can be separated from the Web Services Provider 101 and/or the rendering application, and can be provided by a service, such as the License Interpretation Service 109.

[0080] Thus, according to an exemplary embodiment, the license 127 is validated and then interpreted by the License Interpretation Service 109. However, according to a further exemplary embodiment, this process can be performed in reverse order, and in which case the interpretation can be performed subject to a later validation step.

[0081] The License Interpretation Service 109 can be employed for the task of interpreting licenses 127, which is a counterpart of the license generation model of the License Interpretation Service 105, whereby the Web Services Provider 101 can offload computational tasks not directly associated with providing the service 119. The Web Services

Provider 101 operating as such can offload the task of interpreting the license 127 to the License Interpretation Service 105, and, advantageously, focus in building the service 119. During license 127 interpretation, potentially other services 401 can be employed, as shown in FIG. 4. For example, the service 401 can be contacted to authenticate the principal, to retrieve information stored in a remote service, such as a trusted time clock, and the like.

[0082] FIG. 5 is a schematic illustration of exemplary interactions between the Web Service Provider 101, the License Interpretation Service 109, and the State Tracking Service 111 of the Networked Services Licensing System 100, according to an exemplary embodiment. In FIG. 5, the use of the State Tracking Service 111, during the license 127 interpretation stage 501, and during the exercise of rights stage 503, is shown.

[0083] The interpretation of the license 127 and/or the exercise of a right, can involve information that is stored outside of the license 127. For example, a condition of the license 127 can be that there is a limit to the number of times a resource provided by the Web Services Provider 101 can be accessed. Accordingly, during the interpretation of the license 127, including of such condition; the information regarding the number of times the resource has already been accessed may have to be retrieved in order to accurately and truthfully interpret whether a further access right can be granted.

[0084] Such information can be referred to as the state information 115, and the tracking of the state information 115 can be referred to as "state tracking." The state information 115 can include various types of information, such as information regarding the status of the license 127, the amount of time a resource has been used, information regarding payment for the service 119, information regarding the time of the day the service 119, the license 127, and/or the conditions, were issued, accessed, consumed, presented, and the like. Accordingly, the state information 115 can include any suitable information regarding the Networked Services Licensing System 100, and the like.

[0085] The state information 115 can reside and/or be recorded in persistent storage, such as a database, a memory, a service, and the like, of the Networked Services Licensing System 100. For example, the state information 115, such as the number of times the service 119 has been accessed by the Web Services Client 103, and the like, can be recorded in some persistent storage of the Networked Services Licensing System 100. Additionally, as previously described, the interpretation of the license 127 can result in the obligations 123 that may have to be fulfilled while allowing the exercise of the rights.

[0086] Although the tracking of the state information 115 can be implemented locally, for example, by the Web Services Provider 101, this can create an additional burden for the Web Services Provider 101. In addition, local tracking by the Web Services Provider 101 may be difficult to implement, because the Web Services Provider 101 may not be able to accommodate the local storage of the state information 115. Advantageously, the State Tracking Service 111 addresses the noted and other problems associated with the tracking of state information by the Web Services Provider 101. A rights language, as previously described, can be used to specify, for example, where the Tracking Service 11 is referenced, where the state information 115 related to the conditions of the rights can be managed, and the like. Thus, the State Tracking Service 111 can be used for tracking, providing, and the like, the state information 115 that can be specified in the license 127.

[0087] The Trust Authority Service 113 can include elements and/or services that, for example, establish, manage, and the like, trust relations for the various entities of the exemplary embodiments. For example, the Trust Authority Service 113 can include a Certificate Authority (CA) function for issuing the digital certificates, digital credentials and/or encryption keys 117 that can be employed to sign the licenses 127. Accordingly, the Trust Authority Service 113, for example, can include a corporation's Public Key Infrastructure (PKI), a service provided by a PKI and/or security provider, a separate service employed to establish a trust relation between business partners, and the like.

[0088] Therefore, according to an exemplary embodiment, the Trust Authority Service 113 can include the function issuing of digital credentials 117, for example, used to identify the principals. Exemplary digital credentials 117 can include, for example, an X509 digital certificate, a Microsoft Passport, a Kerberos authentication token, and the like. The credentials 117 of the type described above can be used to specify and/or certify the identity of the holder, but typically convey little additional information about the holder, as most of such additional information typically is provided in a fixed format and/or is implied. For example, a passport holder typically is simply someone that has been authenticated with the Microsoft passport service.

[0089] Accordingly, a need exists to attach additional information about identities, for example, of the principals, in a more expressive and/or robust manner, for example, to express the role of the principal, a membership association for the principal, and the like. A rights language, as previously described, and according to a further exemplary embodiment, advantageously, can be used define a certificate 117 that can be used to convey credentials in a more expressive manner, for example, to express the role of the principal, a membership association for a principal, and the like. The credentials 117 then can be used to associate the holder with additional properties, such as a membership in a business circle, a relationship in a business environment, and the like.

[0090] Typically, a Certificate Authority can attest to the authenticity of the information included in a digital certificate. If the information in the digital certificate can be limited in scope, for example, such as a company name, the functions of the Certificate Authority can be well defined. For example, a Certificate Authority may have an established process

to check a company's name before issuing a digital certificate. However, when the credentials become more expressive, as described above, it becomes more difficult for a Certificate Authority to attest to the authenticity of the credential information. For example, if a credential includes some membership information, the Certificate Authority would have to establish some additional process to validate such membership.

[0091] Accordingly, a generic Certificate Authority typically cannot verify such additional information. Typically, the Certificate Authority, a signer, and the like, of the credential can become the system where the credential is to be used. In this exemplary embodiment, the trust model becomes less open and more monolithic, for example, since the system typically can trust the system. To use credentials with more expressive information in a more open system, for example, within a business network of affiliated services, the Trust Authority Service 113, advantageously, can be employed to attest to additional information that can be included in the certificates 117. According to an exemplary embodiment, a Certificate Authority can be configured to fulfill the above-note needs. However, a "trust broker," such as the Trust Authority Service 113 of the exemplary embodiments, advantageously, can be employed to address the noted and other problems with a Certificate Authority being employed to verify the above-noted additional information.

[0092] Just like the certificates 117, the licenses can be signed and/or verified, for example, through cryptographic techniques. The verification of the license 127 signature can be used, for example, to attest to the integrity of the license 127, the authenticity of the signer, such as the license 127 issuer, and the like. Typically, however, such verification does not establish a "rights trust," for example, to trust that the license 127 was issued with proper authorization, unless the verifier authorized the issuing of the license 127. This is a difference between the license 127 validation, and the license 127 interpretation, as previously discussed.

[0093] For example, Company B issues a license B' to Company A granting Company A the right to issue licenses A' on behalf of Company B. Then, Company A issues a license A' to user X, and user X presents the license A' to Company B to access a protected resource of Company B. In this exemplary embodiment, since company B issued the license B', the trust of license A' can be traced back to license B', which is trusted by default by company B.

[0094] Now, consider the case where Company C also accepts licenses A' for access to a protected resource of Company C. In order to trust the license A', Company C may have to either decide to trust licenses from Company A or issue a license C' to Company A with the right to issue licenses A' on behalf of Company C. As the network becomes large, every license A' would have to be accompanied with each of the authorizing licenses B', C', and so on.

[0095] In the above case, processing of such licenses A' quickly can become cumbersome and/or impractical. According to an exemplary embodiment, however, a "trust broker," such as the Trust Authority Service 113 of the exemplary embodiments, advantageously, can as the "trust broker," for example, to broker deals between companies, issues licenses under its own signature, and the like. In this exemplary embodiment, during the license 127 interpretation process, the signature of the Trust Authority Service 113 can be trusted.

[0096] When the Web Services Client 103 initiates, requests, and the like, the service 119, the Web Services Client 103 can transmit the license 127, for example, as part of a messaging protocol. Advantageously, according to an exemplary embodiment, the information for transmitting the license 127 at the time of the service 119 initiation can be provided in advance, for example, by reading some documentation on a Web site, and the like.

[0097] When the Web Services Client 103 initiates, requests, and the like, the service 119, the Web Services Client 103 can transmit the license 127, for example, as part of a messaging protocol. Although, according to an exemplary embodiment, the information for transmitting the license 127 at the time of the service 119 initiation can be provided in advance, by reading some documentation on a Web site, and the like, there is a need for a protocol, where the need for the license 127 can be communicated through a messaging mechanism. Advantageously, according to a further exemplary embodiment, such a protocol is provided, as will be further described. Exemplary embodiments for the service 119 initiation, for example, involving the license 127, will now be described.

[0098] FIG. 6 illustrates an exemplary workflow for when the Web Services Client 103 knows, for example, in advance, that the license 127 is to be included in the message 121 for the service 119 initiation in the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 6, at step 601, for example, such information can be obtained through various mechanisms, such as by obtaining information from a Web site, e-mail, facsimile, phone call, and the like. At step 603, for example, the license 127 can be encoded as part of the service 119 request message 121, which, at step 605, is transmitted to the Web Services Provider 101. According to an exemplary embodiment, the license 127 can be encoded in the message 121, manually, automatically, and the like, and employ a messaging protocol, for example, including a SOAP header, the messaging protocols of the further described exemplary embodiments, and the like.

[0099] FIG. 7 illustrates an exemplary workflow for when the Web Services Client 103 knows, for example, via a service description language file 709, such as a WSDL file stored in a UDDI-based service discovery server 707, and the like, that the license 127 is to be included in the message 121 for the service 119 initiation in the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 7, at step 701, for example, the WSDL file 709 is retrieved from the UDDI server 707, manually, automatically, and the like. At step 703, for example, the license can be encoded 127 as part of the service 119 request message 121, which, at step 705, is transmitted to the Web Services Provider 101. According to an exemplary embodiment, the license 127 can be encoded in the message 121, manually, automatically,

and the like, and employ a messaging protocol, for example, including a SOAP header, the messaging protocols of the further described exemplary embodiments, and the like.

[0100] FIG. 8 illustrates an exemplary workflow for when the Web Services Client 103 knows, for example, via a service description language file 709, such as a WSDL file stored in the UDDI-based service discovery server 707, and the like, that the license 127 can be obtained from the License Generation Service 105 of the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 8, at step 801, for example, a user at the Web Services Client 103 retrieves, manually, automatically, and the like, the WSDL file 709 from the UDDI server 707, wherein the service description in the WDSL file 709 includes a reference to a service, such as the License Generation Service 105, and the like, that can be used to issue the license 127 for the service 119. At step 803, the user at the Web Services Client 103, for example, initiates the License Generation Service 105.

[0101] At step 805, for example, after satisfying conditions, such as payment of a fee for the license 127, and the like, the Web Services Client 103 obtain the license 127, manually, automatically, and the like, from the License Generation Service 105. At step 807, the user at the Web Services Client 103, for example, encodes the license 127 as part of the service 119 request message 121, which then is transmitted to the Web Services Provider 101. According to an exemplary embodiment, the license 127 can be encoded in the message 121, manually, automatically, and the like, and employ a messaging protocol, for example, including a SOAP header, the messaging protocols of the further described exemplary embodiments, and the like.

[0102] FIG. 9 illustrates an exemplary workflow for when the Web Services Client 103 does not know that the license 127 is to be employed for gaining access to the service 119 in the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 9, at step 901, for example, the Web Services Client 103 attempts to invoke and/or request the service 119 from the Web Services Provider 101, via the service 119 request message 121, which does not include the license 127. At step 903, the Web Services Provider 101 processes the service 119 request message 121, and determines that service 119 request message 121 does not include the license 127. At step 905, the Web Services Provider 101 transmits, for example, an error message 907, and the like, indicating that the license 127 is to be employed for gaining access to the service 119 of the Web Services Provider 101. At this point, the Web Services Client 103 can attempt to obtain the license 127, for example, employing the previously described methods of FIGs. 6-8, and as will be further described. According to an exemplary embodiment, the messages 907 and 121 can employ a messaging protocol, for example, including a SOAP header, the messaging protocols of the further described exemplary embodiments, and the like.

[0103] FIG. 10 illustrates an exemplary workflow for when the Web Services Client 103 attempts to gain access to the service 119 without the license 127, is informed that the license 127 is to be employed, as shown in FIG. 9, and obtains the license 127 for gaining access to the service 119, using the method described in FIG. 8, in the Networked Services Licensing System 100 of FIG. 1. However, any suitable method for obtaining a license, such as the methods of FIGs. 6-8, and the like, can be employed to obtain the license 127.

[0104] Accordingly, as shown in FIG. 10, at step 1001, for example, the Web Services Client 103 attempts to invoke and/or request the service 119 from the Web Services Provider 101, via the service 119 request message 121, which does not include the license 127. At step 1003, the Web Services Provider 101 processes the service 119 request message 121, and determines that service 119 request message 121 does not include the license 127. At step 1005, the Web Services Provider 101 transmits, for example, the error message 907, and the like, indicating that the license 127 is to be employed for gaining access to the service 119 of the Web Services Provider 101.

[0105] The Web Services Client 103, then, determines that the License Generation Service 105, and the like, that can be used to issue the license 127 for the service 119. At step 1007, a user at the Web Services Client 103, for example, initiates the License Generation Service 105. At step 1009, for example, after satisfying conditions, such as payment of a fee for the license 127, and the like, the Web Services Client 103 obtain the license 127, manually, automatically, and the like, from the License Generation Service 105. At step 1011, the user at the Web Services Client 103, for example, encodes the license 127 as part of the service 119 request message 121, which then is transmitted to the Web Services Provider 101. According to an exemplary embodiment, the license 127 can be encoded in the message 121, manually, automatically, and the like, and employ a messaging protocol, for example, including a SOAP header, the messaging protocols of the further described exemplary embodiments, and the like.

[0106] According to the exemplary embodiments, a separation of authority between the generation of the license 127 and the issuing of the license 127 can be provided. For example, the issuing of the license 127 can signify that the issuer of the license 127 authorizes the rights in the license 127. Advantageously, such separation of authority provides for various exemplary embodiments, for example, as illustrated by the following exemplary workflows.

[0107] FIG. 11 illustrates an exemplary workflow for when an Enterprise 1111 out-sources the license 127 generation for gaining access to a service in the Networked Services Licensing System 100 of FIG. 1. The exemplary workflow of FIG. 11 can be used, for example, in combination with the exemplary embodiments described herein. In FIG. 11, the Enterprise 1111, such as the Business Entity B 303, and the like, can out-source the license 127 generation to a service, such as the License Generation Service 105, and the like, according to an exemplary embodiment. Advanta-

geously, in this manner, resources related to the task of the license 127 generation can be freed up for the Enterprise 1111.

[0108] Services of the Enterprise 1111 for which authorization to allow access is desired, and for which the licenses 127 can be generated, can include, for example, services owned by the Enterprise 1111, services owned by business partners of the Enterprise 1111, the service 119 provided by the Web Services Provider 101, and the like. The task of authorizing grants in the license 127, for example, the license 127 issuing, can include digitally signing the license 127, via license signing mechanism 1115, and the like, and can remain with the Enterprise 1111. In this exemplary embodiment, the Enterprise 1111 would have authorization to issue the licenses 127, for example, implicitly, as when the Enterprise 1111 owns the service in question, explicitly, as through the distribution license 305 granting the Enterprise the right to issue the licenses 127 on behalf of another business entity, and the like.

[0109] Accordingly, at step 1101, for example, one or more clients and/or end users 1113, such the Web Services Client 103, and the like, can request the licenses 127 from the Enterprise 1111. If the Enterprise 1111 decides to issue the requested licenses 127 to the clients and/or end users 1113, at step 1103, for example, the Enterprise 1111 requests unsigned licenses from the License Generation Service 105. In a further exemplary embodiment, the Enterprise 1111 can make such request for the unsigned licenses, for example, because the Enterprise 1111 may wish to "push" the licenses 127 onto the clients, such as for advertising purposes, promotional purposes, and the like. The Enterprise 1111 can communicate with the License Generation Service 105, and make the request for the unsigned licenses, using any suitable messaging protocol, such as the license protocol of the exemplary embodiments described herein.

[0110] At step 1105, for example, the License Generation Service 105 processes the request for the unsigned licenses, creates the unsigned licenses using any suitable license generation technique, such as the license generation techniques of the exemplary embodiments described herein, and delivers the unsigned licenses to the Enterprise 1111. At step 1107, for example, the Enterprise 1111 signs the license, and, at step 1109, delivers, transmits, conveys, issues, and the like, the signed licenses 127 to the clients and/or end users 1113.

[0111] The exemplary workflow, wherein the Enterprise 1111 out-sources the license generation and signing, is similar to that of FIG. 11, except that the License Generation Service 105 also can perform the signing of the unsigned licenses to generate the licenses 127. In this exemplary embodiment, the License Generation Service 105 can be configured; for example, as a "proxy" signer, and the like, for the Enterprise 1111. The License Generation Service 105, for example, can safeguard a signing key used to sign the unsigned licenses on behalf of the Enterprise 1111. Accordingly, although the issuing party is the Enterprise 1111, the License Generation Service 105 can act as a proxy for the Enterprise 111. Since the License Generation Service 105 maintains, safeguards, and the like, the signing keys, a requester of the license 127, advantageously, can be authenticated to prevent spoofing of the service, and the like.

[0112] FIG. 12 illustrates an exemplary workflow for when a plurality of Enterprises 1111 out-source the license 127 generation for gaining access to a service in the Networked Services Licensing System 100 of FIG. 1. The exemplary workflow of FIG. 12 can be used, for example, in combination with the exemplary embodiments described herein. As shown in FIG. 12, from the perspective of the License Generation Service 105, advantageously, the License Generation Service 105 can provide the license request, at step 1103, license delivery, at step 1105, and the like, services to the plurality of Enterprises 1111. In this exemplary embodiment, each of the Enterprises 1111, for example, can be associated with a corresponding account, and the License Generation Service 105 can be configured to manage the licenses 127 issued on behalf of the plurality of Enterprises 1111, for example, on a per-account basis, and the like.

[0113] The License Generation Service 105 can utilize any suitable method for generating the licenses of the exemplary embodiments, for example, including the following exemplary methods, as will be described. The exemplary methods, advantageously, can be used to generate various types of licenses, such as the licenses 127, the distribution license 305, and the like.

[0114] FIG. 13 illustrates an exemplary method for license generation, based on license templates 1301, that can be used in the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 13, in this exemplary method, the License Generation Service 105, for example, manages local license templates 1301, and license generation policies 1303, under which the templates 1301 are used to generate a license, and the like. The templates 1301 and the policies 1303 can be created under the agreement of the authorizing entity, for example, an entity that can utilize the License Generation Service 105 in an out-source type of arrangement, and the like.

[0115] The license templates 1301, for example, can include predefined licenses, wherein one or more fields thereof are replaced, filled-in, and the like, when the license is generated. For example, the license templates 1301 can include a license template where the principal is not defined, and can replaced by a specific principal, where a resource, such as the service 119, is undefined, and replaced by a specific resource, and the like, at the time of license generation.

[0116] The license generation policies 1303, for example, can include rules for determining which templates to use, based on the request, and the like. For example, a policy can include a rule, such as "every request for a license involving a specific resource shall use template 123," "every request from company ABC will use the template ID 456 and resolve/replace the principal with the principal transmitted in the request," and the like.

[0117] Accordingly, a license request message 1305 transmitted to the License Generation Service 105 can include

parameters 1307, such as a principal identification/key, resource ID, template ID, and the like, to allow for the generation of a corresponding license based thereon. The specification for the parameters 1307, for example, can be arranged manually, automatically, before-hand, codified in a WSDL description of the service, predetermined, and the like.

[0118] FIG. 14 illustrates an exemplary method for license generation, based on an authorizing license 1401, that can be used in the Networked Services Licensing System 100 of FIG. 1. In this exemplary method, the License Generation Service 105 receives along with the request 1305, the authorizing license 1401 that authorizes the issuing of a license, and which includes the grant or grants that are to be issued. Accordingly, the authorizing license 1401 can include, for example, a license prototype, recipe, and the like. In this manner, local templates typically do have to be employed, as the templates can be defined in the authorizing license 1401. This method can be employed, for example, using a rights language, such as XrML, and the like, that is capable of encoding the recipe to generate the grants within the authorizing license 1401.

[0119] Accordingly, the license request message 1305 transmitted to the License Generation Service 105 can include the parameters 1307, such as a principal identification/key, resource ID, and the like, to allow for the generation of a corresponding license based thereon. The specification for the parameters 1307, for example, can be arranged manually, automatically, before-hand, codified in a WSDL description of the service, predetermined, and the like.

[0120] The method of the exemplary embodiment can provides more flexibility than the exemplary method of FIG. 13. For example, by transmitting the instructions, recipe, license prototype, and the like, for creating a license, advantageously, the License Generation Service 105 can produce various types of licenses, not just licenses defined by the license templates 1301. In addition, the License Generation Service 105 can determine by, for example, evaluating and/or interpreting the authorizing license 1401 transmitted along with the request 1305, if issuance of a license has been authorized.

[0121] The license prototypes can include, for example, grants that are part of the authorizing licenses 1401 within the grant to issue licenses. Thus, the license prototypes can include, for example, grants from which final grants can be created. Such grants are related to the right to issue licenses included in the authorizing license 1401.

[0122] FIG. 15 illustrates an exemplary method for the license 127 generation, based on a license prototypes 1503, for example, within a context of rights language, such as the XrML language, and the like, and that can be in the Networked Services Licensing System 100 of FIG. 1. As shown in FIG. 15, an incoming request 1305 includes the authorizing license 1401, including the license prototype 1503 having zero or more variables "X." Then, at step 1501, for example, the License Generation Service 105 processes the request 1305 to generate the resultant license 127, by employing the license prototype 1503, and resolving the variables from license prototype 1503 with information 1507 from an issued license 1501.

[0123] FIG. 16 illustrates an exemplary method for license generation, from scratch, that can be used in the Networked Services Licensing System 100 of FIG. 1. In FIG. 16, another exemplary method of generating licenses, for example, includes generating licenses from "scratch." In this exemplary method, the License Generation Service 105 typically does not rely on the license templates 1301, and/or the authorizing licenses 1401. Instead, the License Generation Service 105 takes instructions received in the form of detailed parameters 1601 received along with the request 1305 to generate a license, and then generates custom license therefrom. With this exemplary method, the License Generation Service 105 can generate various types of licenses, rights expressions, and the like, based on appropriate detailed parameters 1601. However, the richness of the type of license than can be produced by this exemplary method, for example, can depend on the API employed for programming, and/or messaging, the capabilities of the underlying software, and the like. Accordingly, in this exemplary method, the employed programming and/or messaging interface can be configured so as to be sufficiently detailed to be able to transmit the information included in the detailed parameters 1601 needed to construct a full custom license. For example, such information can include information about the principal, information about the resource, information about the rights, information about conditions, and the like, that can be employed to construct a license.

[0124] Interpretation of a license, such as the license 127, the distribution license 305, and the like, for example, can include determining what right has been granted in the license, what conditions, if any, are associated with such grant, and the like. In an exemplary embodiment, the related process of validating the license can be bundled, associated, related, and the like, with the task of interpreting the license. However, according to a further exemplary embodiment, the license validation process can be separate from the process of license interpretation.

[0125] FIG. 17 illustrates an exemplary workflow for license validation that can be used in the Networked Services Licensing System 100 of FIG. 1. Validating a license, such as the license 127, the distribution license 305, and the like, as the name implies, for example, can include determining if a license is "valid," which typically involves employing a cryptographic technique, and the like. In an exemplary embodiment, the License Validation and Interpretation Service 109, and the like, can perform the license validation process.

[0126] Accordingly, in FIG. 17, at step 1701, for example, a license is received for validation. In an exemplary embodiment, the received license can be encrypted, for example, in order to keep the content thereof confidential, and the like. Accordingly, at step 1703, License Decryption, for example, the license can be decrypted. If, however, the

license is not encrypted, as determined by step 1717, for example, the processes of step 1703 can be bypassed. In addition, if the decryption process on the received license fails, as determined by step 1713, at step 1715, for example, the license can be deemed invalid. In an exemplary embodiment, the encryption and/or decryption processes employed can be performed based on asymmetric cryptographic techniques, symmetrical cryptographic techniques, public key cryptographic techniques, private key cryptographic techniques, and the like.

[0127] At step 1705, Signature Verification and/or Integrity Check, for example, the integrity of the license can be checked, including determining the integrity of the license to insure that the license has not been changed from the when the license was created, digitally signed, and the like, by an authorized issuer, and the like. If, however, the license is not signed, as determined by step 1719, for example, the processes of step 1705 can be bypassed. In addition, if the verification process on the license fails, as determined by step 1713, at step 1715, for example, the license can be deemed invalid.

[0128] Although a license that fails the integrity check may not be trusted, a license that passes the integrity check may still entail the trusting of the key that was used to sign the license. Typically, the signer of the license is the issuer of the license. In an exemplary embodiment, the trusting of the issuer can be part of the license interpretation processes, and the verification process of step 1705 also can be performed based on asymmetric cryptographic techniques, symmetrical cryptographic techniques, public key cryptographic techniques, private key cryptographic techniques, and the like.

[0129] At step 1707, License Revocation Check, for example, in a similar as in the revocation of digitally signed documents, such as digital certificates, and the like, the license also can be revoked for various reasons. If, however, the license is not revoked, as determined by step 1721, for example, the processes of step 1707 can be bypassed. In addition, if the license revocation check on the license fails, as determined by step 1713, at step 1715, for example; the license can be deemed invalid. In an exemplary embodiment, the license revocation step can determine, for example, through appropriate methods, channels, and the like, whether or not the license has been revoked. In addition, in an exemplary embodiment, a revoked license is no longer a valid, and cannot be used to authorize the granting of rights.

[0130] At step 1709, Other Validation, for example, other validity checks, and the like, can be performed on the license. If the license passes the other validity checks employed, at step 1711, for example, the license can be deemed valid. Similarly, if no other validity checks are employed, as determined by step 1723, for example, the processes of step 1709 can be bypassed, and, at step 1711, for example, the license also can be deemed valid. In addition, if the other validity checks on the license fail, as determined by step 1713, at step 1715, for example, the license can be deemed invalid. In an exemplary embodiment, the license can include additional information to attest the validity of the license, such as a validity interval, a specific issuer for the license, and the like, and expired licenses can be considered no longer valid.

[0131] The processes of steps 1707 and 1709 can include determining information within the license, which can entail looking inside the license, and the like, as part of the validation process, according to an exemplary embodiment, because such steps can be more closely related to the validation of a license. However, from a computational point of view, such steps can be considered as part of a license interpretation process, according to a further exemplary embodiment.

[0132] FIG. 18 illustrates exemplary workflows for license interpretation and state tracking that can be used in the Networked Services Licensing System 100 of FIG. 1. Interpreting a license, such as the license 127, the distribution license 305, and the like, for example, can include determining what the license has actually has authorized, conditions of such authorization, and the like. In an exemplary embodiment, as described below, license interpretation can be implemented as a service, wherein the License Validation and Interpretation Service 109, and the like, can perform the license interpretation processes. However, according further exemplary embodiments, a license interpreter can include, for example, any suitable component, device, system, sub-system, mechanism, software, and the like, capable of interpreting a license.

[0133] According to an exemplary embodiment, the Web Services Provider 101, upon receiving the request 121 for the service 119 along with the license 127 from the Web Services Client 103, can validate the license 127, for example, to ensure the integrity, authenticity, and the like, of the license 127. However, according a further exemplary embodiment as described below, the Web Services Provider 101, for example, can off-load the license 127 validation task to the License Interpretation Service 109. Advantageously, the License Interpretation Service 109 can maintain and/or check with external revocation mechanisms, and the like, for example; to determine if a signature associated with the license 127 is valid at the time the license 127 is used, and the like, thus, freeing up such resources and tasks for the Web Services Provider 101.

[0134] Accordingly, in FIG. 18, at step 1801, for example, the Web Services Provider 101 can make the license interpretation request 125, and transmit the license 127 to the License Interpretation Service 109. The Web Services Provider 101 can pass the request 127, for example, via any suitable communications protocol that can allow for the exchange of such queries, and the like. The interpretation of the license 127, for example, can include determining if

the request 121 for the service 119 is authorized, under what conditions, if any, such authorization can be granted, and the like. Thus, such query can be, for example, in the form of "is requester X authorized to access resource Y?" and the like.

[0135] The interpretation of the license 127 also can involve determining, for example, if an issuer trusted by the Web Services Provider 101 has authorized the license 127. If, however, the Web Services Provider 101 does not recognize, cannot trust, and the like, the issuer of the license 127, then a license authorizing the issuer to issue the license 127, such as the distribution license 305, and the like, also can be checked.

[0136] At step, 1807, for example, the result of the license interpretation process can include a response, and the like, from the License Interpretation Service 109 to the Web Services Provider 101, indicating whether or not requested operations, access to services, and the like, granted in a license, such as the license 127, the distribution license 305, and the like, are authorized. Assuming a positive response from the License Interpretation Service 109, and assuming that no further conditions, such obligations 123, are employed, at step 1809, for example, the Web Services Provider can provide a service, such as the service 119, to a client, such as the Web Services Client 103.

[0137] In addition, zero or more obligations 123 that the Web Services Provider 101 may have to perform, for example, as conditions for supplying the service 119, and the like, can result from License Interpretation Service 109 evaluating such conditions specified in the license 127. For example, the obligation 123 can include the Web Services Provider 101 recording the access to the service 119, imposing a time limit for which the services 119 are rendered, and the like. At step 1811, in an exemplary embodiment, for example, the License Interpretation Service 109 also can leverage other services, for example, as specified in the license 127 and/or the distribution license 305, such as retrieving the state information 115, for example, including a count, a limit value, and the like, from some the other service, such as the State Tracking service 111, and the like.

[0138] Thus, according to an exemplary embodiment, a license, such as the license 127, the distribution license 305, and the like, can be used to specify information, such as location information, and the like, for other services, entities, and the like, such as the services, systems, sub-systems, components, devices, and the like, of the Networked Services Licensing System 100 of FIG. 1. In addition, the license interpretation workflow of the exemplary embodiments, for example, can employ any suitable license interpretation protocol, such as the exemplary license interpretation protocol described herein.

[0139] As described above, the License Interpretation Service 109, in the process of interpreting a license, such as the license 127, the distribution license 305, and the like, for example, can employ state information, such as the state information 115, and the like, that can be stored in a state tracking service, such as the State Tracking Service 111, and the like. The location, protocol, and the like, for obtaining the state information 115 can be encoded in the license, for example, based on Web services and/or languages, such as UDDI, WSDL, and the like. By virtue of validating the license, the License Interpretation Service 109 can assure that a link, reference, and the like, specified in the license is for an authorized service, such as the State Tracking Service 111, and the like. Accordingly, at step 1803, for example, the License Interpretation Service 109 transmits a request for state tracking to the State Tracking Service 111.

[0140] The State Tracking Service 111, however, may have to ensure that a requesting entity, such as the License Interpretation Service 109, can be authenticated. In an exemplary embodiment, the License Interpretation Service 109 can be authenticated, for example, by any suitable method, such as by presenting a license, such as the license 127, the distribution license 305, and the like. Then, at step 1805, for example, the State Tracking Service 111 provides the requested state 115 information to the License Interpretation Service 109. In an exemplary embodiment, the transfer of the state information 115 can be made using any suitable protocol, such as the exemplary protocols described herein, and can be made secure, for example, via secured transmission Internet technologies, such as Secure Sockets Layer (SSL) technologies, and the like.

[0141] The License Interpretation Service 109 then can use the state information 115 received from the State Tracking Service 111, at step 1807, for example, to complete the interpretation of the license. In an exemplary embodiment, the state information 115 can in clued, for example, how many times the service 119 has been accessed, a payment record, a time span, and the like.

[0142] As noted above, the License Interpretation Service 109 also can send interpretation information to the Web Services Provider 101, at step 1807, for example, including the obligations 123, and the like. Once the obligations 123 are satisfied, at step 1809, for example, the Web Services Client 103 can exercise a right included in the license 127, such access to the service 119 of the Web Services Provider 101.

[0143] As noted above, however, the use of the service 119 of the Web Services Provider 101 by Web Services Client 103, can entail obligations that may have to be fulfilled by the Web Services Provider 101, for example, such as transfer of updated state information 115, and the like. Accordingly, at step 1811, for example, the Web Services Provider 101 establishes contact with the State Tracking Service 111 to transfer the updated state information 115, and the like. The location, protocol, and the like, for transferring the updated state information 115 to the State Tracking Service 111 can be encoded in the license, for example, based on Web services and/or languages, such as UDDI, WSDL, and the like.

[0144] By virtue of the validity of the license, the Web Services Provider 101 can have assurance that a link, reference, and the like, specified in the license is for an authorized service, such as the State Tracking Service 111, and the like. The State Tracking Service 111, however, may have to ensure that a requesting entity, such as the Web Services Provider 101, can be authenticated. In an exemplary embodiment, the Web Services Provider 101 can be authenticated, for example, by any suitable method, such as by presenting a license, such as the license 127, the distribution license 305, and the like. Once validations, assurances, obligations, and the like, are satisfied, at step 1811, for example, the Web Services Provider 101 can transfer the updated state information 115 to the State Tracking Service 111.

[0145] In order to support the exemplary workflows of the described embodiments, the messages associated with the workflows, for example, used to indicate that a license may have to be employed, to request a license, to indicate that a license is valid, to indicate that a license invalid, and the like, can be encoded, using any suitable messaging protocol, such as the exemplary license protocol described herein. The exemplary license protocol, for example, can be encoded with XrML, XML, and the like, and can be included in messages that are sent between, for example, the Web Service Client and the Web Services Provider 101.

[0146] For example, an exemplary embodiment of the license protocol, employing XML and leveraging the messaging framework of SOAP, is illustrated in Table 1. In an exemplary embodiment, SOAP elements, such as the indication of a fault through a <fault> element during the processing of a message, and the like, can be used in accordance to the SOAP specification.

Table 1: Exemplary License Protocol (XML/SOAP Messaging Framework)

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
The Web Services Provider 101 response after the service 119 initiation without the license 127 by the Web Services Client 103. In this example, the protocol to indicate that the license 127 was not provided can be encapsulated in the <lic:faultDetails> element, shown in bold, and can include a "message" part that can be human readable, and an "errorcode" part for machine processing. The message part can be used for debugging.	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license"> <body> <fault> ... <details> <lic:faultDetails> <message> license missing </message> <errorcode> 0001 </errorcode> <lic:faultDetails> </details> </fault> </body> </envelope>
The Web Services Provider 101 response after the Web Services Client 103 service 119 initiation with an error in the license 127. In this example, the protocol to indicate that there was a fault	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license"> <body> <fault> ... <details>

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
condition with the license 127 can be encapsulated in the <lic:faultDetails> element, shown in bold, and can include: a "message" part that can be human readable, and an "errorcode" part for machine processing. The message part can be used for debugging. The errorcode part can be a number or a string and can include a list of error codes indicating different types of fault conditions. For example, 0034 for expired license, 0035 for un-trusted license, and the like.	**<lic:faultDetails>** **<message> Expired License </message>** **<errorcode> 0034 </errorcode>** **<lic:faultDetails>** </details> </fault> </body> </envelope>
The error message can be followed by this message, including information for how to obtain the license 127. In this example, the fault message and the license information message can be bundled together. In the sample message, the fault message indicates that the license 127 was not provided, and the other message provides information on where to obtain the license 127. The element <lic:RetrievalInfo>, shown in bold, provides information on where to get the license 127 and what kind of license can be employed. In the sample message, a UDDI reference can be given, corresponding to the License Generation Service 105. In addition, a license with a grant of principal equal to the identity of the requester and of right "retrieveAnyDocument" can be employed. Further, a particular issuer can be employed as the issuer of the license 127. The license prototype 1503 or the type of license 127 employed to access the service 119 can be encoded with a rights language (for example, XrML, as in this example).	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license" xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <body> <fault> ... <details> **<lic:faultDetails>** **<message> License Missing </message>** **<errorcode> 0034 </errorcode>** **<lic:faultDetails>** </details> </fault> **<lic:RetrievalInfo>** **<x:serviceReference>** **<x:uddi>** **<x:serviceKey>** **<x:uddi>E234s-asdfa-... </x:uddi>** **</x:serviceKey>** **</x:uddi>** **</x:serviceReference>** **<x:forAll varName= "requester" />** **<x:grant>** **<x:principal varRef= "requester" />** **<ws:retrieveAnyDocument />** **</x:grant>** **<x:issuer>** .... **</x:issuer** **</lic:retrievalInfo>** </body> </envelope>
The Web Services Client 103	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope"

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
requesting the license 127. In this example, a requester, such as the Web Services Client 103, sends a message to the License Generation Service 105 in order to obtain the license 127. (For example, it can be assumed that the requester has been authorized to get a license and knows how to locate and interface with the License Generation Service 105). The message encapsulates the following elements, for example: A credential element in the <wsse:security> element in the <header> section –in the form of an X509 certificate A request in the <lic:request> element in the <body> section, shown in bold. The <lic:request> element can include a prototype grant identifying the service in question. It also can say that the principal is to be resolved at the time the license 127 is created. Also, there can be a type associated with the <lic:request> element. The output of such request (for example, if authorized) can be a license 127 that can be transmitted inside a message to the requester. There are numerous ways to pass the information in the message. The example is one of such many ways. Each of the previously described methods can employ a separate "flavor" of the protocol.	xmlns:lic= "http://www.xrml.org/2002/license" xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <header> <wsse:security xmlns:wsse= "..."> <wsse:binarySecurityToken *id= "myToken"* valueType= "wsse:x509v3" MIIEZzCCA9CgAwIBglQEmtJZC0... </wsse:binarySecurityToken> </wsse:security> </header> <body> <**lic:request type= "licenseGen"**> <**x:forAll varName= "requester"** > < **"the wsse:security value"** /> </**forAll**> <**x:grant**> <**x:principal varRef= "requester"** /> <**ws:access** /> <**x:serviceReference**> <**x:uddi**>**E234s-asdfa-...** </**x:uddi**> <**x:details**> ... </**x:details**> </**x:serviceReference**> </**x:grant**> </**lic:request**> </body> </envelope>
The License Generation Service 105 delivers the license 127 to a requester, such as Web Services Client 103. In this example, the license can be returned as a fully formed license as part of the body of the message. With SOAP, typically, there is no need for an additional protocol, as shown in the example. However, with other mechanisms, there may be a need to include the license within a "wrapper" in the form of <lic:Response>...</lic:Response> to indicate that the enclosed license is a	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license" xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <header> ... </header> <body> <x:license> <x:grant> ... </x:grant> ... </x:license>

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
response to a request and not a license that was generated for other purposes.	... </body> </envelope>
The Web Services Client 103 transmits the license 127 (for example, as token to gain access to the service 119) with service initiation message. In this example, transmitting the license 127 as a token for access to the service 119, leverages the semantics of the messaging protocol, in SOAP, which is a security token passed in the header portion of the message. With SOAP, typically, there is no need for an additional protocol, as shown in the example. However, with other mechanisms, there may be a need to include the license within a "wrapper" in the form of <lic:security>...</lic:security> to indicate that the enclosed license 127 is a license to gain access to the service 119.	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license" xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <header> <wsse:security xmlns:wsse= "..."> </wsse:security> <x:license> <x:grant> ... </x:grant> ... </x:license> </wsse:security> ... </header> <body> ... </body> </envelope>

[0147] The exemplary license interpretation protocol, as illustrated in Table 2, for example, can be part of the license protocol. The license interpretation protocol is discussed separately, for the sake clarity. The Web Services Provider 101 can use the license interpretation protocol, for example, when invoking the License Interpretation Service 109. Similar to the license protocol, the license interpretation protocol can be implemented so as to leverage a messaging exchange protocol, for example, SOAP, and the like, and transmit XrML messages, XML messages, and the like. Table 2 shows the exemplary license interpretation protocol, for example, as XML leveraging the messaging framework of SOAP, and the rights language XrML.

Table 2: Exemplary Interpretation Protocol (XML/SOAP Messaging Framework)

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
The Web Services Provider 101 sends a request message 125 to the License Interpretation Service 109 to request	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license"

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
the interpretation of a license, such as the license 127. In this example, the message can include several parts: In the header, the Web Services Provider 101 can sends credential, including a license that authorizes the access or use of the service The body of the message starts with the request of type "licenseInterpret," shown in bold. This is to indicate that the request is for interpreting a license. Within this element are the parameters that the interpreter employs as input. The example shows that a principal and a resource are passed as parameters signifying that the service will find the granted rights that match those parameters. Following the request is the license or licenses to be interpreted.	xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <header> ... <wsse:security xmlns:wsse= "..."> ... </wsse:security> <x:license> <x:grant> ... </x:grant> ... </x:license> </wsse:security> ... </header> <body> <**lic:request type= "licenseInterpret"** **ID= "1234-1234-1234-1234"**> <**lic:parameter principal= "x:keyholder"**> **MIIEZzCCA9CgAwIBgIQEmtJZC0...** </**lic:parameter**> <**lic:parameter resource= "x:uddi"**> **E234s-asdfa-...** </**lic:parameter**> **...** </**lic:request**> <x:license> <x:grant> ... </x:grant> ... </x:license> ... </body> </envelope>
The License Interpretation Service 109, after the license interpretation request 125, returns the results in a message. In this example, a response 123 corresponding to the request is encapsulated within the <lic:response> element, shown in bold. In this example, the returned parameters are grant fragments (for example, as defined in the rights language) that match the principal and the resource in the original request. Certain conditions can also be resolved in the license interpreter and the result could	<?xml version ='1.0'> <Envelop xmlns= "http://www.w3c.org/2002/06/soap-envelope" xmlns:lic= "http://www.xrml.org/2002/license" xmlns:x= "http://www.xrml.org/2002/xrmlCore" > <header> ... </header> <body> <**lic:response type= ID= "1234-1234-1234-1234"**> <**x:grant**> <**ws:access/**> </**x:grant**> <**x:grant**> <**ws:execute/**

Step in Workflow	Soap Message. Elements of the license protocol are prefixed with "lic:"
be "simpler conditions" that are easier to validate by the requester. The result in this example indicates that the access right has been granted –with no conditions or obligations, and the right to execute has also been granted, but with the obligation to track the exercise of this right as specified by the <x:trackReport> element (for example, defined in the rights language XrML)	<x:trackReport> <x:serviceReference> <x:uddi>E234s-asdfa-... </x:uddi> <x:details> ... </x:details> </x:serviceReference> </x:trackReport> </x:grant> ... </lic:response> ... </body> </envelope>

[0148] In an exemplary embodiment, the state tracking protocol can include any suitable protocol, public, private, proprietary, standardized, the exemplary protocols as described herein, and the like, that can be used to retrieve, transfer, and the like, information, such as the state information 115, and the like, to and from a service, such as the State Tracking Service 111, and the like. Accordingly, the state tracking protocol can be used for retrieving a count of how many times a service, such as the service 119, and the like, has been exercised, for sending the exercise count, for storing an exercise count, and the like.

[0149] In addition, the exchange of certain types of information, such as payment information, time information, and the like, may already be standardized in a protocol by other industries, in which case, according to a further exemplary embodiment, such a standardized protocol can be included in the state tracking protocol. Further, according to a still further exemplary embodiment, a protocol may employed that can depend on the specialization, implementation, and the like, of the State Tracking Service 111. For example, if the State Tracking Service includes a database, then the retrieval and storage of information can be performed via a database query mechanism, and the like.

[0150] Exemplary use scenarios, business applications, and the like, that can be supported by the exemplary embodiments of the Networked Services Licensing System 100 of FIG. 1, as will now be described.

[0151] FIGs. 19 illustrates an exemplary workflow for specifying a license that can be used in the Networked Services Licensing System 100 of FIG. 1. In this example, a service, such as a Web-based License Generation and Interpretation Service 1907 based on, for example, the License Generation 105 and Interpretation 109 Services of the exemplary embodiments, and the like, can allow for the specification of rights, the interpretation of rights, and the like, for generating a license, such as the license 127 and/or the distribution license 305, and the like. According to an exemplary embodiment, the License Generation and Interpretation Service 1907, for example, can be employed as a building block for systems, such as a Rights Clearing Service, a Digital Asset Management System, a Digital Rights Management System, and the like.

[0152] The License Generation and Interpretation Service 1907, in an exemplary embodiment, can include, for example, providing a user interface, such as a Graphical User Interface (GUI), and the like, converting user input into a rights expression, such as a license, based on a rights language, such as XrML, and the like. The License Generation and Interpretation Service 1907, according to a further exemplary embodiment, for example, can also provide one or more user interfaces, each specializing in a particular format, industry, and the like. For example, the License Generation and Interpretation Service 1907 can provide a user interface for video formats, another user interface for music formats, a still further user interface for electronic books, and the like. Advantageously, providing user interfaces tailored to the specific details and/or intricacies of a particular audience, for example, can be a value-added feature, and the like, of the License Generation and Interpretation Service 1907.

[0153] Accordingly to an exemplary embodiment, the License Generation and Interpretation Service 1907, for example, can include accepting rights queries, processing the rights queries against corresponding rights expressions, and the like. For example, an exemplary rights query can be of the form "Does John M., who is an employee of Company N, have the right to purchase up to $1000 worth of supplies from Supplier P?," and the like. The output from such a query, for example, can include an assertion about what rights are available, what conditions are attached to such rights, and the like. The License Generation and Interpretation Service 1907 can add further value, for example, by

providing one or more user interfaces that facilitate user input for a particular type of rights query, and the like.

[0154] Advantageously, employing the same entity for providing both rights specification, and rights interpretation functions, for example, allows for an increase in consistency, accuracy, and the like, in interpreting the rights. In other words, a system that creates the rights specification typically is better equipped to apply the same rules when interpreting such rights. In an exemplary embodiment, the rights expression, the rights expression definitions, the rights expression interpretations, and the like, can be based on any suitable standard, including industry standards, and the like.

[0155] Accordingly, in an exemplary embodiment, a user 1919, an author, for example, wishes to specify the rights associated with some type content in relation to a contract with a publisher. An authoring application 1909 that the user 1919 employs does not provide a way to specify rights metadata for the content, but can call a Web service, such as the License Generation and Interpretation Service 1907 that provides such a function.

[0156] Accordingly, at step 1901, for example, the authoring application connects to License Generation and Interpretation Service 1907 that provides rights specification, interpretation, and the like. For example, the License Generation and Interpretation Service 1907 can specialize in certain industries and provide a user interface with terminology, contract templates, and the like, that can be used and understood in that particular industry, trade, and the like. The user 1919 interacts with the License Generation and Interpretation Service 1907, and, at step 1903, for example, the License Generation and Interpretation Service 1907 converts the information the user 1919 provides into a rights expression, for example, an unsigned license, based on XrML, and the like. The unsigned license is then returned, conveyed, transmitted, and the like, to the user 1919, and the user 1919 can digitally sign the license.

[0157] At step 1905, for example, the user 1919 can send the signed license, for example, together with the associated content, to a Digital Asset Management System 1913 of the publisher, and, for example, including a license store 1915, such as a database and the like. The content can now be managed by the Digital Asset Management System 1913, for example, within a domain, and the like, of the publisher.

[0158] FIG. 20 illustrates an exemplary workflow for interpreting a license that can be used in the Networked Services Licensing System 100 of FIG. 1. For example, in FIG. 20, during a production workflow for a publication, Bob, a rights specialist, wishes to query the rights of a particular asset of the Digital Asset Management System 1913. In this example, the rights of the asset are encapsulated, for example, by an XrML license. The Digital Asset Management System 1913, for example, not having a capability to interpret licenses, for example, by design, because a Web service can provide more specialized capabilities, and the like, accesses the License Generation and Interpretation Service 1907, which provides, for example, an intuitive user interface, such as a GUI, and the like. Advantageously, the License Generation and Interpretation Service 1907 can specialize in interpretation of certain types contracts, licenses, and the like, and allow the operation of the user interface to query the rights that can be employed for a particular publication. In an exemplary embodiment, the License Generation and Interpretation Service 1907 can include, for example, an indexed database where licenses are stored, organized, and the like.

[0159] Accordingly, at step 2001, for example, Bob sends a query along with the XrML license, for example, through the Digital Asset Management System 1913, to the License Generation and Interpretation Service 1907. Then, at step 2003, for example, the License Generation and Interpretation Service 1907 interprets the rights included in the license based on the query request, and returns the result of the query to Bob.

Exemplary Workflow for Accessing the License Issuing and Interpretation Service 1907

[0160] Although the exemplary rights processing workflow described above can be a function provided by a Web service, such as the License Generation and Interpretation Service 1907, the workflow does not describe the process for calling, accessing, and the like, the License Generation and Interpretation Service 1907. For example, in an exemplary embodiment, the XrML license is not used for accessing the License Generation and Interpretation Service 1907. Accordingly, the rights processing functions can be generic functions provided by a Web service, such as the License Generation and Interpretation Service 1907, and the like, and, for example, can be described with any suitable standards-based language for describing Web services, such as WSDL, and the like.

[0161] In many business scenarios, however, it can become advantageous to manage access to a service, such as the License Generation and Interpretation Service 1907, and the like. For example, a user 2005, the owner of the Web-based License Issuing and Interpretation Service 1907 has been providing the service to anyone that can discover his offering, can use the service, and the like. However, the License Generation and Interpretation Service 1907 of the user 2005 has become quite successful, and the user 2005 now wishes to commercialize the License Issuing and Interpretation Service 1907. According to an exemplary embodiment, the user 2005 can add an e-commerce capability to the License Issuing and Interpretation Service 1907.

[0162] Accordingly, the user 2005, for example, could add an e-commerce package to the License Issuing and Interpretation Service 1907, which can entail the creation of various mechanisms, such as a customer account processing mechanism, a financial transaction processing mechanism, a login and password processing mechanism, and the like.

However, such a service can create barriers for the service and its customers. For example, the login process, the handling forgotten passwords, the processing of payments, the determining of how much to charge, the determining of what methods to employ, and the like, could become cumbersome.

[0163] Therefore, according to a further exemplary embodiment, the user 2005 can configure the License Issuing and Interpretation Service 1907, for example, such that access is granted based on a presentation of a license, for example, manually, automatically, and the like. Conceptually, such a system can include, for example, submitting a license during the initial communication protocol with the License Issuing and Interpretation Service 1907. In an exemplary embodiment, a client of the License Issuing and Interpretation Service 1907 and the License Issuing and Interpretation Service 1907 can follow any suitable license protocol, such as the exemplary license protocol described herein. In this exemplary embodiment, a license, such as an XrML license, and the like, can be presented, for example, when an application communicates with the License Issuing and Interpretation Service 1907. If the license validates, the services of the License Issuing and Interpretation Service 1907 can be rendered.

[0164] In the examples of FIGs. 19 and 20, the authoring application can be configured to include the capability to present a license, for example, when the application requests services from License Issuing and Interpretation Service 1907. FIG. 21 illustrates an exemplary workflow for controlling consumption of a service that can be used in the Networked Services Licensing System 100 of FIG. 1. In FIG. 21, at step 2101, for example, authoring application 1909 of the user 1919 communicates with the License Issuing and Interpretation Service 1907 and requests service. At step 2103, for example; during the initial protocol, a license is presented in order to access the services of the License Issuing and Interpretation Service 1907. Then, at step 2105, for example, upon acceptance of the license, the License Issuing and Interpretation Service 1907 can render its services.

[0165] The user 2005 now ponders the question of who would issue the licenses that are used to access the License Issuing and Interpretation Service 1907. According to an exemplary embodiment, the user 2005 can configure the License Issuing and Interpretation Service 1907 to manage the issuing of the licenses. However, this can become quite taxing to the system and himself.

[0166] In addition, the user 2005 would have develop and maintain an e-commerce site and a database for his customers. However, the user 2005 figures that managing a customer database is not something that will add value to the License Issuing and Interpretation Service 1907, and does not see the economic potential of maintaining and/or data-mining the customer database.

[0167] Accordingly, the user 2005 would rather keep the License Issuing and Interpretation Service 1907 simple, allowing the user 2005 to focus on the basic capabilities and functionality of the service. Therefore, according to a further exemplary embodiment, the user 2005 can configure the License Issuing and Interpretation Service 1907 to employ licenses, for example, that can be issued by a trusted third party, bundled with the authoring application 1909, and the like.

[0168] FIG. 22 illustrates an exemplary workflow for issuing licenses by a third party that can be used in the Networked Services Licensing System 100 of FIG. 1. For example, in an exemplary embodiment, the user 2005 can issue licenses to business partners of the user 2005, for example, granting the right to issue licenses for access to License Issuing and Interpretation Service 1907, such as the distribution license 305, and the like. The business partners of the user 2005 then can issue the distribution licenses to end-users, such as the user 1919.

[0169] For example, the business partners the user 2005 can include companies, for example, such as Company ABC 2207 that creates and sells the authoring applications 1909, such as word processors, image creation software, and the like. At step 2201, for example, the user 2005 can make a business deal with the Company ABC 2207, for example, based on granting the Company ABC 2207 the right to issue licenses for access to the License Issuing and Interpretation Service 1907, and the like, at step 2203. Then, at step 2205, for example, the licenses for accessing the License Issuing and Interpretation Service 1907 can be issued on-demand, bundled with the authoring applications 1909, and the like, by the Company ABC 2207. Advantageously, in this exemplary embodiment, the user 2005 can bundle access to the License Issuing and Interpretation Service 1907 with a third party application, such as the authoring applications 1909, and the like.

[0170] In an exemplary embodiment, the user 2005 and/or the Company ABC can use a third party service, such the License Generation and Issuing Service 105, and the like, to generate the licenses of the exemplary embodiments. In addition, signature keys can to be obtained to sign the licenses, for example, through security services, such as the Trust Authority Service 113, and the like.

[0171] According to the exemplary embodiments, the user 2005 can commercialize the Web-based License Issuing and Interpretation Service 1907, advantageously, without adding the resources employed to run and manage an e-commerce system. The user 2005 can determine the conditions for access to the License Issuing and Interpretation Service 1907, for example, by employing the licenses of the exemplary embodiments, such as XrML licenses, and the like. Advantageously, according to the exemplary embodiments, the user 2005 does not have to deal, for example, with managing of the customer base, and the like. The improved License Issuing and Interpretation Service 1907, for example, can entail some improvement to the Web services software, such as the capability to process licenses, but

the such changes can be negligible in comparison with the deployment of a full-fledge e-commerce setup.

[0172] According to exemplary embodiments, the user 2005 can employ various compensation methods that, advantageously, can be described in a rights language, such as XrML, and the like. For example, according to an exemplary embodiment, a non-tracked, not encoded in a license, out of band, and the like, compensation method can be employed. In this exemplary compensation method, the user 2005 can arrange a flat-fee, per-use, and the like, deal, whereby the user 2005 can issue a distribution license, for example, granting the Company ABC 2207 an unlimited right to issues licenses for accessing the License Issuing and Interpretation Service 1907. The Company ABC 2207 can compensate the user 2005, for example, based on the number of licenses for accessing the License Issuing and Interpretation Service 1907 the Company ABC 2207 bundles with its software, such as the authoring applications 1909, based on a one-time payment, and the like. In this embodiment, the user 2005 would have to trust the data that the Company ABC 2207 collects, for example, with respect to software sales, and the like.

[0173] According to an exemplary embodiment, a tracked, encoded in a license, per distributor use, and the like, compensation method can be employed. In this exemplary compensation method, the user 2005 can employ, for example, compensation rules, and the like, that can be encoded in the distribution license the user 2005 issues to the Company ABC 2207. For example, the distribution license can be configured to specify that every time the right to issue a license for accessing the License Issuing and Interpretation Service 1907 is exercised by the Company ABC 2207, conditions may have to be met, such as the making of a payment of a certain amount to an account of the user 2005, that each use of the distribution license is tracked and settled through other means, and the like. Advantageously, with this exemplary embodiment, accurate, trustworthy, and the like, sales information can be made possible, because accurate tracking can be enabled.

[0174] According to an exemplary embodiment, a tracked, encoded in a license, per end-user use, and the like, compensation method can be employed. In this exemplary compensation method, the distribution license that the user 2005 issues to the Company ABC 2207 can also specify, for example, that when an end-user license is issued, for example, by the Company ABC 2207, certain rights, conditions, and the like, may have to be specified in the end-user licenses that the Company ABC 2207 issues. For example, the user 2005 can specify in the distribution license that the end-user usage of the licenses issued by the Company ABC 2207 for accessing the License Issuing and Interpretation Service 1907 be tracked, and the like. Accordingly, when the License Issuing and Interpretation Service 1907 of the user 2005 receives, processes, and the like, a license from the user 1919, the license can specify the parameters to track the usage of the license. Advantageously, with this exemplary embodiment, at the end of an accounting period, such data can be gathered, processed, and the like, for payment.

[0175] In an exemplary embodiment, the Company ABC 2207 may realize that by bundling additional services, the Company ABC 2207 can increase its competitive advantage in the marketplace. In this exemplary embodiment, for example, the Company ABC 2207 can reach out to other companies, Web services, and the like, such as document translator services, multilingual spell checker services, editorial tool services, and the like. Then, the Company ABC 2207 can make business deals with such other companies and include licenses that can be used to access such additional services. Advantageously, with this exemplary embodiment, the Company ABC can aggregate several services to bundle with its products:

[0176] In an exemplary embodiment, each license, such as an XrML license, and the like, can be used to express individual rights, conditions, and the like, for each the aggregated services. For example, the license for Web service B can be expressed with a right for an unlimited use, the license for Web service C can be expressed with a condition for a maximum count of 10 uses, and the like. Advantageously, with this exemplary embodiment, employing licenses that can determine the rules for access and use of a service can facilitate service aggregation.

[0177] According to an exemplary embodiment, the user 2005 can issue distribution licenses to his business partners, and, in turn, his business partners can issue licenses to the end-users for accessing the License Issuing and Interpretation Service 1907. This exemplary embodiment illustrates a single tier distribution model, wherein the business partners of the user 2005 can be the distributors for access to the services of the user 2005.

[0178] FIG. 23 illustrates an exemplary workflow for syndication of a service that can be used in the Networked Services Licensing System 100 of FIG. 1. According to a further exemplary embodiment, however, the user 2005 can focus on the technical details of the Web-based License Issuing and Interpretation Service 1907, and, for example, outsource business dealings, and the like, with companies, such as the Company ABC 2207, and the like. In this exemplary embodiment, in essence a syndication model, the user 2005 can grant a syndication agent, such as a Syndication Company 2311, a syndication license that grants the Syndication Company 2311 the right to issue distribution licenses that grant the ABC Company 2207 the right to issue licenses for accessing the License Issuing and Interpretation Service 1907.

[0179] The Networked Services Licensing System 100, for example, as described with respect to FIGs. 1-23, can store information relating to various processes described herein. This information can be stored in one or more memories, such as a hard disk, optical disk, magneto-optical disk, RAM, and the like, of the devices and sub-systems of Networked Services Licensing System 100. One or more databases of the devices and subsystems of the Networked

Services Licensing System 100 of FIG. 1 can store the information used to implement the exemplary embodiments. The databases can be organized using data structures, for example, records, tables, arrays, fields, graphs, trees, lists, and the like, included in one or more memories, such as the memories listed above, and the like.

[0180] All or a portion of the Networked Services Licensing System 100, for example, as described with respect to FIGs. 1-23, can be conveniently implemented using one or more general-purpose computer systems, microprocessors, digital signal processors, micro-controllers, and the like, programmed according to the teachings of the exemplary embodiments. Appropriate software can be readily prepared by programmers of ordinary skill based on the teachings of the exemplary embodiments. In addition, the Networked Services Licensing System 100 can be implemented by the preparation of application-specific integrated circuits or by interconnecting an appropriate network of conventional component circuits.

[0181] Although the present invention is described in terms of exemplary workflows, other workflows are possible, as will be appreciated by those skilled in the relevant art(s). For example, during services initiation, typically a license is presented at the time of service request. However, it is possible that the license be presented at another time, cached, and the like, so that further service request do not entail the submission of a license. A license could be "pre-presented" and retained by the Web service, the client, and the like. The license could, after being pre-presented, be "pre-validated." In such a case, when a request for accessing services is made it would be determined if the request is from an authorized requestor, and the license would be interpreted.

[0182] Although the exemplary workflows are described as functional steps associated with the exemplary devices of the Networked Services Licensing System 100, one or more of the functional steps of the exemplary workflows can be performed by any suitable device or devices, such as one or more general-purpose computer systems, microprocessors, digital signal processors, micro-controllers, and the like, programmed according to the teachings of the exemplary embodiments, as will be appreciated by those skilled in the relevant art(s).

[0183] Although the present invention is described in terms of Web services, the present invention is applicable to other services, such as any suitable distributed network service, and the like, as will be appreciated by those skilled in the relevant art(s).

[0184] Although the present invention is described in terms of a Web services model, the present invention is applicable to other models, such as a syndication model that is replicated for services, and the like, as will be appreciated by those skilled in the relevant art(s). For example, in an exemplary embodiment, a third party collects services from service providers and makes them available singly or in combination to users as a third party service.

[0185] In such an example, the Web Services Provider 101 may not or, cannot provide the syndication function, but they can set some of the conditions, rights, and the like, for the services. This exemplary embodiment, thus, enables the third party service provider to provide, for example, access and tracking services to a user of the third party service on behalf of the owners of the services. Advantageously, the services market, especially for component services, can be greatly enabled, accelerated, and the like, with this exemplary embodiment. By contrast, conditional access typically cannot handle such examples well and/or may be impractical.

[0186] Although the present invention is described in terms of an "on-line" mode of operation, the present invention is applicable to other modes of operation, such as "offline" modes, and the like, as will be appreciated by those skilled in the relevant art(s). For example, a hard drive on a personal computer (PC) can include license generating software, a license, and license interpretation software. The communications protocol of the exemplary embodiments, in this example, can be employed for communications within the hard drive.

[0187] Advantageously, the Web Services Client 103 can present a validated license and obtain access to a Web service without having to be on-line at the time the service is obtained. For example, the service could reside on the PC hard drive, such as where the service includes the execution of a computer program, or could be obtained from or through another device, such as a server or CD or other storage medium.

[0188] To the extent an on-line transaction is employed for some reason, such as for making a financial payment, the on-line session can be conducted at a time other than at the time the request for the use of the service is made. In the case of a financial transaction, the transaction can be made off-line using a digital storage device, such as a pre-paid "smart card" and the like. In addition, any suitable information to be exchanged can be exchanged using a physical storage device instead of an on-line communication. For example, a license can be presented by inserting a smart card into the PC.

[0189] While the present invention have been described in connection with a number of exemplary embodiments and implementations, the present invention is not so limited, but rather covers various modifications, equivalent arrangements, and the like, which fall within the purview of the appended claims.

[0190] THE FOLLOWING IS A LIST OF FURTHER PREFERRED EMBODIMENTS OF THE INVENTION:

Embodiment 1. A method for controlling consumption of a distributed network service (119) in accordance with rights expression information (127) associated with said distributed network service (119) and specifying a manner of use of said distributed network service (119), said method comprising:

determining said rights expression information (127) associated with said distributed network service (119), said rights expression information (127) indicating a manner of use of said distributed network service (119); and

controlling consumption of said distributed network service (119) based on said rights expression information (127).

Embodiment 2. The method as recited in embodiment 1, further comprising:

transmitting said rights expression information (127) from a client (103) to a provider (101) of said distributed network service (119).

Embodiment 3. The method as recited in any one of embodiments 1 to 2, further comprising:

receiving said rights expression information (127) at said client (103) from a rights expression information issuing service (105).

Embodiment 4. The method as recited in any one of embodiments 1 to 3, further comprising:

receiving a right to issue (305) said rights expression information (127) at said rights expression information issuing service (105) from a business network (107) associated with said rights expression information issuing service (105).

Embodiment 5. The method as recited in any one of embodiments 1 to 4, further comprising:

interpreting said rights expression information (127) transmitted from said client (103) to said provider (101) at a rights expression information interpretation service (109) to determine if said provider (101) has allowed access to said distributed network service (119).

Embodiment 6. The method as recited in any one of embodiments 1 to 5, further comprising:

interpreting said rights expression information (127) transmitted from said client (103) to said provider (101) based on state data (115) associated with said rights expression information (127) and received from a state tracking service (111).

Embodiment 7. The method as recited in any one of embodiments 1 to 6, further comprising:

receiving at least a portion of said state data (115) at said state tracking service (111) from said provider (101).

Embodiment 8. The method as recited in any one of embodiments 1 to 7, further comprising:

configuring said rights expression information issuing service (105), said rights expression information interpretation service (109), and said state tracking service (111) as a middle layer provided between a trust authority service (113) and said service provider (101) and said client (103), wherein said trust authority service (113) manages trust relationships between said rights expression information issuing service (105), said rights expression information interpretation service (109), and said state tracking service (111).

Embodiment 9. The method as recited in any one of embodiments 1 to 7, further comprising:

configuring said rights expression information issuing service (105), said rights expression information interpretation service (109), and said state tracking service (111) as specialized services provided by a specialized service provider provided between a trust authority service (113) and said service provider (101) and said client (103), wherein said trust authority service (113) manages trust relationships between said rights expression information issuing service (105), said rights expression information interpretation service (109), and said state tracking service (111).

Embodiment 10. The method as recited in embodiment 9, wherein said trust authority service (113) attests to information included in a trust certificate (117) associated with said rights expression information (127).

Embodiment 11. The method as recited in embodiment 1, further comprising:

expressing said rights expression information (127) using a rights expression language.

Embodiment 12. The method as recited in embodiment 1, wherein said rights expression language includes a grammar-based rights expression language.

Embodiment 13. The method as recited in embodiment 12, wherein said grammar-based rights expression language includes extensible rights Markup Language (XrML).

Embodiment 14. The method as recited in embodiment 1, wherein said step of controlling access, comprises: authorizing access to said distributed network service (119) based on said rights expression information (127).

Embodiment 15. The method as recited in embodiment 1, further comprising:

specifying in said rights expression information (127) identification information for said distributed network service (119).

Embodiment 16. The method as recited in embodiment 1, further comprising:

specifying in said rights expression information (127) identification information for a service that is associated with said distributed network service (119).

Embodiment 17. A computer system for controlling consumption of a distributed network service (119) in accordance with rights expression information (127) associated with said distributed network service (119) and specifying a manner of use of said distributed network service (119), said system comprising:

a distributed network services provider (101) configured to provide said distributed network service (119);

a client (103) of said provider (101) configured to consume said distributed network service (119); a license issuing server (105) configured to determine said rights expression information (127) associated with said distributed network service (119), said rights expression information (127) indicating a manner of use of said distributed network service (119); and

a license interpretation server (109) configured to control consumption of said distributed network service (119) based on said rights expression information (127).

Embodiment 18. A computer-readable medium carrying one or more sequences of one or more instructions for controlling consumption of a distributed network service (119) in accordance with rights expression information (127) associated with said distributed network service (119) and specifying a manner of use of said distributed network service (119), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the following steps:

determining said rights expression information (127) associated with said distributed network service (119), said rights expression information (127) indicating a manner of use of said distributed network service (119); and

controlling consumption of said distributed network service (119) based on said rights expression information (127).

Embodiment 19. A system for controlling consumption of a distributed network service (119) in accordance with rights expression information (127) associated with said distributed network service (119) and specifying a manner of use of said distributed network service (119), said system comprising:

means (105) for determining said rights expression information (127) associated with said distributed network service (119), said rights expression information (127) indicating a manner of use of said distributed network service (119); and
means (109) for controlling consumption of said distributed network service (119) based on said rights expres-

sion information (127).

Embodiment 20. A method for controlling consumption of a networked service (119) in accordance with rights expression information (127) associated with said networked service (119) and specifying a manner of use of said networked service (119), said method comprising:

determining said rights expression information (127) associated with said networked service (119), said rights expression information (127) indicating a manner of use of said networked service (119);

controlling consumption of said networked service (119) based on said rights expression information (127);
transmitting said rights expression information (127) from a client (103) to a provider (101) of said networked service (119);

receiving said rights expression information (127) at said client (103) from a rights expression information issuing server (105); and

interpreting said rights expression information (127) transmitted from said client (103) to said provider (101) at a rights expression information interpretation server (109) to determine if said provider (101) has allowed access to said networked service (119), and based on state data (115) associated with said rights expression information (l 27) and received from a state tracking server (111),

wherein said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111) are configured as a middle layer provided between a trust authority server (113) and said service provider (101) and said client (103), and
said trust authority server (113) manages trust relationships between said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111).

Embodiment 21. A computer system for controlling consumption of a networked service (119) in accordance with rights expression information (127) associated with said networked service (119) and specifying a manner of use of said networked service (119), said system comprising:

a rights expression information issuing server (105) configured to determine said rights expression information (127) associated with said networked service (119), said rights expression information (127) indicating a manner of use of said networked service (119); and

a rights expression information interpretation server (109) configured to control consumption of said networked service (119) based on said rights expression information (127),

wherein said rights expression information (127) is transmitted from a client (103) to a provider (101) of said networked service (119),
said rights expression information (127) is received at said client (103) from said rights expression information issuing server (105), said rights expression information (127) transmitted from said client (103) to said provider (101) is interpreted at said rights expression information interpretation server (109) to determine if said provider (101) has allowed access to said networked service (119), and based on state data (115) associated with said rights expression information (127) and received from a state tracking server (111),
said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111) are configured as a middle layer provided between a trust authority server (113) and said service provider (101) and said client (103), and
said trust authority server (113) manages trust relationships between said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111).

Embodiment 22. A computer-readable medium carrying one or more sequences of one or more instructions for controlling consumption of a networked service (119) in accordance with rights expression information (127) associated with said networked service (119) and specifying a manner of use of said networked service (119), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the following steps: ,

determining said rights expression information (127) associated with said networked service (119), said rights

expression information (127) indicating a manner of use of said networked service (119); controlling consumption of said networked service (119) based on said rights expression information (127);

transmitting said rights expression information (127) from a client (103) to a provider (101) of said networked service (119); receiving said rights expression information (127) at said client (103) from a rights expression information issuing server (105); and

interpreting said rights expression information (127) transmitted from said client (103) to said provider (101) at a rights expression information interpretation server (109) to determine if said provider (101) has allowed access to said networked service (119), and based on state data (115) associated with said rights expression information (127) and received from a state tracking server (111),

wherein said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111) are configured as a middle layer provided between a trust authority server (113) and said service provider (101) and said client (103), and
said trust authority server (113) manages trust relationships between said rights expression information issuing server (105), said rights expression information interpretation server (109), and said state tracking server (111).

Embodiment 23. A system for controlling consumption of a networked service (119) in accordance with rights expression information (127) associated with said networked service (119) and specifying a manner of use of said networked service (119), said system comprising:

means (105) for determining said rights expression information (127) associated with said networked service (119), said rights expression information (127) indicating a manner of use of said networked service (119);

means (109) for controlling consumption of said networked service (119) based on said rights expression information (127); and

means (103) for transmitting said rights expression information (127) to a means (101) for providing said networked service (119), and for receiving said rights expression information (127) from said means (105),

wherein said means (109) interprets said rights expression information (127) transmitted from said means (103) to said means (101) to determine if said means (101) has allowed access to said networked service (119), based on state data (115) associated with said rights expression information (127) and received from a means (111) for state tracking,
said means (105), said means (109), and said means (111) are configured as a middle layer provided between a means (113) for providing trust authority and said service provider (101) and said client (103), and
said means (113) manages trust relationships between said means (105), said means (109), and said means (111).

Claims

1. A computer-implemented method for exercising rights based on determining trust in an issuance of a rights expression, the method comprising:

   issuing rights expressions by a chain of servers, forming a chain of rights expressions issued from server to server and finally from the last server to a client, such that each of the rights expressions except the last includes a specification of rights for the next server to issue the rights in the next rights expression;
   determining whether or not each of the servers has a right to issue the respective rights expression;
   exercising by the client the rights expressed in the last rights expression as being trusted, if it is determined that each of the servers had a right to issue the respective rights expression; and
   not exercising by the client the rights expressed in the last rights expression as not being trusted, if it is determined that at least one of the servers did not have the right to issue the respective rights expression.

2. The method of claim 1, wherein some of the rights expressions include specifications of rights to use content.

3. The method of claim 1, wherein the determination on whether or not each of the servers in the chain has a right to issue the respective rights expression is done through one or more determining servers for at least one of the

servers in the chain.

4. The method of claim 3, wherein some of the determining servers are the servers in the chain.

5. The method of claim 3, wherein some of the determining servers are not the servers in the chain.

6. The method of claim 1, wherein the determination on whether or not each of the servers in the chain has a right to issue the respective rights expression involves verification of signatures up the chain until a signature is recognized.

7. A system for exercising rights based on determining trust in an issuance of a rights expression, the system comprising:

a client;
a chain of servers configured to issue rights expressions, forming a chain of rights expressions issued from server to server and finally from the last server to the client, such that each of the rights expressions except the last includes a specification of rights for the next server to issue the rights in the next rights expression; and
means for determining whether or not each of the servers has a right to issue the respective rights expression,

wherein the client is configured to exercise the rights expressed in the last rights expression as being trusted, if each of the servers had a right to issue the respective rights expression, and not exercise the rights expressed in the last rights expression as not being trusted, if at least one of the servers did not have the right to issue the respective rights expression.

8. The system of claim 7, wherein some of the rights expressions include specifications of rights to use content.

9. The system of claim 7, wherein the determining means includes one or more determining servers for at least one of the servers in the chain.

10. The system of claim 9, wherein some of the determining servers are the servers in the chain.

11. The system of claim 9, wherein some of the determining servers are not the servers in the chain.

12. The system of claim 7, wherein the determining means includes means for verifying signatures up the chain until a signature is recognized.

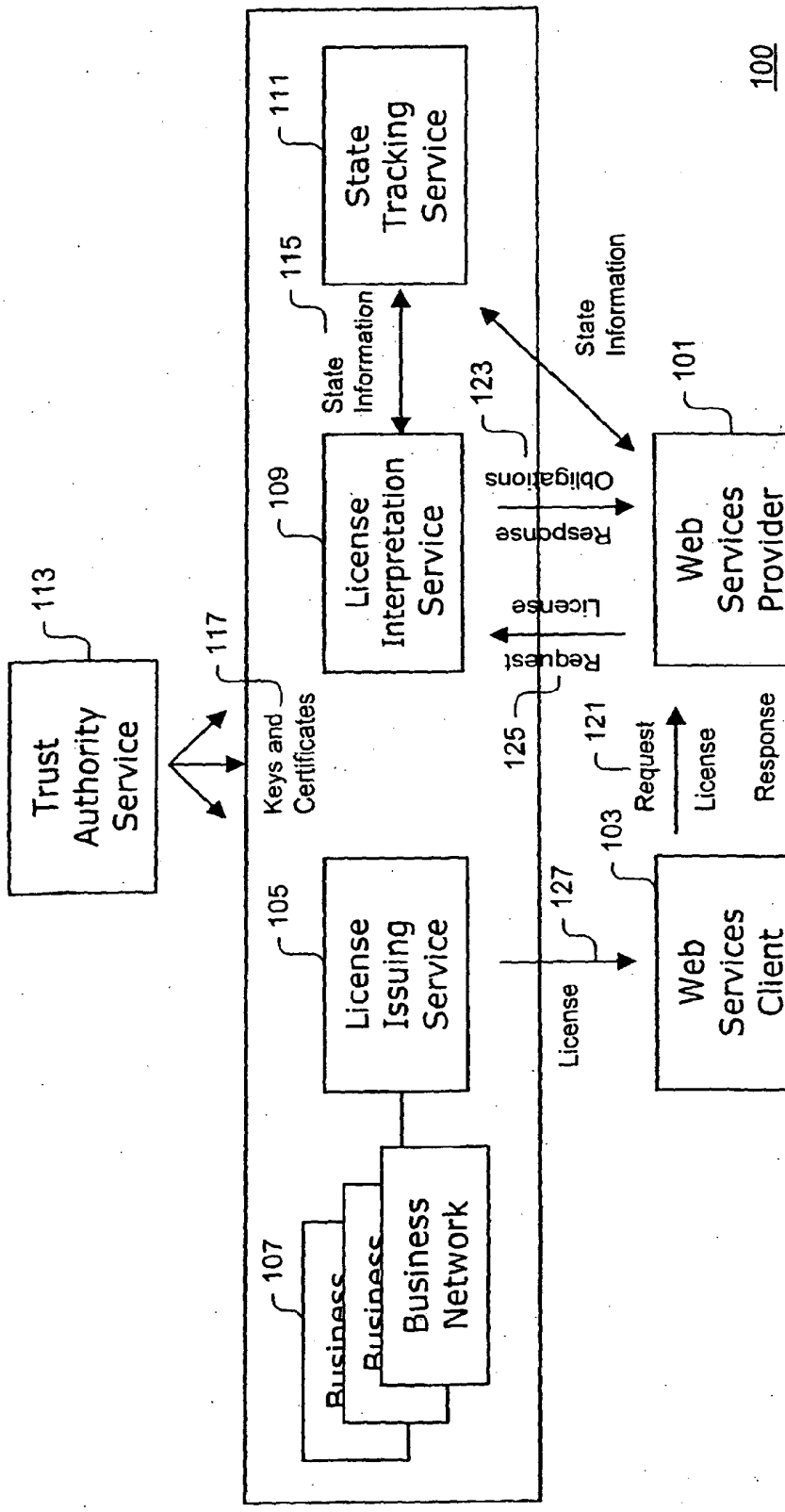

100
Trust Authority Service
113
Keys and Certificates
117
License Interpretation Service
109
State Tracking Service
111
State Information
115
State Information
123
Obligations
Response
License
Request
125
Web Services Provider
101
License Issuing Service
105
Business Network
107
Business
Business
License
127
Request
121
License
Response
Service
119
103
Web Services Client

FIG. 1

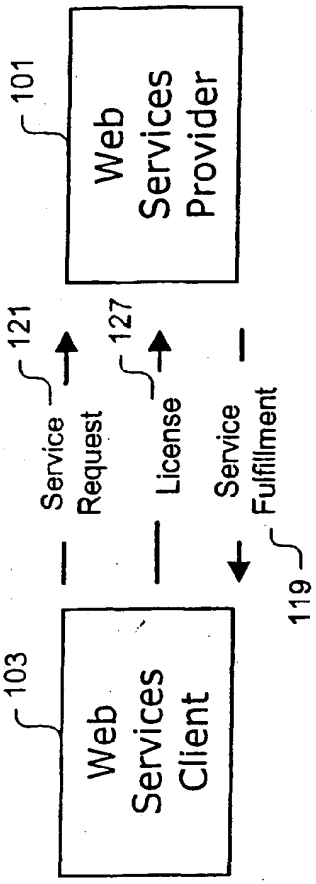

101
Web Services Provider
121
Service Request
127
License
Service Fulfillment
119
103
Web Services Client

FIG. 2

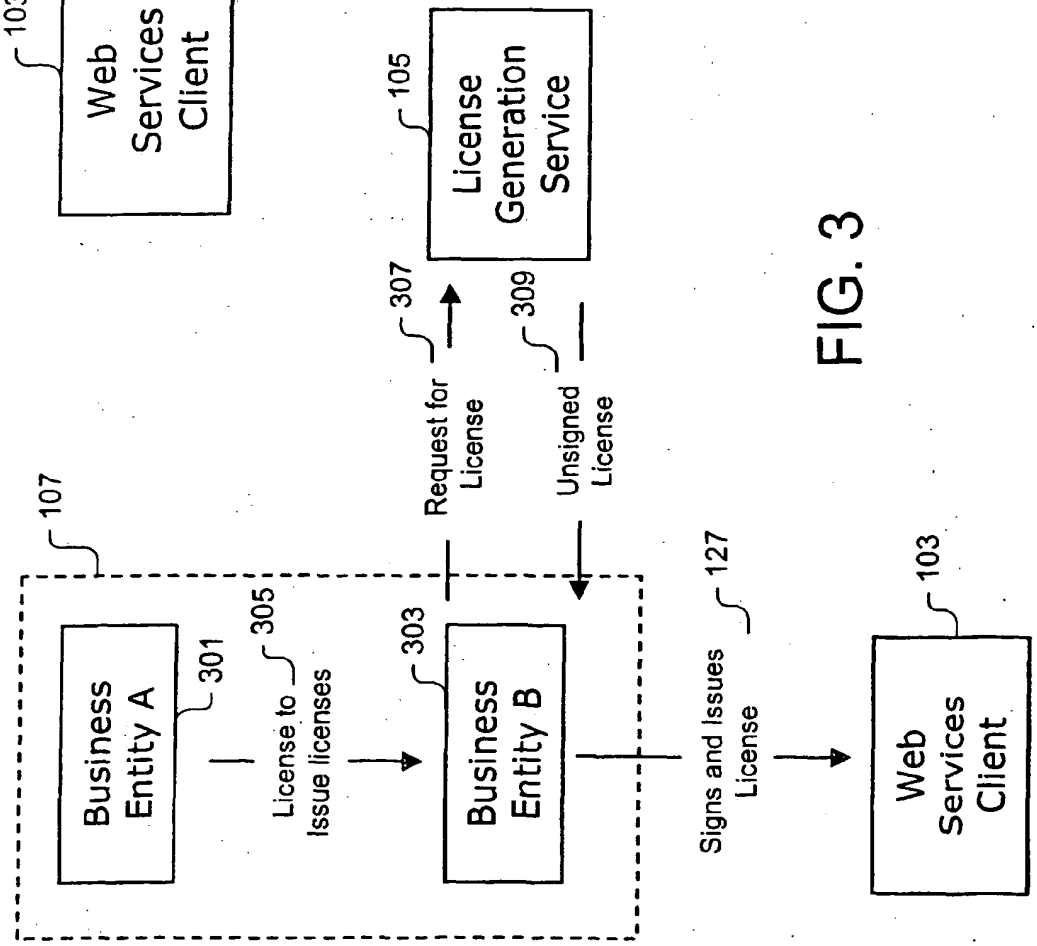

105
License Generation Service
307
Request for License
309
Unsigned License
107
Business Entity A
301
305
License to Issue licenses
303
Business Entity B
127
Signs and Issues License
103
Web Services Client

FIG. 3

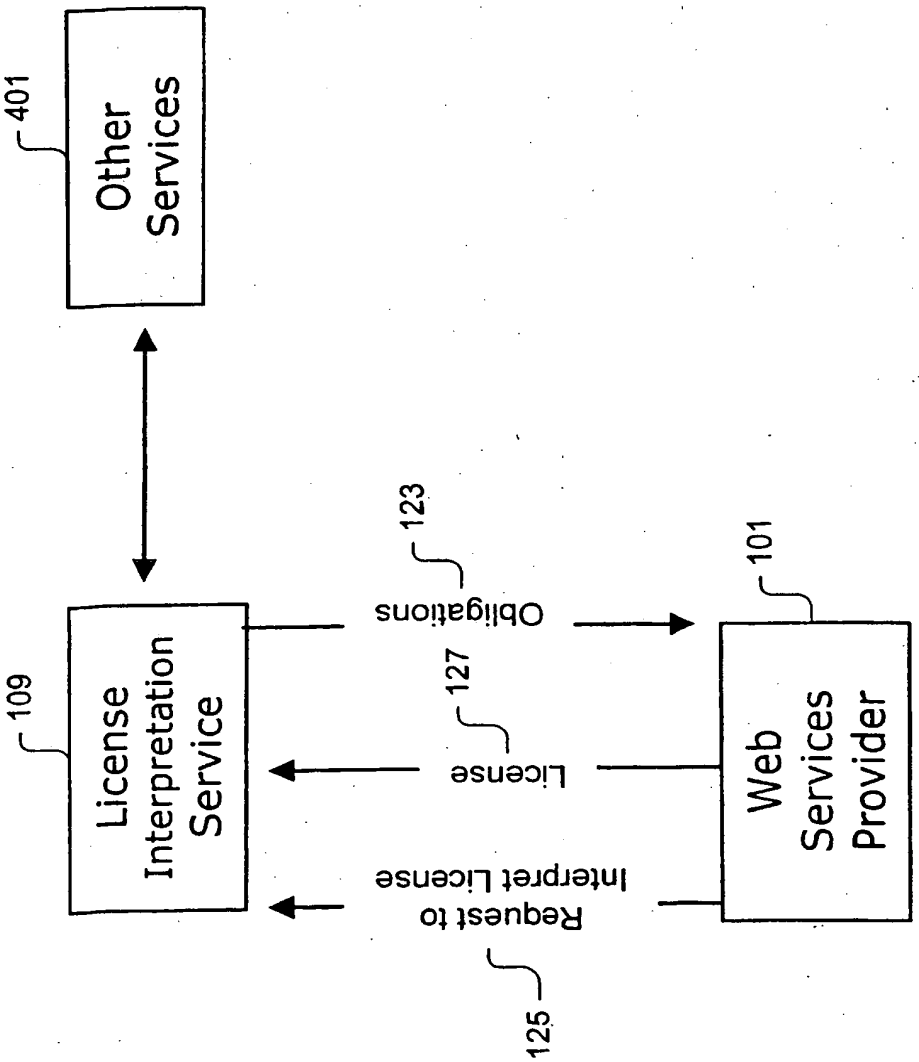

401
Other Services
123
Obligations
101
109
License Interpretation Service
127
License
Web Services Provider
Request to Interpret License
125

FIG. 4

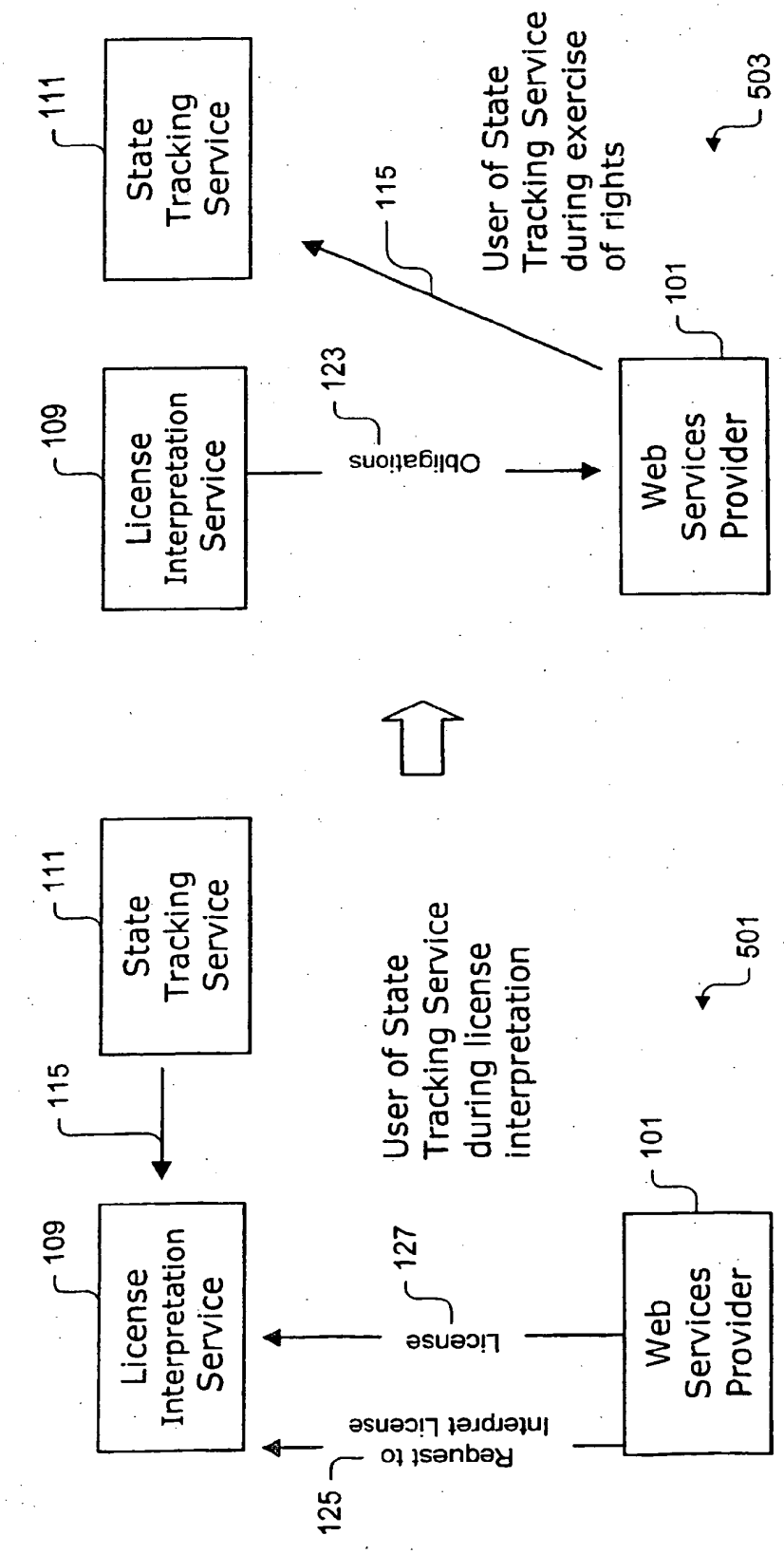

State Tracking Service
111
License Interpretation Service
109
Obligations
123
Web Services Provider
101
115
User of State Tracking Service during exercise of rights
503
State Tracking Service
111
115
User of State Tracking Service during license interpretation
501
License Interpretation Service
109
127
License
Web Services Provider
101
Request to Interpret License
125

FIG. 5

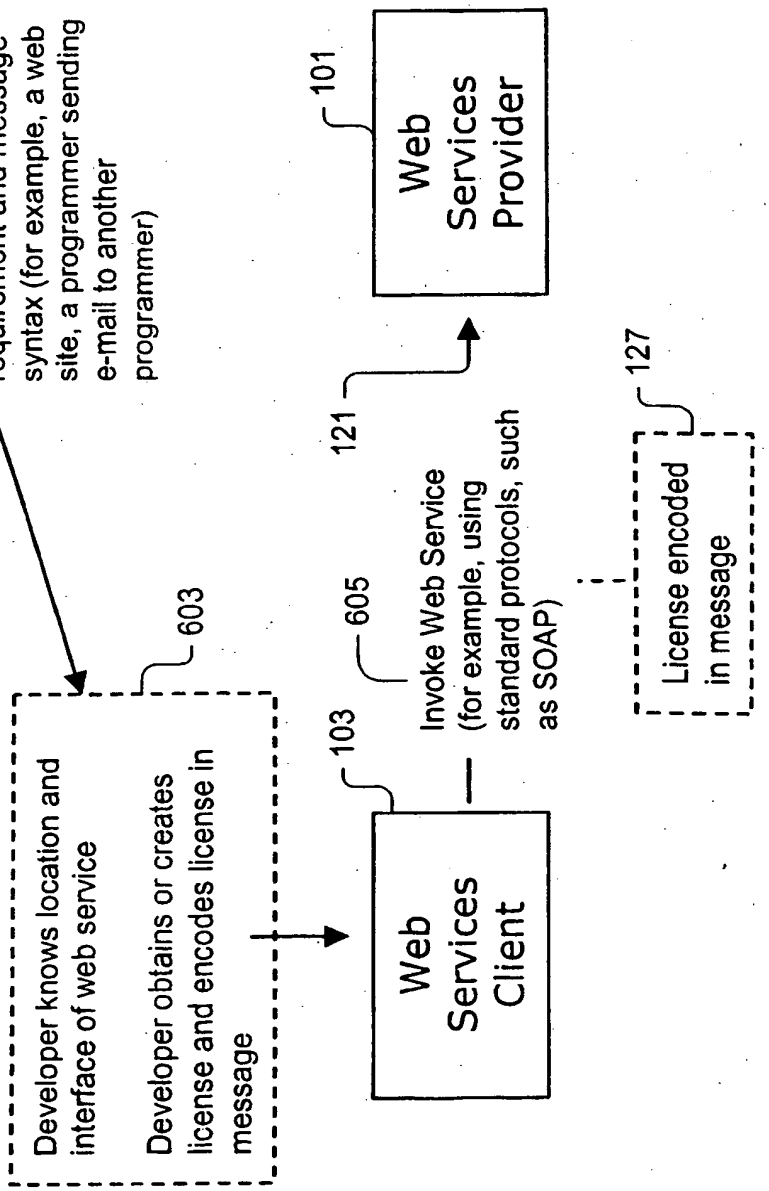

601
Information on license requirement and message syntax (for example, a web site, a programmer sending e-mail to another programmer)
101
Web Services Provider
121
603
Developer knows location and interface of web service
Developer obtains or creates license and encodes license in message
103
Web Services Client
605
Invoke Web Service (for example, using standard protocols, such as SOAP)
127
License encoded in message

FIG. 6

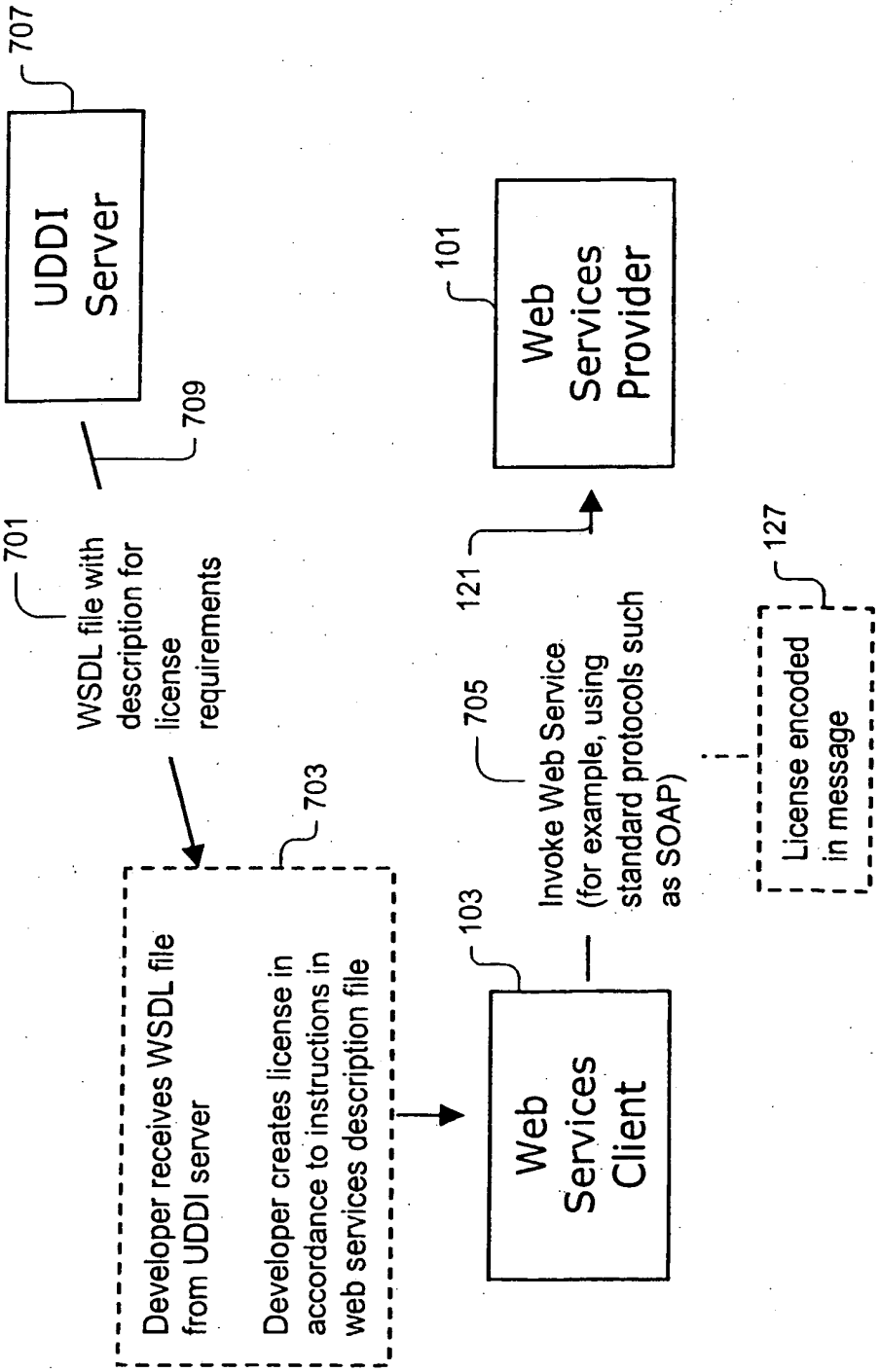

UDDI Server
707
709
WSDL file with description for license requirements
701
Web Services Provider
101
121
Invoke Web Service (for example, using standard protocols such as SOAP)
705
Developer receives WSDL file from UDDI server
Developer creates license in accordance to instructions in web services description file
703
Web Services Client
103
License encoded in message
127

FIG. 7

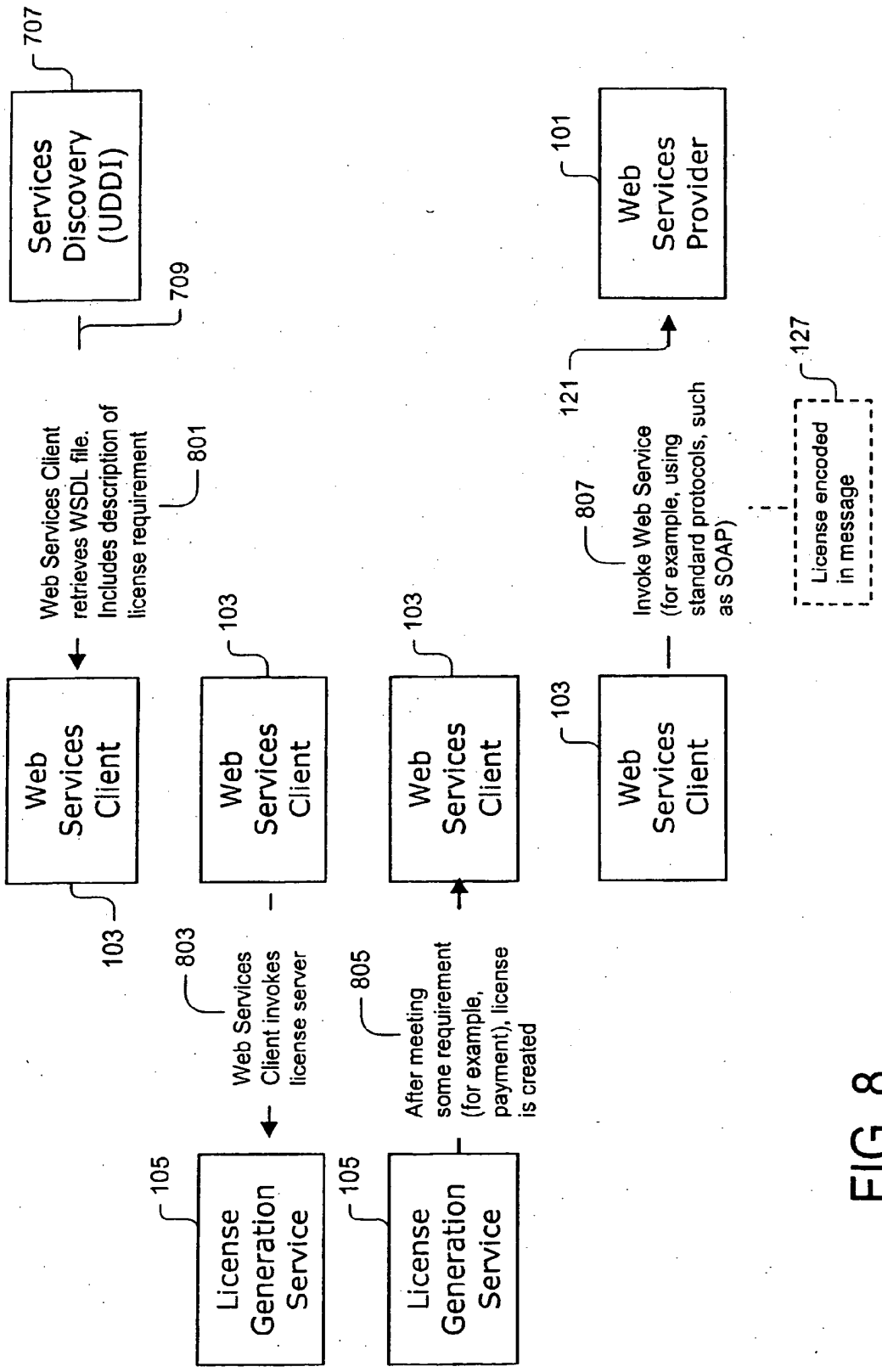

Services Discovery (UDDI)
707
709
Web Services Provider
101
Web Services Client retrieves WSDL file. Includes description of license requirement
801
121
Invoke Web Service (for example, using standard protocols, such as SOAP)
807
127
License encoded in message
Web Services Client
103
Web Services Client
103
Web Services Client
103
Web Services Client
103
Web Services Client invokes license server
803
After meeting some requirement (for example, payment), license is created
805
License Generation Service
105
License Generation Service
105

FIG. 8

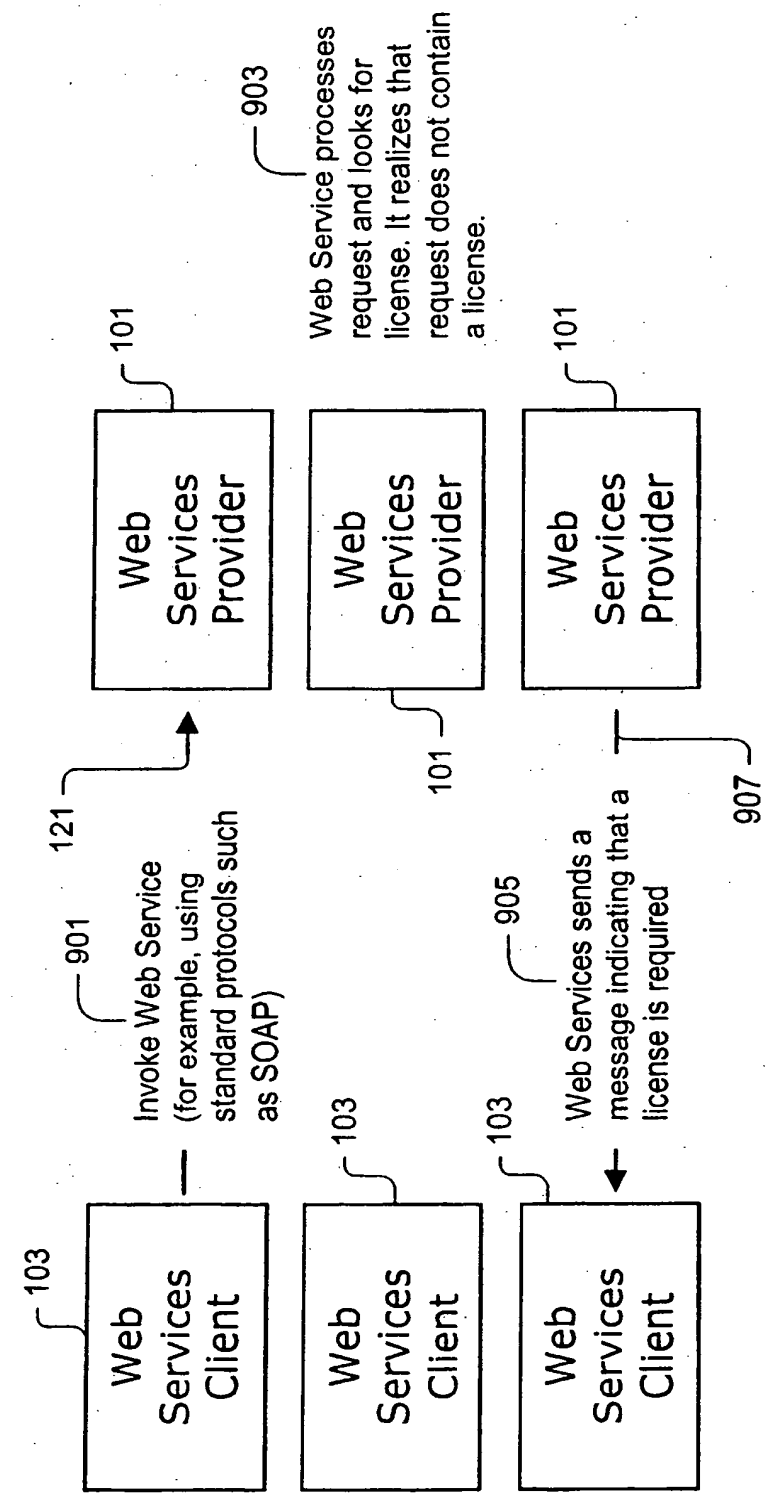

Web Services Client
103
Web Services Client
103
Web Services Client
103
Invoke Web Service (for example, using standard protocols such as SOAP)
901
121
Web Services Provider
101
Web Services Provider
101
Web Services Provider
101
Web Service processes request and looks for license. It realizes that request does not contain a license.
903
Web Services sends a message indicating that a license is required
905
907

FIG. 9

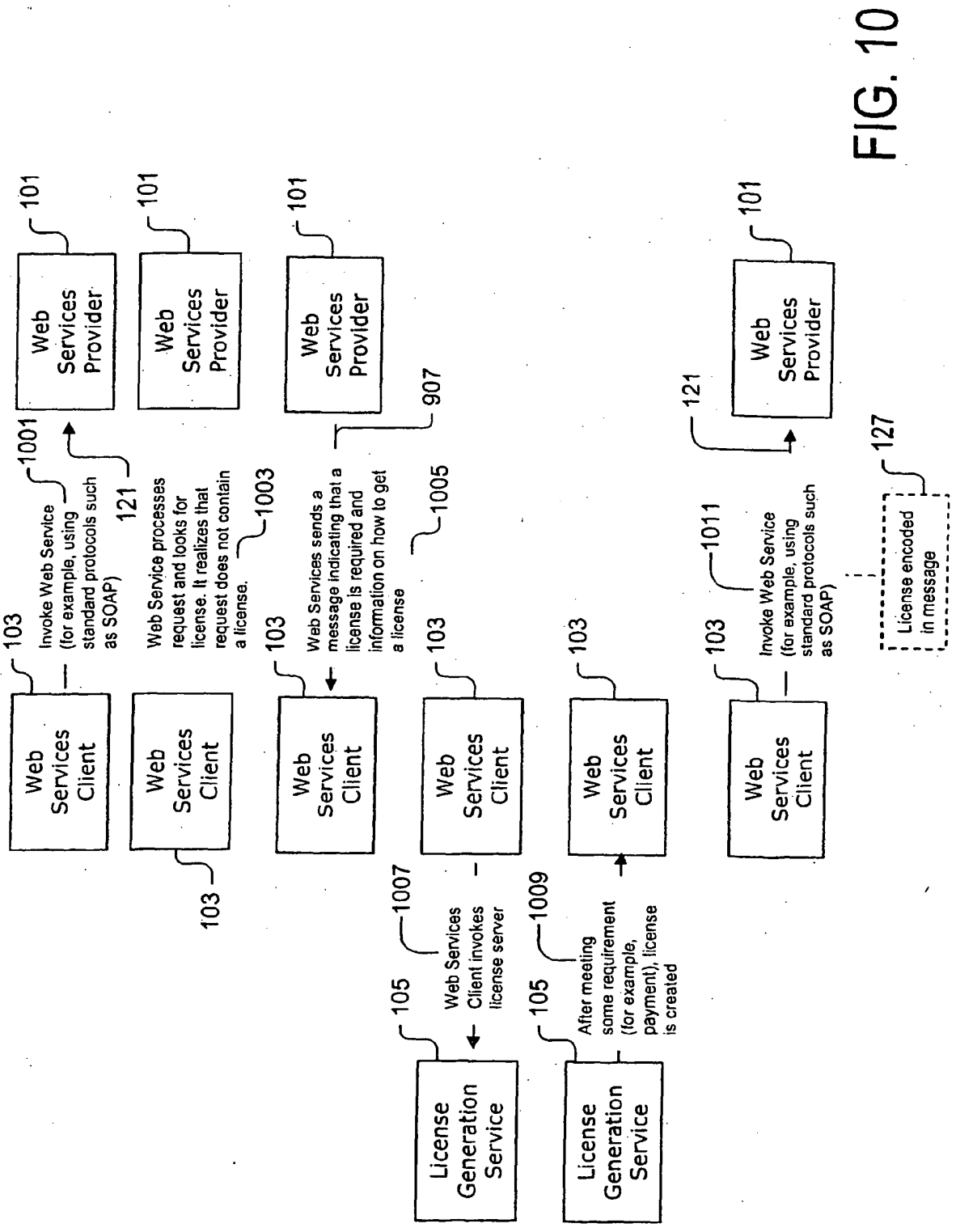

Web Services Client
Web Services Provider
103
101
1001
Invoke Web Service (for example, using standard protocols such as SOAP)
121
1003
Web Service processes request and looks for license. It realizes that request does not contain a license.
1005
Web Services sends a message indicating that a license is required and information on how to get a license
907
1007
Web Services Client invokes license server
1009
After meeting some requirement (for example, payment), license is created
105
License Generation Service
1011
Invoke Web Service (for example, using standard protocols such as SOAP)
127
License encoded in message

FIG. 10

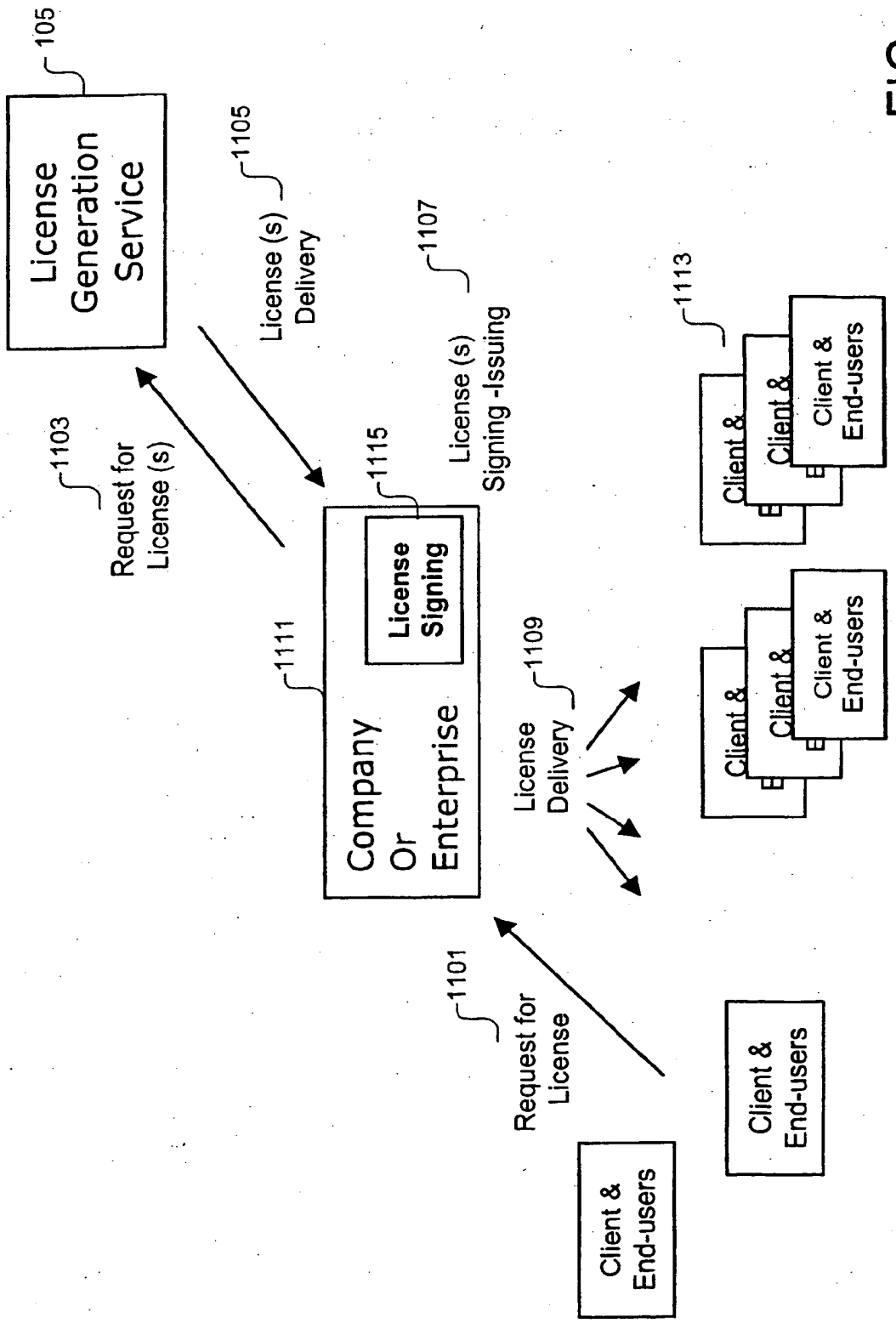

License Generation Service
105
License (s) Delivery
1105
Request for License (s)
1103
License (s) Signing -Issuing
1107
License Signing
1115
Company Or Enterprise
1111
License Delivery
1109
Request for License
1101
Client & End-users
Client & End-users
Client & End-users
Client & End-users
Client & End-users
1113

FIG. 11

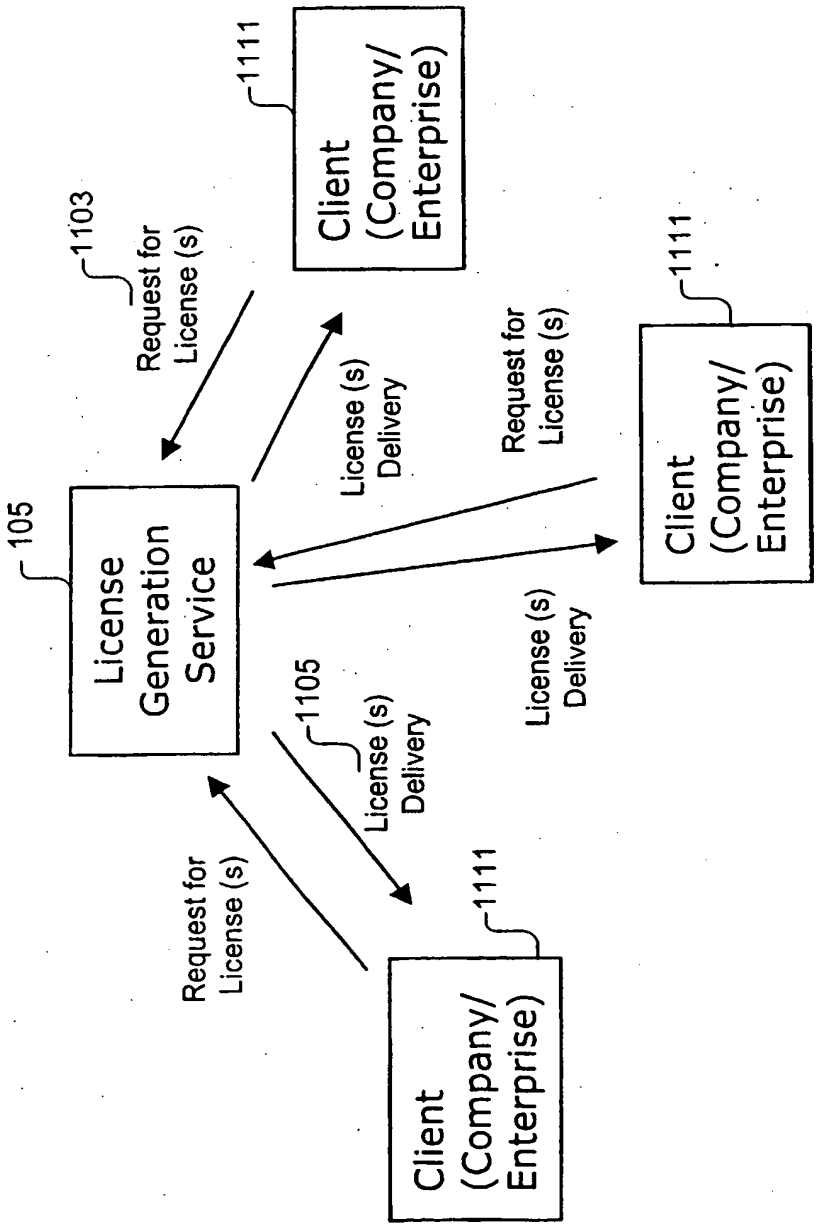

105
License Generation Service
1103
Request for License (s)
1111
Client (Company/ Enterprise)
License (s) Delivery
Request for License (s)
1111
Client (Company/ Enterprise)
License (s) Delivery
1105
License (s) Delivery
Request for License (s)
1111
Client (Company/ Enterprise)

FIG. 12

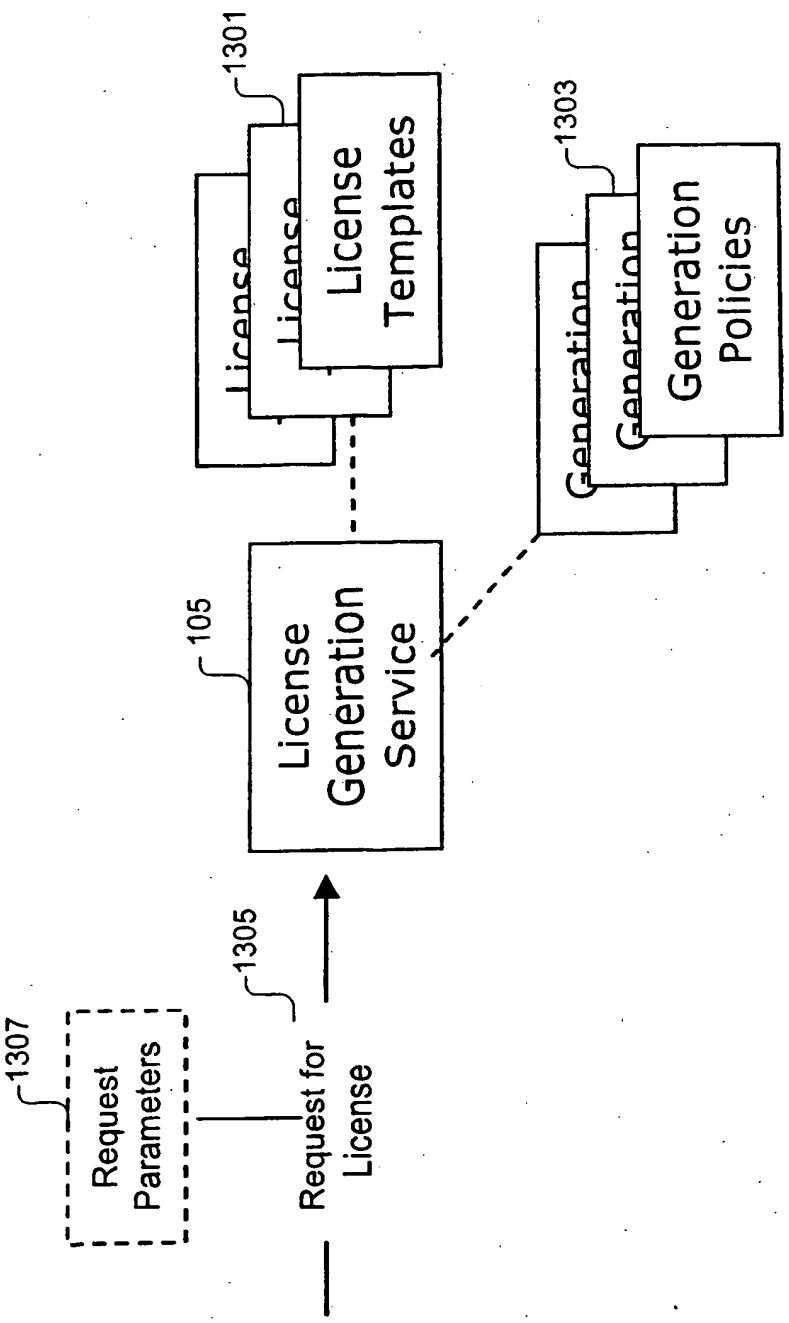

1307
Request Parameters
1305
Request for License
105
License Generation Service
1301
License
License
License Templates
1303
Generation
Generation
Generation Policies

FIG. 13

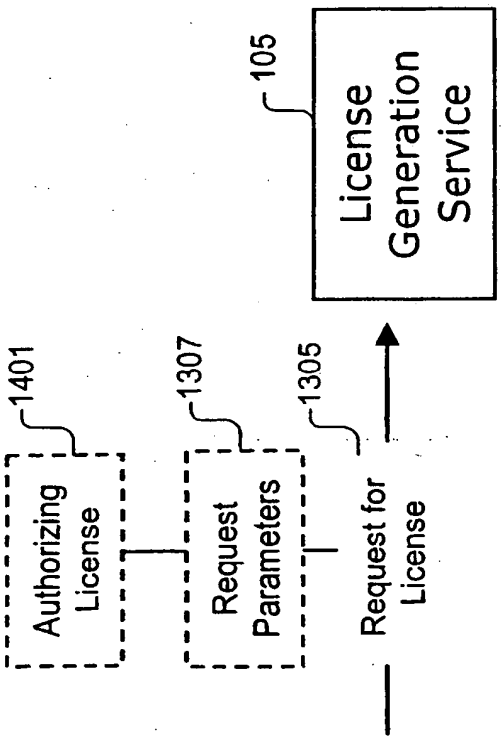

105
License Generation Service
1401
Authorizing License
1307
Request Parameters
1305
Request for License

FIG. 14

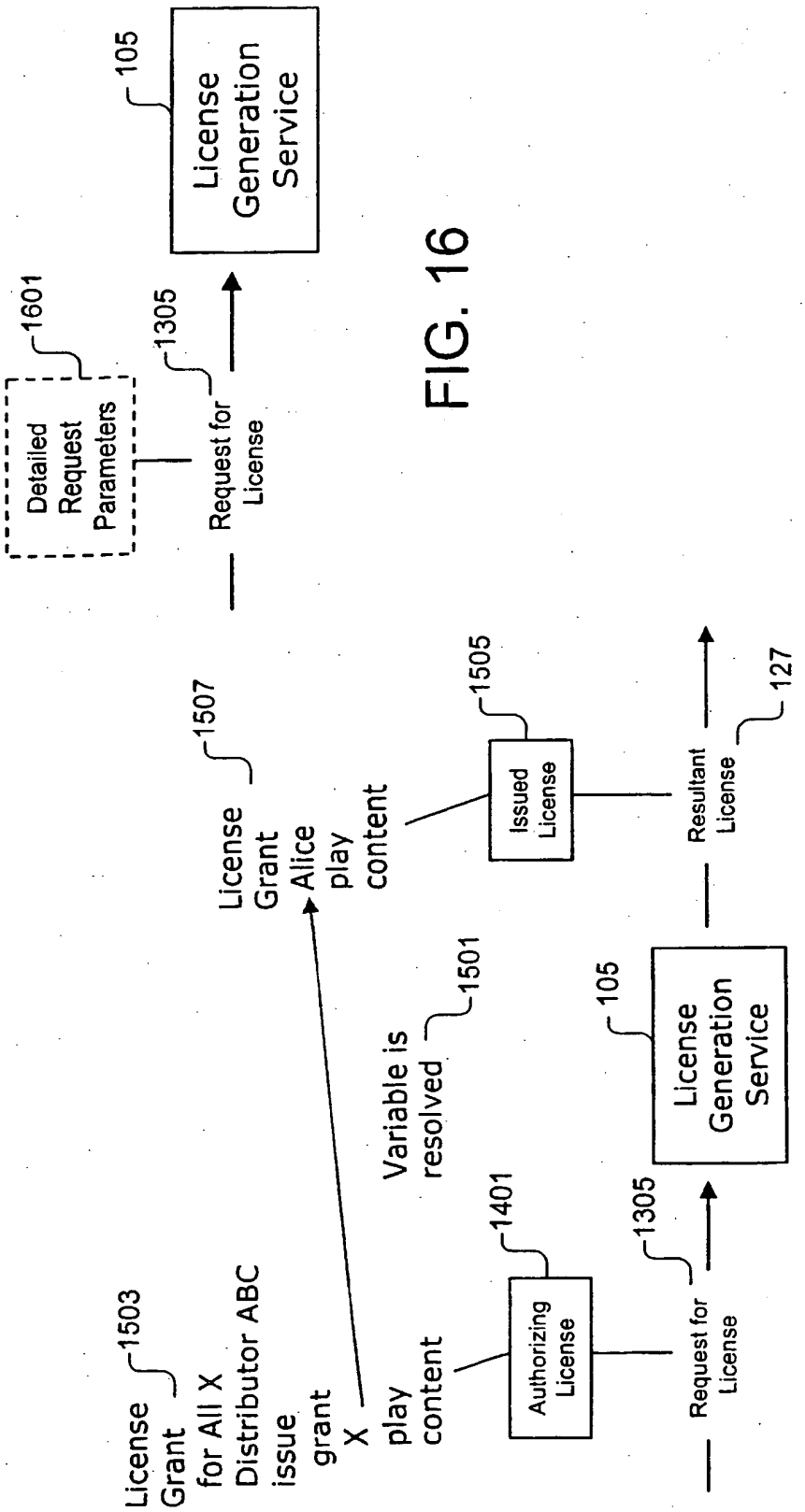

License Generation Service
105
Request for License
1305
Detailed Request Parameters
1601
License Grant Alice play content
1507
Issued License
1505
Resultant License
127
Variable is resolved
1501
License Generation Service
105
Request for License
1305
Authorizing License
1401
License Grant for All X Distributor ABC issue grant X play content
1503

FIG. 16

FIG. 15

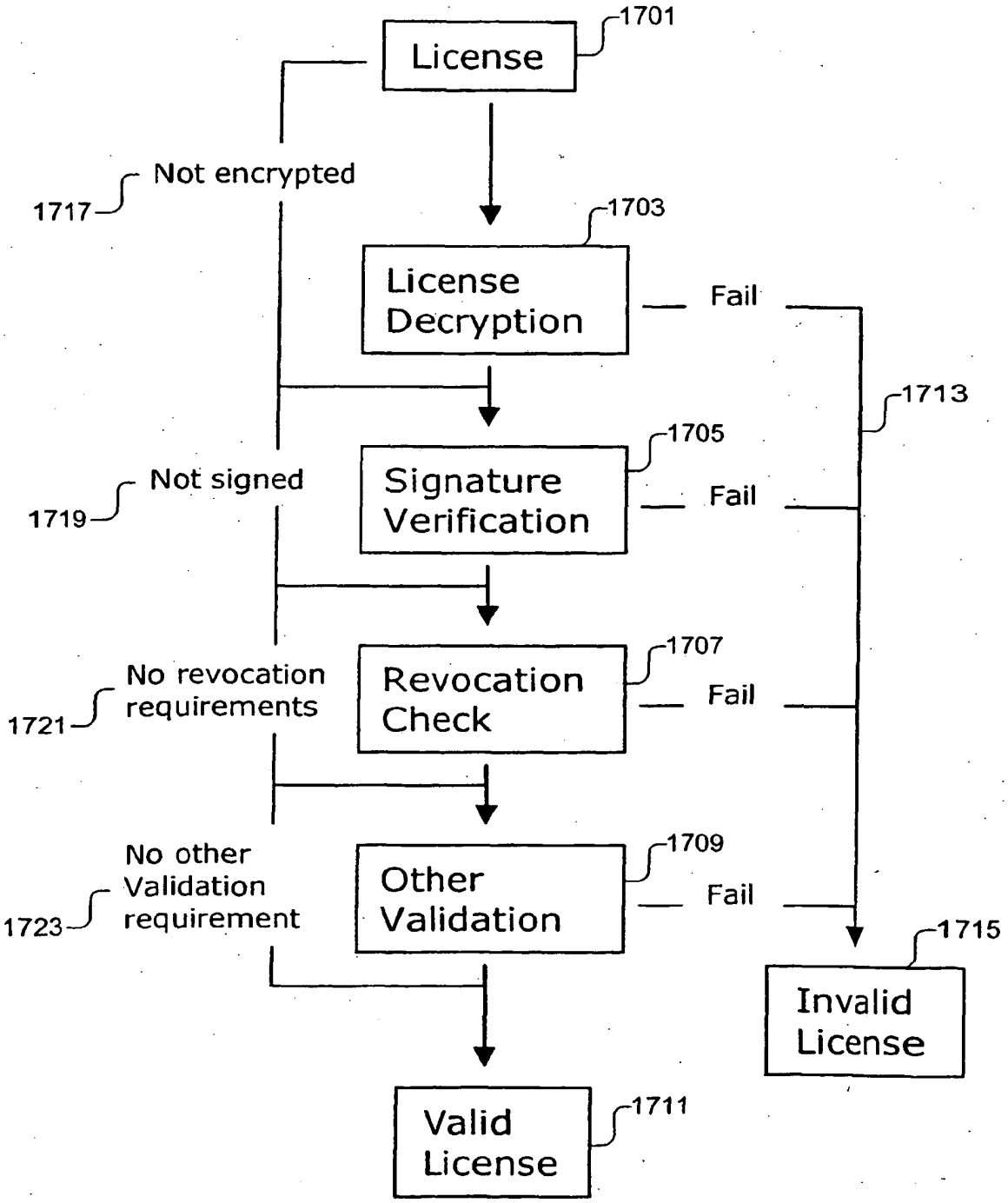

License
1701
Not encrypted
1717
1703
License Decryption
Fail
1713
Not signed
1719
1705
Signature Verification
Fail
No revocation requirements
1721
1707
Revocation Check
Fail
No other Validation requirement
1723
1709
Other Validation
Fail
1715
Invalid License
Valid License
1711

FIG. 17

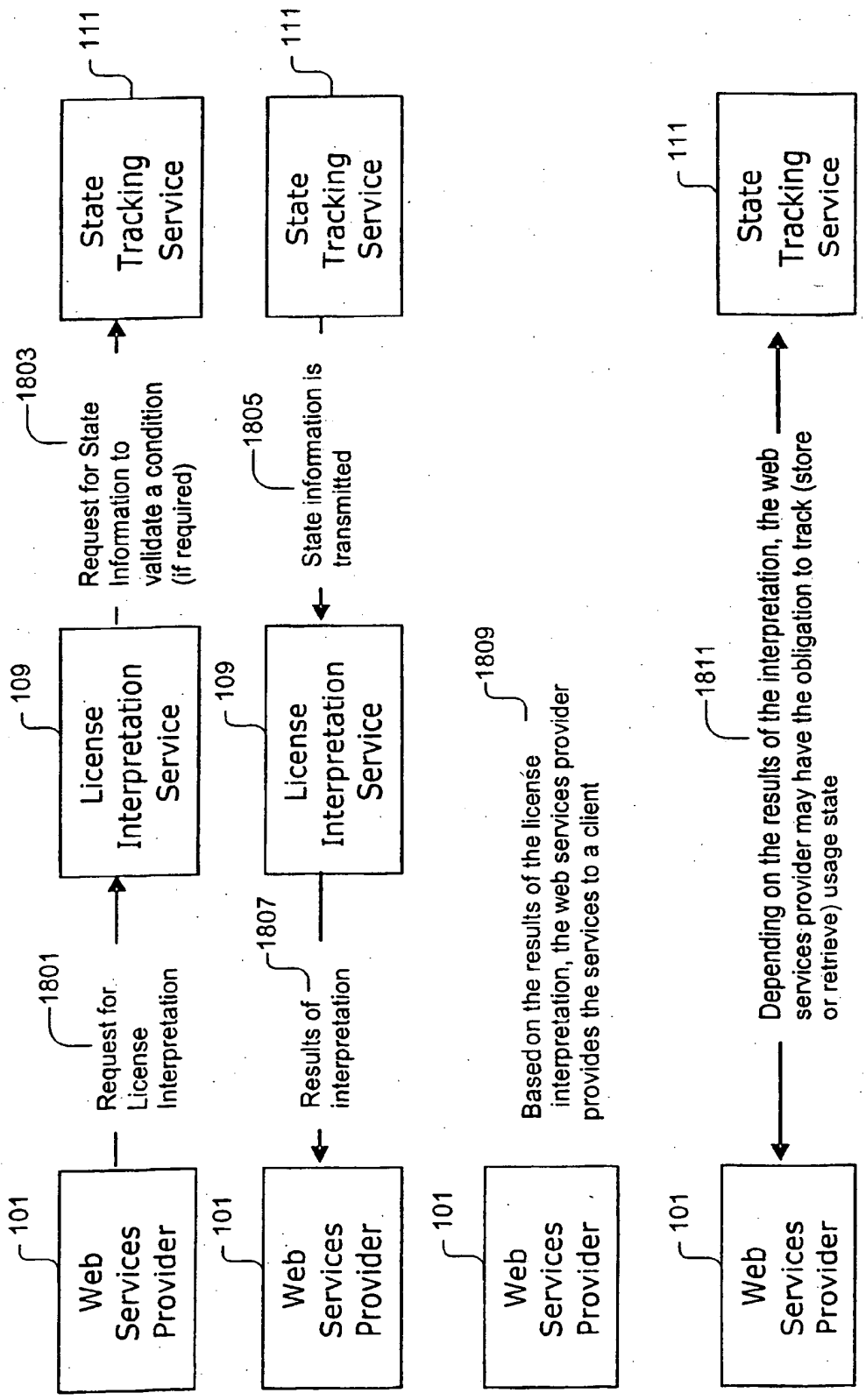

Web Services Provider
101
Request for License Interpretation
1801
License Interpretation Service
109
Request for State Information to validate a condition (if required)
1803
State Tracking Service
111
Results of interpretation
1807
State infomation is transmitted
1805
Based on the results of the license interpretation, the web services provider provides the services to a client
1809
Depending on the results of the interpretation, the web services provider may have the obligation to track (store or retrieve) usage state
1811

FIG. 18

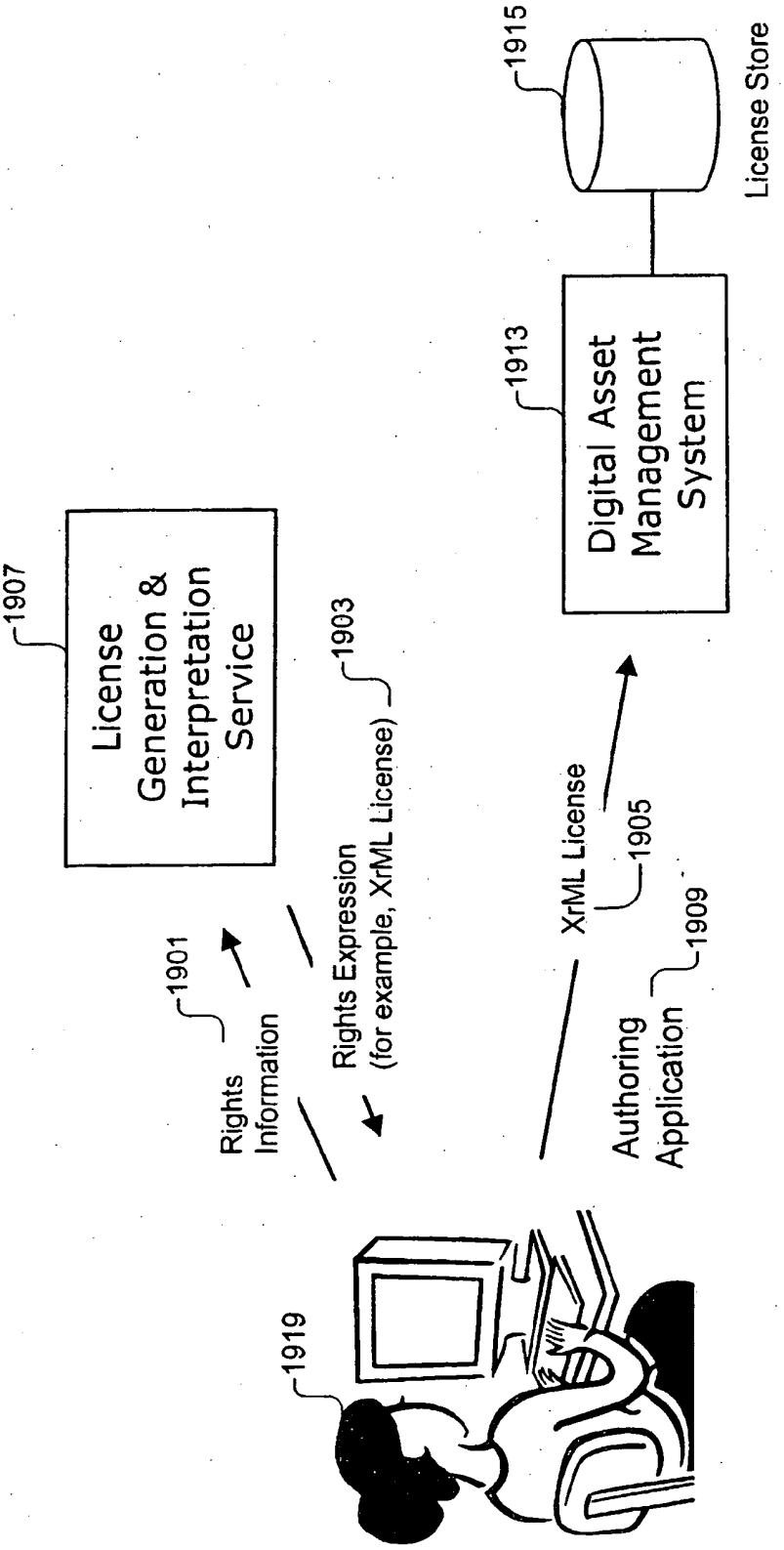

1907
License Generation & Interpretation Service
1903
Rights Expression (for example, XrML License)
1901
Rights Information
1905
XrML License
1909
Authoring Application
1919
1913
Digital Asset Management System
1915
License Store

FIG. 19

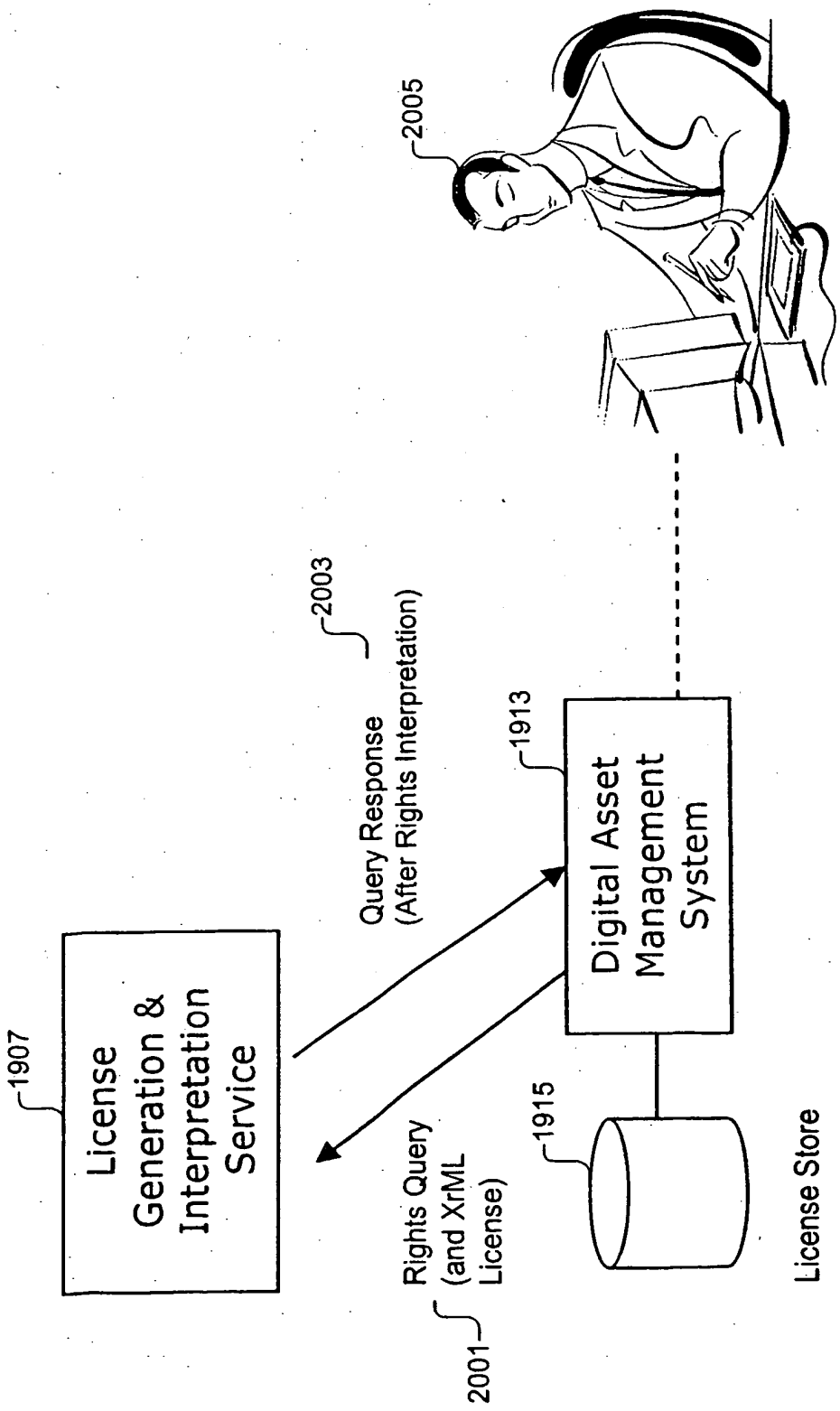

2005
2003
Query Response
(After Rights Interpretation)
1913
Digital Asset
Management
System
1907
License
Generation &
Interpretation
Service
1915
Rights Query
(and XrML
License)
2001
License Store

FIG. 20

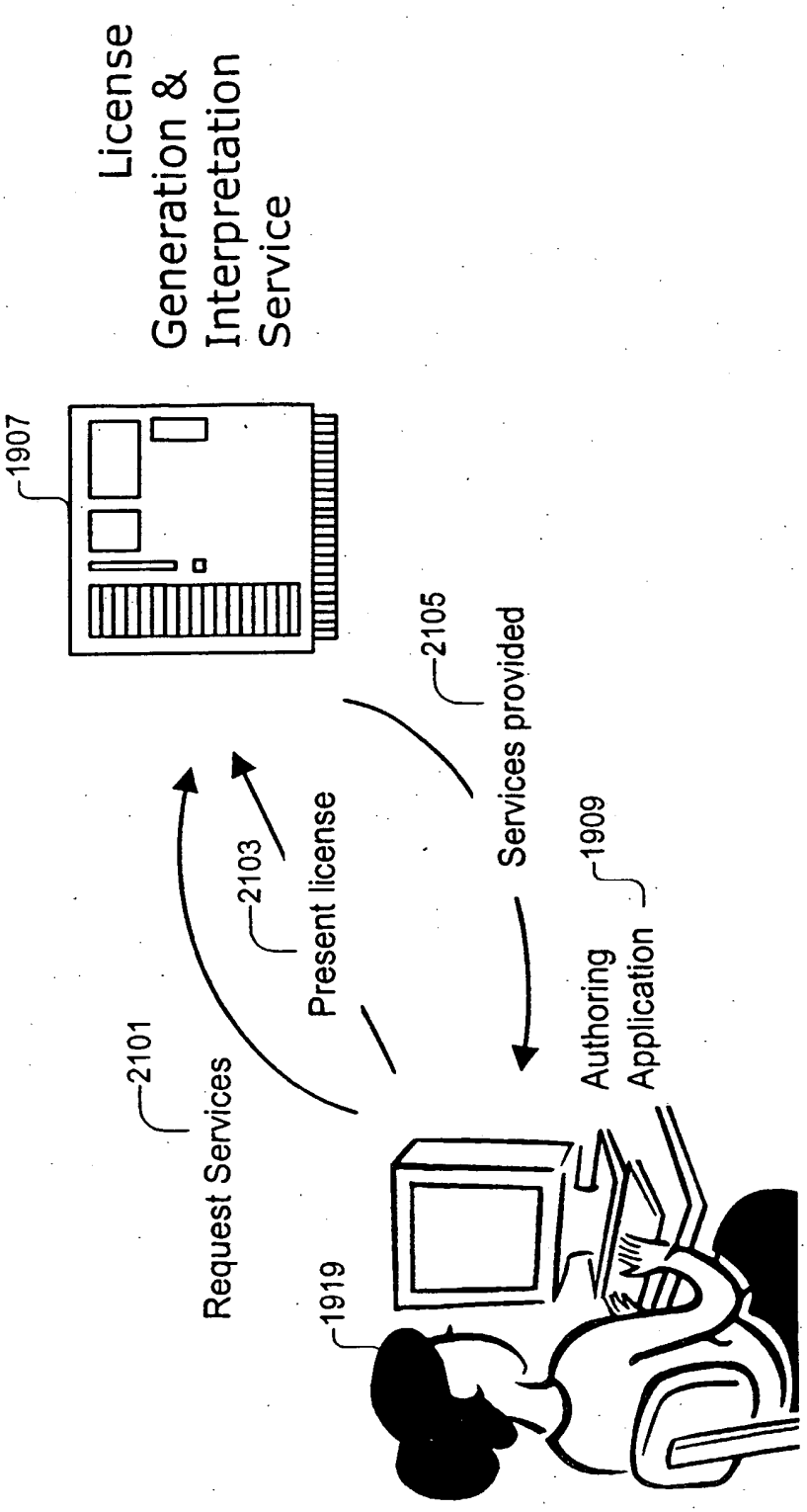

License Generation & Interpretation Service
1907
2105
Services provided
2103
Present license
1909
Authoring Application
2101
Request Services
1919

FIG. 21

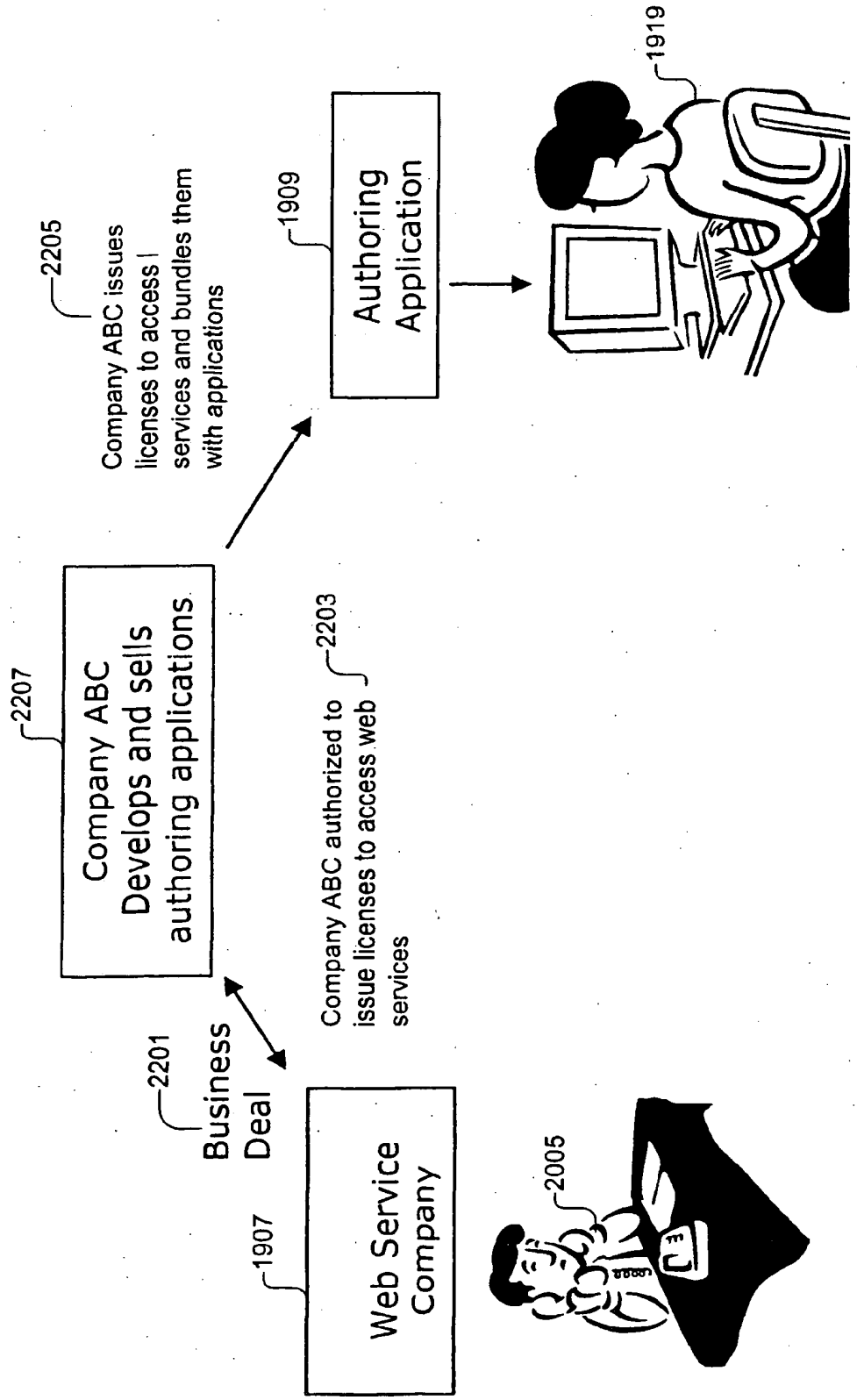

Web Service Company
1907
Business Deal
2201
Company ABC Develops and sells authoring applications
2207
Company ABC authorized to issue licenses to access web services
2203
Company ABC issues licenses to access I services and bundles them with applications
2205
Authoring Application
1909
2005
1919

FIG. 22

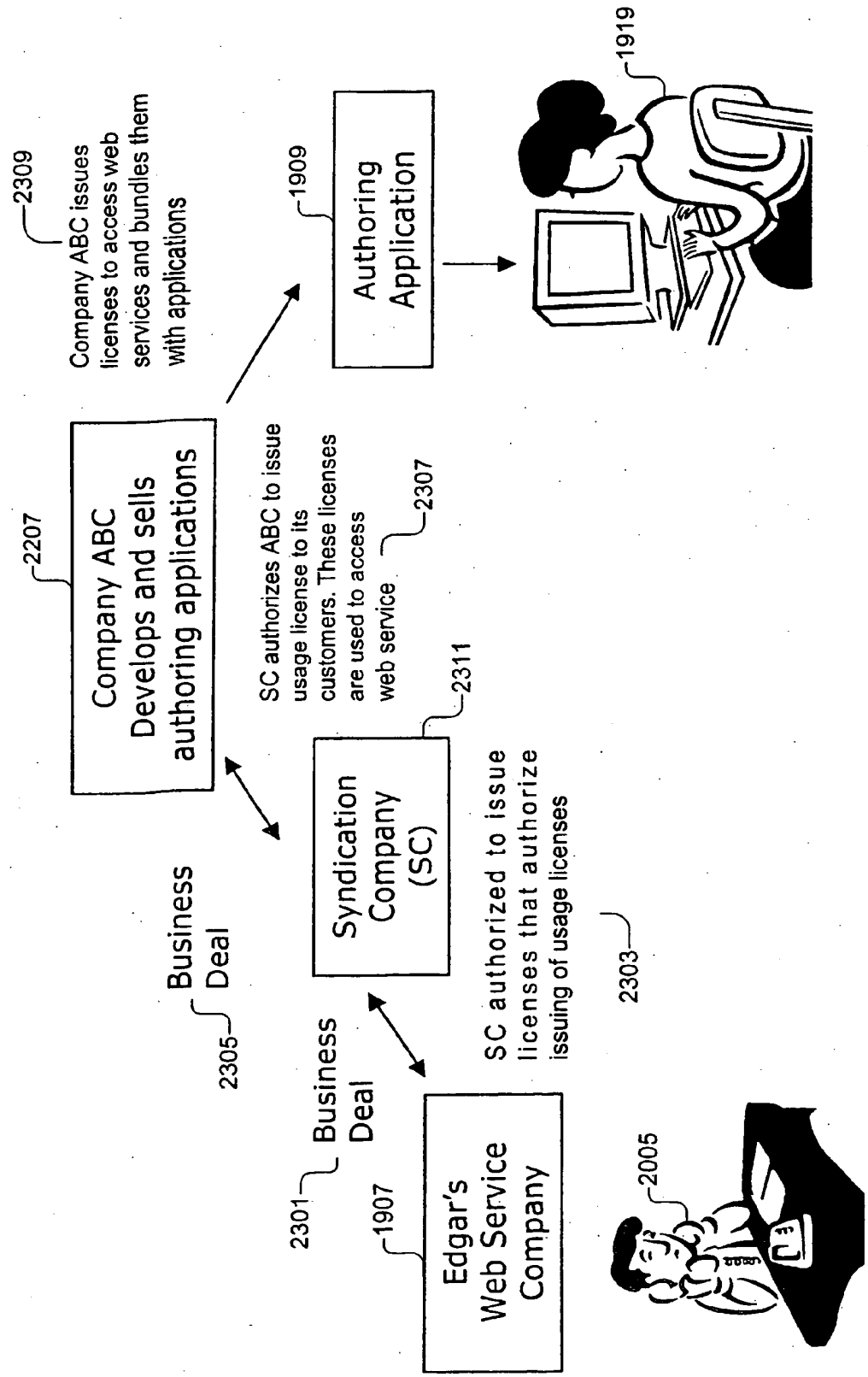

Edgar's Web Service Company
1907
2301
Business Deal
2305
Business Deal
Syndication Company (SC)
2311
SC authorized to issue licenses that authorize issuing of usage licenses
2303
SC authorizes ABC to issue usage license to its customers. These licenses are used to access web service
2307
Company ABC Develops and sells authoring applications
2207
Company ABC issues licenses to access web services and bundles them with applications
2309
Authoring Application
1909
1919
2005

FIG. 23

European Patent Office

DECLARATION

which under Rule 45 of the European Patent Convention shall be considered, for the purposes of subsequent proceedings, as the European search report

Application Number EP 04 02 2578

The Search Division considers that the present application, does not comply with the provisions of the EPC to such an extent that it is not possible to carry out a meaningful search into the state of the art on the basis of all claims

Reason:

The claims of the application are formulated to merely specify commonplace features relating to matter excluded from patentability under Art. 52(2) and (3) EPC and its technological implementation. Due to the attendant lack of resolution of technical definition present, the search division could not establish a technical problem addressed in order to be able to carry out a meaningful search into the state of the art (Rule 45 EPC). See also Guidelines Part B Chapter VIII. Accordingly no search has been carried out.

The applicant's attention is drawn to the fact that a search may be carried out during examination following a declaration of no search under Rule 45 EPC, should the problems which led to the declaration being issued be overcome (see EPC Guideline C-VI, 8.5).

CLASSIFICATION OF THE APPLICATION (Int.Cl.7)

G06F17/60
G06F21/00

Place of search	Date	Examiner
The Hague	4 November 2004	Rossier, T

EPO FORM 1504 (P04C37)

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Filer:	William Grecia
Attorney Docket Number:	

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	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Claims:				
Multiple dependent claims	2203	1	195	195
Miscellaneous-Filing:				
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**957**

Electronic Acknowledgement Receipt

EFS ID:	9174255
Application Number:	12985351
International Application Number:	
Confirmation Number:	4165
Title of Invention:	PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-JAN-2011
Filing Date:	
Time Stamp:	02:22:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$957
RAM confirmation Number	9419
Deposit Account	
Authorized User	

File Listing:

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

1		PDMAS.pdf	163504 6a60a90367c54a877408433ac9110eb6273 2623f	yes	32

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	26
	Claims	27	31
	Abstract	32	32

Warnings:

Information:

2	Request for Early Publication	earlypubreq.pdf	103150 1d754c8d02053ae784e667fead38e0d4419 690d9	no	1

Warnings:

Information:

3	Transmittal of New Application	sb0005_fill.pdf	1078293 274707bae70fd746ff203e50fbd6688d8d42 9e29	no	2

Warnings:

Information:

4	Oath or Declaration filed	sb0001.pdf	805666 1c996a403ff6a987997c7e54aba04de58633 fccb	no	4

Warnings:

Information:

5		IDS.pdf	526386 8639c6a41cb5b6701974856713e23277511 56f13	yes	15

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Information Disclosure Statement (IDS) Filed (SB/08)	1	3
	Information Disclosure Statement (IDS) Filed (SB/08)	4	9
	Information Disclosure Statement (IDS) Filed (SB/08)	10	11
	Information Disclosure Statement (IDS) Filed (SB/08)	12	13
	Information Disclosure Statement (IDS) Filed (SB/08)	14	15

Warnings:					
Information:					
6	Drawings-only black and white line drawings	Figures.pdf	151502 ddf112e81fb37bee3ead3d602c484d3b8081fda1	no	7
Warnings:					
Information:					
7	Foreign Reference	ep156462.pdf	310001 fb0e871c80a74beced20616a7b2541706aae3df6	no	23
Warnings:					
Information:					
8	Foreign Reference	ep1505530.pdf	733006 7291939c05c034eed6cc3097afdd2ea2d7b4ee1a	no	53
Warnings:					
Information:					
9	NPL Documents	VUDU.pdf	410172 c2392b6f8712b5c48192192e135cf6770a680d62	no	2
Warnings:					
Information:					
10	NPL Documents	YouTube.pdf	670025 26f8688d5c6d69698c0196579f3dfdd59c7d933d	no	6
Warnings:					
Information:					
11	NPL Documents	Napster.pdf	42769 943c1e679f1fe1f6c1e047fc1d9e1c5f7a91f66f	no	1
Warnings:					
Information:					
12	NPL Documents	CinemaNow.pdf	607409 c518e653f48e5e7ab0f9f78b56cf5cea7d0c9f13	no	2
Warnings:					
Information:					
13	NPL Documents	Netflix.pdf	161991 e366de68e1de58d02e931ec69f59c4d666554c41	no	1
Warnings:					
Information:					
14	NPL Documents	Zune.pdf	124222 ce5f1fb692c973d1bd0a9116a2ef87174ff64ffb	no	2

Warnings:					
Information:					
15	NPL Documents	iTunes.pdf	940016 ae7bfae0400b23bfd5f31df5f3978ccb7d1cc c33	no	4
Warnings:					
Information:					
16	NPL Documents	Mi2N2.pdf	890369 4f48fa1dc1362532b3a91dcec6e90e677803 8c48	no	2
Warnings:					
Information:					
17	NPL Documents	UltraViolet.pdf	93552 ab341a990fedaf5a5cd2df39781a3b74db4f 83e7	no	2
Warnings:					
Information:					
18	NPL Documents	Ditch.pdf	429900 5cb6df5ec2090477d7e780067897a6110a2 8617a	no	2
Warnings:					
Information:					
19	NPL Documents	Hollywood.pdf	139407 d223bf7b6257763b8f8186133df90e3d990 6fb9f	no	3
Warnings:					
Information:					
20	NPL Documents	AWS.pdf	110955 8b7bca9d5323d3632b3492eb5eddda4cb1 c4d6b8	no	1
Warnings:					
Information:					
21	NPL Documents	Graph.pdf	283380 e13ac3c6a1eabba94549afe91571e1e3b84 23991	no	5
Warnings:					
Information:					
22	NPL Documents	Mi2N.pdf	871393 06d137dc19107e564641d2a6b41be3155a 77c2c0	no	2
Warnings:					
Information:					
23	NPL Documents	STR3EM.pdf	287111 5febe4487a0444cad1b10cb7cf6fa6078b2f d3e7	no	1

Warnings:					
Information:					
24	NPL Documents	DECE1.pdf	610352 0d40a7e857bbd06679789789d70bfc94a55c487f	no	5
Warnings:					
Information:					
25	NPL Documents	KeyChest.pdf	1060620 4f5dbb37d175d7307c022f73eb6f048fd5d1b47e	no	10
Warnings:					
Information:					
26	NPL Documents	wikidrm.pdf	1018197 c3c5571d9dfc8d35fa63ef8ce0984f8565089cac	no	21
Warnings:					
Information:					
27	NPL Documents	DVD.pdf	1793468 7582d1e9c7d0e09b7b0187cb1b6240e334aad5dd	no	9
Warnings:					
Information:					
28	NPL Documents	First_Look.pdf	581406 cd2f270b7291dd21c6253cbe0f2a9015b48de2af	no	7
Warnings:					
Information:					
29	NPL Documents	Xbox.pdf	1210101 54cb919d7c088c73d6cd659c22f3d2c026151f75	no	31
Warnings:					
Information:					
30	NPL Documents	SMPTE.pdf	166362 4b0292a2cb4b54df8268aec930b44cbd68fb538a	no	2
Warnings:					
Information:					
31	NPL Documents	CMX.pdf	173214 fe36aea803b455790d5b64b41854f3a339046a61	no	4
Warnings:					
Information:					
32	Fee Worksheet (PTO-875)	fee-info.pdf	38105 936957cca3c2ac9186c40633a3536297ff6867b33	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	16586004

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.

TITLE

PERSONALIZED DIGITAL MEDIA ACCESS SYSTEM (PDMAS)

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of, and claims the priority benefit of, US patent application Serial Number 12/728,218 filed March 21, 2010.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to the field of digital rights management schemes used by creators of electronic products to protect commercial intellectual property copyrights privy to illegal copying using computerized devices. More specifically, the present invention teaches a more personal system of digital rights management which employs electronic ID, as part of a web service membership, to manage access rights across a plurality of devices.

[0004] 2. Description of the Prior Art

[0005] Digital rights management (DRM) is a generic term for access control technologies used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content across devices. DRM refers to any technology that inhibits undesirable or illegal uses of the digital content. The term generally doesn't refer to forms of copy protection that can be circumvented without modifying the file or device, such as serial numbers or key files. It can also refer to restrictions associated with specific instances of digital works or devices.

[0006] Traditional DRM schemes are defined as authentication components added to digital files that have been encrypted from public access. Encryption schemes are not DRM methods but DRM systems are implemented to use an additional layer of authentication in which

permission is granted for access to the cipher key required to decrypt files for access. A computer server is established to host decryption keys and to accept authentication keys from Internet connected client computers running client software in which handles the encrypted files. The server can administer different authorization keys back to the client computer that can grant different sets of rules and a time frame granted before the client is required to connect with the server to reauthorize access permissions. In some cases content can terminate access after a set amount of time, or the process can break if the provider of the DRM server ever ceases to offer services.

[0007] In the present scenario, consumer entertainment industries are in the transition of delivering products on physical media such as CD and DVD to Internet delivered systems. The Compact Disc, introduced to the public in 1982, was initially designed as a proprietary system offering strict media to player compatibility. As the popularity of home computers and CD-ROM drives rose, so did the availability of CD ripping applications to make local copies of music to be enjoyed without the use of the disc. After a while, users found ways to share digital versions of music in the form of MP3 files that could be easily shared with family and friends over the Internet. The DVD format introduced in 1997 included a new apparatus for optical discs technology with embedded copy protection schemes also recognized as an early form of DRM. With internet delivered music and video files, DRM schemes has been developed to lock acquired media to specific machines and most times limiting playback rights to a single machine or among a limited number of multiple machines regardless of the model number. This was achieved by writing the machine device ID to the metadata of the media file, then cross referencing with a trusted clearinghouse according to pre-set rules. DRM systems employed by DVD and CD technologies consisted of scrambling (also known as encryption) disc sectors in a pattern to which hardware developed to unscramble (also known as decryption) the disc sectors are required for playback. DRM

systems built into operating systems such as Microsoft Windows Vista block viewing of media when an unsigned software application is running to prevent unauthorized copying of a media asset during playback. DRM used in computer games such as SecuROM and Steam are used to limit the amount of times a user can install a game on a machine. DRM schemes for e-books include embedding credit card information and other personal information inside the metadata area of a delivered file format and restricting the compatibility of the file with a limited number of reader devices and computer applications.

[0008] In a typical DRM system, a product is encrypted using Symmetric block ciphers such as DES and AES to provide high levels of security. Ciphers known as asymmetric or public key/private key systems are used to manage access to encrypted products. In asymmetric systems the key used to encrypt a product is not the same as that used to decrypt it. If a product has been encrypted using one key of a pair it cannot be decrypted even by someone else who has that key. Only the matching key of the pair can be used for decryption. After receiving an authorization token from a first-use action are usually triggers to decrypt block ciphers in most DRM systems. User rights and restrictions are established during this first-use action with the corresponding hosting device of a DRM protected product.

[0009] Examples of such prior DRM art include Hurtado (U.S. Pat. No. 6,611,812) who described a digital rights management system, where upon request to access digital content, encryption and decryption keys are exchanged and managed via an authenticity clearing house. Other examples include Alve (U.S. Pat. No. 7,568,111) who teaches a DRM and Tuoriniemi (U.S. Pat. No. 20090164776) who described a management scheme to control access to electronic content by recording use across a plurality of trustworthy devices that has been granted permission to work within the scheme.

[00010] Recently, DRM schemes have proven unpopular with consumers and rights organizations that oppose the complications with compatibility across machines manufactured by different companies. Reasons given to DRM opposition range from limited device playback restrictions to the loss of fair-use which defines the freedom to share media products will family members.

[00011] Prior art DRM methods rely on content providers to maintain computer servers to receive and send session authorization keys to client computers with an Internet connection. Usually rights are given from the server for an amount of time or amount of access actions before a requirement to reconnect with the server is required for reauthorization. At times, content providers will discontinue servers or even go out of business some years after DRM encrypted content was sold to consumers causing the ability to access files to terminate.

[00012] In the light of the foregoing discussion, the current states of DRM measures are not satisfactory because unavoidable issues can arise such as hardware failure or property theft that could lead to a paying customer loosing the right to recover purchased products. The current metadata writable DRM measures do not offer a way to provide unlimited interoperability between different machines. Therefore, a solution is needed to give consumers the unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments.

SUMMARY OF THE INVENTION

[00013] An object of the present invention is to provide unlimited interoperability of digital media between unlimited machines with management of end-user access to the digital media.

[00014] In accordance with an embodiment of the present invention, the invention is a process of an apparatus which in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods (herein referred to as The App) is used to: handle at least one branding action which could include post read and write requests of at least one writable metadata as part of at least one digital media asset to identify and manage requests from at least one excelsior enabler, and can further identify and manage requests from a plurality of connected second enablers; with at least one token and at least one electronic identification reference received from the at least one excelsior enabler utilizing at least one membership. Here, controlled by the at least one excelsior enabler, The App will proceed to receive the at least one token to verify the authenticity of the branding action and further requests; then establish at least one connection with at least one programmable communications console of the at least one membership to request and receive the at least one electronic identification reference; and could request and receive other data information from the at least one membership. The method then involves sending and receiving variable data information from The App to the at least one membership to verify a preexisting the at least one branding action of the at least one writable metadata as part of the at least one digital media asset; or to establish permission or denial to execute the at least one branding action or the post read and write requests of the at least one writable metadata. To do this, controlled by the at least one excelsior enabler. The App may establish at least one connection, which is usually through the Internet, with a programmable communications console, which is usually a combination of an API protocol and graphic user interface (GUI) as part of a web service. In addition, the at least one excelsior enabler provides reestablished credentials to the programmable communications console as part of the at least one membership, in which The App is facilitating and monitoring, to authenticate the data

communications session used to send and receive data requests between the at least one membership and The App.

[00015] In accordance with another embodiment of the present invention, the present invention teaches a method for monitoring access to an encrypted digital media and facilitating unlimited interoperability between a plurality of data processing devices. The method comprises receiving a branding request from at least one communications console of the plurality of data processing devices, the branding request being a read and write request of metadata of the encrypted digital media, the request comprising a membership verification token corresponding to the encrypted digital media. Subsequently, the membership verification token is authenticated, the authentication being performed in connection with a token database. Thereafter, connection with the at least one communications console is established. Afterwards, at least one electronic identification reference is requested from the at least one communications console. Further, the at least one electronic identification reference is received from the at least one communications console. Finally, branding metadata of the encrypted digital media is performed by writing the membership verification token and the electronic identification reference into the metadata.

[00016] The present invention is particularly useful for giving users the freedom to use products outside of the device in which the product was acquired and extend unlimited interoperability with other compatible devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[00017] For a more complete understanding of the present invention, the needs satisfied thereby, and the objects, features, and advantages thereof, reference now is made to the following description taken in connection with the accompanying drawings.

[00018] FIG. 1 shows a system for monitoring access to an encrypted digital media according to an embodiment of the present invention.

[00019] FIG. 2 shows a system for authoring an encrypted digital media according to an embodiment of the present invention.

[00020] FIG. 3 shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention.

[00021] FIG. 4 shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention.

[00022] FIG. 5 shows personalized digital rights management component as part of a compatible machine with writable static memory.

[00023] FIG.6 shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention

[00024] FIG.7 shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention.

[00025] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention

DETAILED DESCRIPTION OF THE DRAWINGS

[00026] Before describing in detail the particular system and method for personalised digital media access system in accordance with an embodiment of the present invention, it should be observed that the present invention resides primarily in combinations of system components related to the device of the present invention.

[00027] Accordingly, the system components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[00028] In this document, relational terms such as `first` and `second`, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms `comprises`, `comprising`, or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by `comprises . . . a` does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises the element.

The present invention is directed at providing infinite access rights of legally acquired at least one encrypted digital media asset to the content acquirer, explained in this document as the excelsior enabler, and optionally to their recognized friends and family, explained in this document as a plurality of secondary enablers. To explain further, the excelsior enabler and secondary enablers defined comprises human beings or computerized mechanisms programmed to process steps of the invention as would normally be done manually by a human being. Additionally,, an apparatus used alone or in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods with a connection are needed (herein referred to as The App). To deliver the requirements of the invention, communicative and connected elements comprise: verification, authentication,

electronic ID metadata branding, additional technical branding, and cross-referencing. The connection handling the communicative actions of the invention will usually be the Internet and can also be an internal apparatus cooperative. The App can further be defined as a Windows OS, Apple OS, Linux OS, and other operating systems hosting software running on a machine or device with a capable CPU, memory, and data storage. The App can be even further defined as a system on a chip (SOC), embedded silicon, flash memory, programmable circuits, cloud computing and runtimes, and other systems of automated processes.

[00029] The digital media assets used in this system are encrypted usually with an AES cipher and decryption keys are usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connection usually an Internet server. As explained earlier, the system we will discuss will work as a front-end to encrypted files as an authorization agent for decrypted access.

[00030] FIG. 1 shows a system **100** for monitoring access to an encrypted digital media according to an embodiment of the present invention. The system **100** includes a first recipient module **102**, an authentication module **104**, a connection module **106**, a request module **108**, a second receipt module **110** and a branding module **112**. The first receipt module **102** receives a branding request from at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media and includes a membership verification token corresponding to the encrypted digital media. Examples of the encrypted digital media includes, and are not limited to, one or more of a video file, audio file, container format, document, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

[00031] Subsequently, the authentication module **104** authenticates the membership verification token. The authentication is performed in connection with a token database. Further, the connection module **106** establishes communication with the at least one communication console.

[00032] According to an embodiment of the present invention, the connection is established through one of internet, intranet, Bluetooth, VPN, Infrared and LAN.

[00033] According to another embodiment of the present invention, the communication console is a combination of an Application Programmable interface (API) protocol and graphic user interface (GUI) as a part of web service. The API is a set of routines, data structures, object classes, and /or protocols provided by libraries and / or operating system services. The API is either one of language dependent or language independent.

[00034] The request module **108** requests at least one electronic identification reference from the at least one communication console. The second receipt module **110** receives the at least one electronic identification reference from the least one communication console. The branding module **112** brands metadata of the encrypted digital media by writing the membership verification token and the electronic identification into the metadata.

[00035] **FIG. 2** shows a system **200** for authoring an encrypted digital media according to an embodiment of the present invention. The figure includes a selection module **202**, a password module **204**, a customization module **206**, a database module **208** and an encryption module **210**. The selection module **202** facilitates selection of one or more media items to form the encrypted digital media. Examples of the one or media items include, and are not limited to, one or more of a video, an audio and a game.

[00036] According to an embodiment of the present invention, the one or more media items are one or more of remote URL links and local media files.

[00037] The password module **204** prompts the user to enter a master password which provides access to the encrypted digital media. Subsequently, the customization module **206** allows the user to customize the user access panel of the encrypted digital media.

[00038] According to an embodiment of the present invention, the customization module **206** facilitates adding one or more of a banner, a logo, an image, an advertisement, a tag line, a header message and textual information to the user access panel of the encrypted digital media.

[00039] Further, the database module **208** connects the encrypted digital media to a database of membership verification token required for decrypting the encrypted digital media.

[00040] According to an embodiment of the present invention, the membership verification token is a kodekey. The kodekey is a unique serial number assigned to the encrypted digital media.

[00041] The encryption module **210** encrypts the one or more media items to create the encrypted digital media.

[00042] According to an embodiment of the present invention, the system **200** further includes a watermark module. The watermark module watermarks information on the encrypted digital media, wherein the watermark is displayed during playback of the encrypted digital media.

[00043] According to another embodiment of the present invention, the system **200** further includes an access module. The access module allows the user to define access rights. Examples of the access rights include, but are not limited to, purchasing rights, rental rights and membership access rights.

[00044] According to yet another embodiment of the present invention, the system **200** further includes a name module. The name module allows the user to name the encrypted digital media.

[00045] FIG. 3 shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention. The process is achieved by way of an enabler using an apparatus or otherwise known as an application in which facilitates digital media files. The apparatus interacts with all communicative parts required to fulfill the actions of the invention. The figure shows a Kodekey Graphical User Interface (GUI) **301**, a product metadata **302**, a networking card **303**, internet **304**, **306** and **308**, database **305** and **309** and an APIwebsite.com GUI **307**. A user posts a branding request via the Kodekey GUI interface **301**. The Kodekey GUI interface **301** is the GUI for entering token. The Kodekey GUI interface **301** prompts the user to enter the token and press the redeem button present on the Kodekey GUI interface **301**. The product metadata **302** is read / writable metadata associated with the digital media to be acquired. The networking card **303** facilitates querying of optional metadata branding process and referenced. The Kodekey GUI interface is connected to the database **305** via the internet **304** through the networking card **303**. The database **305** is the database used to read/write and store the tokens, also referred to as token database. The user is redirected to the APIwebsite.com GUI **307** through the internet **306**. The APIwebsite.com is the GUI to the membership API in which the electronic ID is collected and sent back to the Kodekey GUI interface **301**. The APIwebsite.com GUI **307** prompts the user to enter a login id and a password to access the digital media which is acquired from the database **309** through the internet **308**. The database **309** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00046] Examples of the encrypted digital files include, and are not limited to, a video file, an audio file, container formats, documents, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

[00047] FIG. 4 shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention. Subsequently, the communicative parts to cross-reference information stored in the metadata of the digital media asset are checked which has been previously handled by the process of FIG. 1. The figure shows an enabler access request **401**, a product metadata **402**, a networking card **403**, an internet **404**, **406** and **408**, a database **405** and **409** and an APIwebsite.com GUI **407**, The enabler access request **401** facilitates the user to make a request for the digital media. The product metadata **402** is read / writable metadata associated with the digital media to be acquired. The networking card **403** facilitates querying of optional metadata branding process and referenced. The database **405** is the database used to read/write and store the tokens. The APIwebsite.com GUI **407** is the GUI in which the electronic ID is collected and sent back to the Kodekey GUI interface **301.** The APIwebsite.com GUI **407** prompts the user to enter a login id and a password to access the digital media from the database **409** through the internet **408**. The database **409** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00048] FIG. 5 shows personalized digital rights management component as part of a compatible machine with writable static memory. The figure represents an authorization sequence action in which a machine is authorized to accept a personalized digital media file. The figure includes STR3EM Machine GUI **501** including the connect icon **502**, a load key file icon **503**, a networking card **504**, an internet **505**, **508** and **510**, a database **506** and **511**, a machine memory **507** and a APIwebsite.com GUI **509**. The STR3EM Machine GUI **501** prompts the user to connect or load a key file to authorize the device through the connect icon

502 and the load key file icon **503**. The STR3EM Machine GUI **501** is connected to the networking card **504**. The networking card **504** facilitates querying of optional metadata branding process and referenced. Further, the STR3EM machine GUI **501** is connected to the database **506** via the internet **505**. The database **506** is the database used to read/write and store the tokens. Moreover, STR3EM Machine GUI **501** is connected to the machine memory **507**. The machine memory **507** represents the internal memory of the machine or device so authorizations can be saved for access of the digital media. The APIwebsite.com GUI **509** is connected to the STR3EM machine GUI through the internet **508**. Further, APIwebsite.com GUI **509** is connected to the database **511** through the internet **510**. The APIwebsite.com GUI **509** prompts the user to enter the login id and a password to authorize the access to digital media. The database **511** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00049] FIG.6 shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention. At step **602**, a branding request is made by a user from at least at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media.

[00050] According to an embodiment of the present invention, the request includes a membership verification token corresponding to the encrypted digital media.

[00051] Subsequently, the membership verification token is authenticated at step **604**. The authentication is performed in connection with a token database. Further, connection with the at least communication console is established at step **606**. Afterwards, at least one electronic identification reference is requested from the at least one communications console at the step **608**. At step **610**, at least one electronic identification reference in received from the at least

one communication console. Finally, metadata of the encrypted digital media is branded by writing the membership verification token and the electronic identification reference into the metadata at the step **612**.

[00052] FIG.7 shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention. At step **702**, one or more media items are selected by the user to form the encrypted digital media. Subsequently, a master password is entered for providing access to the encrypted digital media for editing at step **704**. Afterwards, the user customizes the user panel of the encrypted digital media at step **706**. Further, the encrypted digital media is connected to a database of membership verification tokens required for decrypting the encrypted digital media at the step **708**. Finally, the one or more media items are encrypted to create the encrypted digital media at the step **710.**

[00053] According to various embodiments of the present invention, the verification is facilitated by at least one token handled by at least one excelsior enabler. Examples of the token include, and are not limited to, a structured or random password, e-mail address associated with an e-commerce payment system used to make an authorization payment, or other redeemable instruments of trade for access rights of digital media. Examples of e-commerice systems are PayPal, Amazon Payments, and other credit card services.

[00054] According to an embodiment of the present invention, an identifier for the digital media is stored in a database with another database of a list of associated tokens for cross-reference identification for verification.

[00055] According to an embodiment of the present invention, the database of a list of associated tokens includes Instant Payment Notification (IPN) received from successful financial e-commerce transactions that includes the identifier for the digital media; import of CSV password lists, and manually created reference phrases.

[00056] For this discussion, the structured or random password example will be used as reference. The structured or random passwords can be devised in encoded schemes to flag the apparatus of permission type such as: 1) Purchases can start a password sequence with "P" following a random number, so further example would be "PSJD42349MFJDF". 2) Rentals can start or end a password sequence with "R" plus (+) the number of days a rental is allowed, for example "R7" included in "R7SJDHFG58473" flagging a seven day rental. 3) Memberships can start or end a password sequence with "M" plus (+) optionally the length of months valid for example "M11DFJGH34KF" would flag an eleven-month membership period.

[00057] According to an embodiment of the present invention, the tokens are stored in a relational database such as MySQL or Oracle. Cloud storage systems such as Amazon's Web Services Simple Storage Solution, or also known as S3, provides a highly available worldwide replicated infrastructure. In addition to S3, monetization offerings such as DevPay offer developers the opportunity to make money from applications developed to use the services.

[00058] The verification will reference to the S3 and DevPay services for example purposes only as many options such as FTP, SimpleDB, solid state storage and others can be used to host the token hosting needed for the verification element of this invention. The token represents permission from the content provider to grant access rights to the excelsior enabler and thereafter the plurality of secondary enablers. To set up the verification the content provider can manually or automatically generate a single or a plurality of structured or random password in which will represent the token. By using public or private access of S3 as part of an apparatus, the content provider can create empty text files giving each the name of the passwords generated. Because S3 is associated with a highly available worldwide infrastructure, to check this password token can be done my simply constructing a HTTP

request from the apparatus and triggering follow up actions based on either a 200 HTTP response, which means OK at which point the next action can happen, or a 400 HTTP response which means ERROR at which point the verification process is voided. An additional token can be used to provide a flag to the apparatus that the verification element has been fulfilled for an initial verification token. Creating an alternate version of the first token by appending a reference to the end, for example, does this: "M11DFJGH34KF_user@str3em.com_01_01_11". In this example, it is defined that the eleven month authorized membership token was verified by a user@str3em.com on January 1, 2011. By providing a second token, the first token becomes locked to ownership by the excelsior enabler preventing unauthorized users from reusing the first token without providing the authentication associated with the alternative referenced second token. In the interest of providers of the apparatus delivering this invention, this document will teach a method of a HTTP PUT calculation scheme for automatic royalty billing and administration for the token element used in the invention. Amazon's DevPay allow developers to attach monetary charges to data services of S3 offered as an embedded component of the apparatus. By using the "PUT" requests parameter, tokens generated by the apparatus are monitored, calculated, and charged to clients of the apparatus provider. For example: the default charge measure for DevPay is $0.05 for every 1000 PUT request. By changing the amount to $1.00 for every 1000 PUT requests, the apparatus provider is paid a $0.10 royalty for each token created. Content providers using a connected apparatus like DevPay to deliver and manage digital media distribution do not need to have restrictions on the tokens created as with prior art DRM key providers as DevPay is charged on a pay-as-you-need model on a monthly basis. As a novelty to the apparatus provider, if a content provider fails to pay royalties due, the DevPay hosting will automatically deny token access to all related media products in distribution and restore this verification element when royalties are paid in full.

[00059] The authentication element of this invention is at least handled first by the at least one excelsior enabler with a connection to a membership. In the present discussion, the connection is equal to the Internet and the membership is equal to a web service. Further, the web service must be available for two way data exchange to complete the authentication process of this invention. Data exchange with a web service is usually facilitated with a programmable communications console, at most times, will be an Applications Programmable Interface (API). An API is a set of routines, data structures, object classes, and/or protocols provided by libraries and/or operating system services in order to support the building of applications. An API may be language-dependent: that is, available only in a particular programming language, using the particular syntax and elements of the programming language to make the API convenient to use in this particular context. Alternatively an API may be language-independent: that is, written in a way that means it can be called from several programming languages (typically an assembly/C-level interface). This is a desired feature for a service-style API that is not bound to a particular process or system and is available as a remote procedure call. A more detailed description of API that can be used for an apparatus can be found in the book, "Professional Web APIs with PHP: eBay, Google, Paypal, Amazon, FedEx plus Web Feeds", by Paul Reinheimer, Wrox publishers (2006). A program apparatus, scripts, often calls these APIs or sections of code residing on user computerized devices. For example, a web browser running on a user computer, cell phone, or other device can download a section of JavaScript or other code from a web server, and then use this code to in turn interact with the API of a remote Internet server system as desired. A Graphic User Interface (GUI) can be installed for human interaction or processes can be preprogrammed in a programmable script such as PHP, ASP.Net, Java, Ruby on Rails and others. The authentication element of the invention is usually embedded as a process of the apparatus but could be linked dynamically. In this

document, the embedded version using a GUI will be used as reference. The web service equipped with the API is usually a well-known membership themed application in which the users must use an authentic identification. Some example includes Facebook in which as a rule, members are required to use their legal name identities. A reference number or name with the Facebook Platform API represents this information. Other verified web services in which real member names are required such as the LinkedIn API and the PayPal API and even others could be used, but for this discussion, Facebook will be used only as an example of how the authentication element of the invention is utilized. The Facebook API system, as well as others, operates based on an access authentication system called from a connected apparatus (which is usually an Internet powered desktop or browser based application) with an API Key, an Application Secret Key and could also include an Application ID. For example, the Facebook API Application Keys required to establish a data exchange session with the connected apparatus might look like:

API Key

37a925fc5ee9b4752af981b9a30e9a73gh

Application Secret

f2a2d92ef395cce88eb0261d4b4gsa782

Application ID

51920566446

[00060] The collective API keys are usually embedded in the source code of the apparatus, or stored on a remote Internet server, and could be included in the encrypted digital media metadata and inserted on-the-fly into calls made to the API from the connected apparatus. This allows dynamic API connection of the apparatus using keys issued to individual content providers so in the event of a reprimand of a single the individual content provider by the API

provider, the collective the individual content providers and the enablers of the connected apparatus are not affected.

[00061] Upon an access request of the digital media, the excelsior enabler interacts with the apparatus, usually software or web application, to enter membership credentials in a GUI front-end connected to the API. The membership credentials are usually comprised of a login element comprising a name, phrase, or e-mail address, and a secret password. The credentials can be generated by the enabler or automatically generated by the web service. Once the enabler authenticates their identity with the membership, the apparatus facilitating the data communication can request relevant information to fulfill the process chain of the invention. For example, Facebook API Platform defines members as ID numbers, so if a member's real name is John Doe, then Facebook API ID (also programmatically known as the FBID) would be 39485678. Once the enabler successfully sign in to the GUI element then the apparatus will query the API for at least one electronic identification reference, in this discussion is the FBID. The FBID is received to the permanent or temporary memory of the apparatus to sustain the branding and cross-referencing requirements of the invention. Additional information can be requested according to membership status or connected "friends" of the enabler. Additional information can be made required for successful authentication and includes: a minimum amount of total friends, a minimum amount of female friends, a minimum amount of male friends, a minimum amount of available pictures, a minimum age limit and other custom rules can be defined by the apparatus. An example of how this would work is a content provider can define a minimum of 32 Facebook friends are required to access an encrypted digital media asset offered for sale or promotion. This is achieved by the apparatus handling a access request in which the enabler has not yet acquired access rights by executing and parsing information returned by the Facebook "Friends.get" API command.

[00062] XML return example of the Facebook "Friends.get" API command where a plurality of FBID are returned to the apparatus for parsing additional information as may be required to satisfy successful authentication:

<?xml version="1.0" encoding="UTF-8"?>

<friends_get_response xmlns="http://api.facebook.com/1.0/"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://api.facebook.com/1.0/ http://api.facebook.com/1.0/facebook.xsd" list="true">

<uid>222333</uid>

<uid>1240079</uid>

</friends_get_response>

[00063] When authenticating a compatible device or machine which may not have access to a connection for the authentication element, a key file or part of the metadata thereof could be made on another connected compatible device or machine and allow the enabler to execute Friends.get API command to collect and store the complete list of a plurality of FBID to the key file or the metadata thereof. The compatible device or machine which may not have access to a connection for the authentication element with an embedded interaction console, usually a user GUI, can request and load the key file or part of the metadata thereof to save the complete list of a plurality of electronic identification references, in this discussion is reference as the FBID, to storage or metadata as part of the compatible device or machine. This step ensures the cross-referencing element requirement of the invention can take place in the event the connection for the authentication element is not present in the compatible device or machine.

[00064] Another example is a content provider can allow shared access to friends of the excelsior enabler after a time period, like for example, 90 days. After the 90 day period, when

media access is requested using the authentication element by a plurality of secondary enablers, which are usually friends and family of the excelsior enabler, the FBID of the excelsior enabler is cross-referenced with the FBID of the requesting secondary enabler by way of the apparatus ability to execute the Facbeook "Friends.areFriends" API command.

[00065] XML return example of the Facebeook "Friends.areFriends" API command where FBID 2223322 and 2222333 are friends and FBID 1240077 and 1240079 are not friends:

<?xml version="1.0" encoding="UTF-8"?>

<friends_areFriends_response

xmlns=http://api.facebook.com/1.0/

xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

xsi:schemaLocation="http://api.facebook.com/1.0/ http://api.facebook.com/1.0/facebook.xsd" list="true">

<friend_info>

<uid1>222332</uid1><uid2>222333</uid2>

<are_friends>1</are_friends>

</friend_info>

<friend_info>

<uid1>1240077</uid1><uid2>1240079</uid2>

<are_friends>0</are_friends>

</friend_info>

</friends_areFriends_response>

[00066] Such usability can be important to sustain "fair use" rights of consumers of the digital media to emulate usability found with physical media products such as CD and DVD that can be loaned to friends and family after an inception grace period.

[00067] Once the information of the verification and authentication elements is acquired, the apparatus handles the next process of writing the information to the digital media metadata and can include additional information gathered from components of The App. Components of The App can include MAC address from a networking card, CRC checksum of an embedded file or circuit, SOC identifier, embedded serial number, OS version, web browser version, and many other identifiable components as part of The App. For this discussion, the MAC address from a networking card as part of The App will be used as reference of a secondary electronic identification reference. In computer networking, a Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address. The novelty of embedding the MAC address along with the FBID of the excelsior enabler is to provide a plurality of electronic identification references in which cross-referencing actions can allow more rapid access to be granted with less interaction from an enabler. For example, to retrieve the FBID from Facebook to cross-reference with the FBID stored in the digital media metadata requires the enabler to possibly physically need to enter their login and password credentials to the GUI connected to the apparatus. It may be possible that web browser cookies allow automatic Facebook login by storing an active session key, but the session key is not guaranteed to be active at the time of an access request. While the enabler may not have an issue executing another authentication command, several remote operations could exist to control authentication and access requests separately from each other. The apparatus can execute a programmable retrieval command, usually a GET command, to locate and retrieve the MAC address from an attached or connected networking card. After

the FBID is acquired, the MAC address is also acquired to write the plurality of electronic identifications to the metadata of the at least one encrypted digital media asset by; obtaining the decryption key to decrypt the encrypted digital media asset which is usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connected source, usually an Internet server with an encrypted HTTPS protocol. A plurality of MAC addresses can be stored along with the FBID of the excelsior enabler to manage access rights across a plurality of devices. To understand metadata and the uses, metadata is defined simply as to "describe other data". It provides information about certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document. Web pages often include metadata in the form of Meta tags. Description and keywords Meta tags are commonly used to describe the Web page's content. Most search engines use this data when adding pages to their search index. In the invention, the FBID and MAC addresses are written to the digital media asset metadata to prepare for the instant or delayed cross-referencing element of the invention. The same process of writing the information to the digital media metadata is true with secondary enablers allowing the same benefits of cross-referencing.

[00068] Cross-referencing, the last element of the invention is used to verify access rights of an enabler of a pre or post personalized encrypted digital media asset. Once an enabler executes an action for access request, the apparatus will obtain the decryption key to first seek the MAC address record. If the MAC address is found, then a cross-reference process is executed by comparing the MAC address retrieved from the metadata of the digital media file with the MAC address retrieved from the networking card connected to the apparatus or The App. If the comparison action proves to be true, then access rights are granted to the enabler.

If the comparison fails, then the apparatus can either ask the enabler to participate in communication with the authentication element of the invention, or could deny further interactivity with the enabler. In this discussion, the apparatus requires the enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook API. If the comparison action proves to be true, then access rights is granted to the excelsior enabler and the current MAC address of the networking card as part of The App is appended to the metadata of the encrypted digital media asset and access rights is granted to the excelsior enabler. If the FBID cross-reference fails, then the apparatus can either ask the potential secondary enabler to participate in communication with the authentication element of the invention, or could deny further interactivity with the potential secondary enabler. In this discussion, the apparatus requires the potential secondary enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook "Friends.areFriends" API command to determine if the potential secondary enabler identity is true or false. The determination is in accordance to any possible access grace periods set by the content provider of the encrypted digital media asset. If the comparison action proves to be true, then access rights is granted to the secondary enabler and the current MAC address of the networking card as part of The App and the FBID retrieved are appended to the established metadata information of the encrypted digital media asset and access rights can be granted to a plurality of secondary enablers; unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments is achieved.

[00069] While the present invention has been described in connection with preferred embodiments, it will be understood by those skilled in the art that variations and modifications of the preferred embodiments described above may be made without departing from the scope of the invention. Other embodiments will be apparent to those skilled in the art from a consideration of the specification or from a practice of the invention disclosed herein. It is intended that the specification and the described examples are considered exemplary only, with the true scope of the invention indicated by the following claims.

[00070] CLAIMS

What is claimed is:

1. A method for monitoring access to an encrypted digital media, the method facilitating unlimited interoperability between a plurality of data processing devices, the method comprising:

    a. receiving a branding request from at least one communications console of the plurality of data processing devices, the branding request being a read and write request of metadata of the encrypted digital media, the request comprising a membership verification token corresponding to the encrypted digital media;

    b. authenticating the membership verification token, the authentication being performed in connection with a token database;

    c. establishing connection with the at least one communications console;

    d. requesting at least one electronic identification reference from the at least one communications console;

    e. receiving the at least one electronic identification reference from the at least one communications console; and

    f. branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata.

2. The method according to claim 1, wherein the membership verification token is one or more of a structured password, a random password, e-mail address and one or more redeemable instruments of trade for access rights of the encrypted digital media.

3. The method according to claim 1, wherein the branding request being a request from an excelsior enabler through a data processing device of the plurality of data processing devices, the excelsior enabler being the user acquiring access rights to the encrypted digital media.

4. The method according to claim 3, wherein the branding request being a request from one or more secondary enablers connected to the excelsior enabler, the plurality of second enablers comprising one or more of human beings and programmed computerized mechanisms in network of the excelsior enabler.

5. The method according to claim 1 or 3, wherein the membership verification token represents verification from content provider to grant access rights to the excelsior enabler and the one or more secondary enablers.

6. The method according to claim 1, wherein the encrypted digital media is shared with one or more users after a predefined period.

7. The method according to claim 1, wherein the encrypted digital media is one of a video file, audio file, container format, document, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

8. The method according to claim 1, wherein the electronic identification reference is a web service account, the web service capable of facilitating service two way data exchange to complete the verification process.

9. The method according to claim 1, wherein the electronic identification reference is a key certificate, the key certificate being uploaded by the at least one communications console for branding the encrypted digital media.

10. A computer program product for use with a computer, the computer program product comprising a computer usable medium having a computer readable program code stored therein for monitoring access to an encrypted digital media, the method facilitating unlimited interoperability between a plurality of data processing devices, the computer program product performing the steps of:

    a. receiving a branding request from at least one communications console of the plurality of data processing devices, the branding request being a read and write request of metadata of the encrypted digital media, the request comprising a membership verification token corresponding to the encrypted digital media;

    b. authenticating the membership verification token, the authentication being performed in connection with a token database;

    c. establishing connection with the at least one communications console;

    d. requesting at least one electronic identification reference from the at least one communications console;

    e. receiving the at least one electronic identification reference from the at least one communications console; and

    f. branding metadata of the encrypted digital media by writing the membership verification token and the electronic identification reference into the metadata.

11. The computer program product according to claim 10, wherein the membership verification token is one or more of a structured password, a random password, e-mail address and one or more redeemable instruments of trade for access rights of the encrypted digital media.

12. The computer program product according to claim 10, wherein the branding request being a request from an excelsior enabler through a data processing device of the plurality of data processing devices, the excelsior enabler being the user acquiring access rights to the encrypted digital media.

13. The computer program product according to claim 12, wherein the branding request being a request from one or more secondary enablers connected to the excelsior enabler, the plurality of second enablers comprising one or more of human beings and programmed computerized mechanisms in network of the excelsior enabler.

14. The computer program product according to claim 10 or 13, wherein the membership verification token represents verification from content provider to grant access rights to the excelsior enabler and the one or more secondary enablers.

15. A computer program product for use with a computer, the computer program product comprising a computer usable medium having a computer readable program code stored therein for authoring an encrypted digital media capable of unlimited interoperability between a plurality of data processing devices, the computer program product performing the steps of:

    a. selecting one or more media items to form the encrypted digital media;

    b. entering a master password which provides access to the encrypted digital media for editing;

    c. customizing user access panel of the encrypted digital media;

    d. connecting the encrypted digital media to a database of membership verification tokens required for decrypting the encrypted digital media; and

    e. encrypting the one or more media items to create the encrypted digital media.

16. The computer program product according to claim 15, wherein the one or more media items is one or more of a video, an audio and a game.

17. The computer program product according to claim 15 further comprising watermarking information on the encrypted digital media, the watermark being displayed during playback of the encrypted digital media.

18. The computer program product according to claim 15, wherein the membership verification token is a kodekey, the kodekey being a unique serial number assigned to the encrypted digital media.

19. The computer program product according to claim 15 further comprising defining access rights to the encrypted digital media, wherein the access rights includes one of a purchasing rights, rental rights and membership access rights.

20. The computer program product according to claim 15 further comprising defining a predefined time after which the encrypted digital media is shared with one or more users, the one or more users being network of friends of the excelsior enabler.

ABSTRACT

The invention is an apparatus that facilitates access to encrypted digital media to accept verification and authentication from an excelsior enabler using at least one token and at least one electronic identification. The at least one electronic identification could be a device serial number, a networking MAC address, or a membership ID reference from a web service. Access to the product is also managed with a plurality of secondary enablers using the at least one electronic identification reference.

USPTO CUSTOMER #70984
INVENTOR: WILLIAM GRECIA

Electronic filing request:

Applicant William Grecia hereby requests early publication as set forth in 37 CFR 1.219 and 37 CFR 1.215 for the non-provisional patent application attached with this request. Early publication request fee is attached through EFS Web Customer Number 70984.

Sincerely yours,

William Grecia

Inventor Pro Se