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	REQUEST ID
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	157942

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 02/02/2022 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

X Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/Greg T. Sueoka/
Name:	Greg T. Sueoka
Registration Number:	33800

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:21-cv-00210	3/5/2021	Western District of Texas

PLAINTIFF	DEFENDANT
PROXENSE,LLC,	SAMSUNG ELECTRONICS,CO., LTD. and SAMSUNG ELECTRONICSAMERICA, INC,

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,352,730	1/8/2013	Proxense, LLC
2	9,298,905	3/29/2016	Proxense, LLC
3	10,698,989	6/30/2020	Proxense, LLC
4	9,049,188	6/2/2015	Proxense, LLC
5	9,235,700	1/12/2016	Proxense, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	03/29/2016	9298905	10001-04540 US	8239

89194 7590 03/09/2016

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

John J. Giobbi, Bend, OR;
Proxense, LLC, Bend, OR

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

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.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

89194 7590 02/22/2016

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
02/22/2016	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):

docketing@patentlawworks.net
patents@patentlawworks.net

Response to Rule 312 Communication	Application No.	Applicant(s)
	14/521,982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

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

1. ☒ The amendment filed on *04 February 2016* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

Please enter amendments filed 02/04/2016, and disregard amendments filed 01/20/2016. Thank you.

/TAGHI ARANI/ Supervisory Patent Examiner, Art Unit 2438	/PHY ANH VU/ Examiner, Art Unit 2438

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

89194 7590 12/16/2015
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

TITLE OF INVENTION: Biometric Personal Data Key (PDK) Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2438	713-186000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Patent Law Works LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Proxense, LLC
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Bend, OR

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ☒ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
❑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
❑ A check is enclosed.
☒ Payment by credit card. ~~Form PTO-2038 is attached.~~ XXXXXXXXXXXXXXXX
❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

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

Authorized Signature /Paige Alsbury/ Date February 19, 2016
Typed or printed name Paige M. Alsbury Registration No. 72,965

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

Electronic Patent Application Fee Transmittal

Application Number:	14521982
Filing Date:	23-Oct-2014
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Paige McDede Alsbury/Cynthia Kersey
Attorney Docket Number:	10001-04540 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

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

Electronic Acknowledgement Receipt	
EFS ID:	24968986
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	19-FEB-2016
Filing Date:	23-OCT-2014
Time Stamp:	16:45:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	3830
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	04540US2016-02-19-IssueFeeTransmittal.pdf	95723 2390c8657c485ce4523058c7186f63caae2c10a1	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30517 f8d9d51ece875e57daa7527ab3071f274611ee02	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	126240		

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.

Response to Rule 312 Communication	Application No.	Applicant(s)
	14/521,982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

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

1. ☒ The amendment filed on *04 February 2016* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

Please enter claim set dated 02/04/2016, and disregard the claim set filed 01/20/2015. Thank you.

/PHY ANH VU/
Examiner, Art Unit 2438

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2438
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: February 4, 2016 By: /Matthew M. Holmes/
Matthew M. Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. § 1.312
AND COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Sir/Madam:

In response to the Notices of Allowance and Allowability dated December 16, 2015, please amend the above-identified application as indicated in the present Amendment and disregard the Amendment filed January 20, 2016, which included errors in the numbers identifying the dependencies of dependent claims:

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (Currently Amended) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on an integrated device;

responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ~~user as the legitimate user based on the comparison of the~~ ID code, allowing the user to complete a financial transaction.

3. (Previously Presented)The method of claim 2, further comprising:

registering an age verification for the user in association with the ID code.

4. (Previously Presented) The method of claim 2, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (Previously Presented) The method of claim 2, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Previously Presented) The method of claim 2, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Currently Amended) The method of claim 2, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

8. (Canceled)

9. (Currently Amended) The method of claim 2, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

10. (Previously Presented) The method of claim 2, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (Previously Presented) An integrated device comprising:

a persistent storage media that persistently stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction.

12. (Previously Presented) The integrated device of claim 11, wherein the ID code is transmitted to the third-party trusted authority over a network.

13. (Previously Presented) The integrated device of claim 11, wherein an age verification is registered in association with the ID code.

14. (Previously Presented) The integrated device of claim 11, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (Currently Amended) A system, comprising:

an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the-ID code; an authentication circuit that receives the ID code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received ~~a user~~ based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.

16. (Previously Presented) The system of claim 15 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (Previously Presented) The system of claim 15, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (Previously Presented) The system of claim 15, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

19. (Currently Amended) The system of claim 15, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

20. (Currently Amended) The system of claim 15, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

REMARKS/ARGUMENTS

Regarding the present Amendment, entry of this Amendment is respectfully requested since the Amendment does not add new matter and does not require a new search.

With regard to the amendments to claims 1 and 15, during the final review of the allowed claim language prior to paying the issue fee, Applicant's Representative noticed inconsistencies between the language of claims 1, 11 and 15. The amendments to claims 1 and 15 are needed to make the claim language of claims 1 and 15 more consistent with the language of claim 11. Since claim 11 recites "receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction" and claim 11 is allowed, neither the amendment of claim 1 to recite "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction" nor the amendment of claim 15 to recite "the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes" require a new search and claims 1 and 15 as amended herein are allowable.

With regard to the amendments to claims 7, 9, 19 and 20, the amendments are intended to enhance readability as the language "the complete a financial transaction" is awkward and to address an antecedent basis issue since the independent claims recite "a financial transaction." The amendment was not presented previously because the portions of claims 7, 9, 19 and 20

amended includes language that was entered by the Examiner's Amendment that accompanied the Notice of Allowability.

With regard to the Examiner's statement for reasons of allowance, the Examiner's statement is based on claim elements of independent claim 1. It should be noted that the claim language of independent claims 11 and 15 may differ from that of claim 1, and that claims 11 and 15 are patentable for the elements they recite, which may differ from claim 1.

Respectfully submitted,
JOHN J. GIOBBI

Dated: February 4, 2016 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

Electronic Acknowledgement Receipt	
EFS ID:	24822283
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	04-FEB-2016
Filing Date:	23-OCT-2014
Time Stamp:	16:24:05
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		04540US2016-02-04-ReplacementAfterAllowance312Amendment.pdf	84617 28343d59048e9a5ad758d2e18e581b117e8983d3	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	8
Warnings:			
Information:			
	Total Files Size (in bytes):	84617	

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

89194 7590 02/01/2016

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
02/01/2016	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):

docketing@patentlawworks.net
patents@patentlawworks.net

Response to Rule 312 Communication	Application No.	Applicant(s)
	14/521,982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

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

1. ☒ The amendment filed on *20 January 2016* under 37 CFR 1.312 has been considered, and has been:

a) ☐ entered.

b) ☒ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/TAGHI ARANI/ Supervisory Patent Examiner, Art Unit 2438	/PHY ANH VU/ Examiner, Art Unit 2438

OK TO ENTER: /P.V./

01/21/2016

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (Currently Amended) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on an integrated device;

responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ~~user as the legitimate user based on the comparison of the~~ ID code, allowing the user to complete a financial transaction.

3. (Previously Presented)The method of claim 1, further comprising:

registering an age verification for the user in association with the ID code.

4. (Previously Presented) The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (Previously Presented) The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Previously Presented) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Currently Amended) The method of claim 1, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

8. (Canceled)

9. (Currently Amended) The method of claim 1, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

10. (Previously Presented) The method of claim 1, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (Previously Presented) An integrated device comprising:

a persistent storage media that persistently stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction.

12. (Previously Presented) The integrated device of claim 9, wherein the ID code is transmitted to the third-party trusted authority over a network.

13. (Previously Presented) The integrated device of claim 9, wherein an age verification is registered in association with the ID code.

14. (Previously Presented) The integrated device of claim 9, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (Currently Amended) A system, comprising:

an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the-ID code; an authentication circuit that receives the ID code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received ~~a user~~ based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.

16. (Previously Presented) The system of claim 13 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (Previously Presented) The system of claim 13, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (Previously Presented) The system of claim 13, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

19. (Currently Amended) The system of claim 13, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

20. (Currently Amended) The system of claim 13, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2438
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: January 20, 2016 By: /Matthew M. Holmes/
Matthew M. Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. § 1.312
AND COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Sir/Madam:

In response to the Notices of Allowance and Allowability dated December 16, 2015, please amend the above-identified application as indicated in the present Amendment:

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (Currently Amended) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on an integrated device;

responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ~~user as the legitimate user based on the comparison of the~~ ID code, allowing the user to complete a financial transaction.

3. (Previously Presented)The method of claim 1, further comprising:

registering an age verification for the user in association with the ID code.

4. (Previously Presented) The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (Previously Presented) The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Previously Presented) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Currently Amended) The method of claim 1, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

8. (Canceled)

9. (Currently Amended) The method of claim 1, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

10. (Previously Presented) The method of claim 1, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (Previously Presented) An integrated device comprising:

a persistent storage media that persistently stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction.

12. (Previously Presented) The integrated device of claim 9, wherein the ID code is transmitted to the third-party trusted authority over a network.

13. (Previously Presented) The integrated device of claim 9, wherein an age verification is registered in association with the ID code.

14. (Previously Presented) The integrated device of claim 9, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (Currently Amended) A system, comprising:

an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the-ID code; an authentication circuit that receives the ID code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received ~~a user~~ based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.

16. (Previously Presented) The system of claim 13 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (Previously Presented) The system of claim 13, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (Previously Presented) The system of claim 13, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

19. (Currently Amended) The system of claim 13, wherein ~~the complete a~~ completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

20. (Currently Amended) The system of claim 13, wherein ~~the complete a~~ completing the financial transaction includes accessing an application.

REMARKS/ARGUMENTS

Regarding the present Amendment, entry of this Amendment is respectfully requested since the Amendment does not add new matter and does not require a new search.

With regard to the amendments to claims 1 and 15, during the final review of the allowed claim language prior to paying the issue fee, Applicant's Representative noticed inconsistencies between the language of claims 1, 11 and 15. The amendments to claims 1 and 15 are needed to make the claim language of claims 1 and 15 more consistent with the language of claim 11. Since claim 11 recites "receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to-complete a financial transaction" and claim 11 is allowed, neither the amendment of claim 1 to recite "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction" nor the amendment of claim 15 to recite "the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes" require a new search and claims 1 and 15 as amended herein are allowable.

With regard to the amendments to claims 7, 9, 19 and 20, the amendments are intended to enhance readability as the language "the complete a financial transaction" is awkward and to address an antecedent basis issue since the independent claims recite "a financial transaction." The amendment was not presented previously because the portions of claims 7, 9, 19 and 20

amended includes language that was entered by the Examiner's Amendment that accompanied the Notice of Allowability.

With regard to the Examiner's statement for reasons of allowance, the Examiner's statement is based on claim elements of independent claim 1. It should be noted that the claim language of independent claims 11 and 15 may differ from that of claim 1, and that claims 11 and 15 are patentable for the elements they recite, which may differ from claim 1.

Respectfully submitted,
JOHN J. GIOBBI

Dated: January 20, 2016 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

Electronic Acknowledgement Receipt	
EFS ID:	24668668
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	20-JAN-2016
Filing Date:	23-OCT-2014
Time Stamp:	16:45:08
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		04540US2016-01-20-312Amendment.pdf	91265 9e12ada93bec3628c2f5e37f7971112 8a891b937	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	8
Warnings:			
Information:			
	Total Files Size (in bytes):	91265	

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

89194 7590 12/16/2015

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 12/16/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

TITLE OF INVENTION: Biometric Personal Data Key (PDK) Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2016

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

89194 7590 12/16/2015
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

TITLE OF INVENTION: Biometric Personal Data Key (PDK) Authentication

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/16/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2438	713-186000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
❑ Issue Fee
❑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
❑ A check is enclosed.
❑ Payment by credit card. Form PTO-2038 is attached.
❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

89194 7590 12/16/2015

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

EXAMINER	
VU, PHY ANH TRAN	
ART UNIT	**PAPER NUMBER**
2438	

DATE MAILED: 12/16/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Examiner-Initiated Interview Summary	**Application No.** 14/521,982	**Applicant(s)** GIOBBI, JOHN J.	
	Examiner PHY ANH VU	**Art Unit** 2438	

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

(1) *PHY ANH VU*. (3)_____.

(2) *Matthew Holmes*. (4)_____.

Date of Interview: *24 November 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *7, 9, 13, and 19-20*.

Identification of prior art discussed: *n/a*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Per SPE's approval, Examiner contacted Applicant's representative, Mr. Matthew Holmes to suggest filing a Terminal Disclaimer (TD) in order to move the case forward. Amendments to claims 7, 9, 13 and 19-20 were also suggested so that they can be consistent with their independent claims.

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

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/PHY ANH VU/ Examiner, Art Unit 2438	

Notice of Allowability	Application No. 14/521,982	Applicant(s) GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *09/14/2015*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *2-7 and 9-20*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 06/07/2015; 11/02/2015
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11/24/2015* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/PHY ANH VU/
Examiner, Art Unit 2438

DETAILED ACTION

This Office Action is in response to the Amendment filed 09/14/2015 and the Terminal Disclaimer filed 11/23/2015.

Authorization for this Examiner's Amendment was given in an interview with Mr. Matthew Holmes on 11/25/2015.

Notice of Pre-AIA or AIA Status

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

Response to Arguments

The 101 rejections made the previous Office Action is hereby withdrawn due to the amendment filed.

EXAMINER'S AMENDMENTS

Amend claims 7, 9, 13 and 19-20 as follow:

Claim 7:

The method of claim 2, wherein the ~~**action**~~ **complete a financial transaction** includes accessing an application.

Claim 9:

The method of claim 2, wherein the ~~**action**~~ **complete a financial transaction** includes accessing one or more of a casino machine, a keyless lock, ~~**a garage door opener,**~~ an ATM machine, ~~**a hard drive, computer software,**~~ a web site, a file and a financial account.

Claim 13:

The integrated device of claim 11, wherein an age verification is registered in association with the ~~**device**~~ ID code.

Claim 19:

The system of claim 15, wherein the ~~**action**~~ **complete a financial transaction** includes accessing one or more of a casino machine, a keyless lock, ~~**a garage door opener,**~~ an ATM machine, ~~**a hard drive, computer software,**~~ a web site, a file and a financial account.

Claim 20:

The system of claim 15, wherein the ~~**action**~~ **complete a financial transaction** includes accessing an application.

ALLOWABLE SUBJECT MATTER

Claims 2-7 and 9-20 are allowed while claims 1 & 8 are cancelled.

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

The present invention is directed to method, device and system for authenticating user using biometric information.

The closest prior arts cited are generally directed to various aspects of authenticating users using biometric information. However, none of the cited arts found alone or in combination suggests or teaches all the elements of the independent claims. For instance, no parts of the cited arts teach or suggest limitations such as persistently storing biometric data of a legitimate user and an ID code on an integrated device; responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third- party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction.

Therefore, the claims are allowable for the above reason.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on Wed 7:00-5:30, TH-F 7-5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PHY ANH VU/
Examiner, Art Unit 2438
/TAGHI ARANI/
Supervisory Patent Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	**Application No.** 14/521,982	**Applicant(s)** GIOBBI, JOHN J.	
	Examiner PHY ANH VU	**Art Unit** 2438	

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

(1) *PHY ANH VU*. (3)_____.

(2) *Matthew Holmes*. (4)_____.

Date of Interview: *24 November 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *7, 9, 13, and 19-20*.

Identification of prior art discussed: *n/a*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Per SPE's approval, Examiner contacted Applicant's representative, Mr. Matthew Holmes to suggest filing a Terminal Disclaimer (TD) in order to move the case forward. Amendments to claims 7, 9, 13 and 19-20 were also suggested so that they can be consistent with their independent claims.

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

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/PHY ANH VU/ Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 14/521,982	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,256,737 B1	07-2001	Bianco; Peter Garrett	G07C9/00158	713/186
*	B	US-2002/0056043 A1	05-2002	Glass, Randal W.	G06F21/32	713/179
*	C	US-2002/0091646 A1	07-2002	Lake, Lawrence L.	G06Q20/04	705/67
*	D	US-6,657,538 B1	12-2003	Ritter; Rudolf	G06F21/32	340/5.8
*	E	US-6,853,988 B1	02-2005	Dickinson; Alexander G.	G06F21/32	380/277
*	F	US-2013/0019295 A1	01-2013	PARK; Sung-Jin	H04L9/3213	726/7
*	G	US-2013/0111543 A1	05-2013	Brown; Jeremy Ray	H04L63/0884	726/1
*	H	US-2013/0276140 A1	10-2013	COFFING; Dan	H04L12/5895	726/27
*	I	US-2013/0331063 A1	12-2013	CORMIER; Jean-Philippe Paul	H04L63/0272	455/411
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2438

CPC								
Symbol							**Type**	**Version**
G06F		21	/	35			F	2013-01-01
G06F		21	/	32			I	2013-01-01
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					
			/					

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

/PHY ANH VU/ Examiner.Art Unit 2438	11/25/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/TAGHI ARANI/ Supervisory Patent Examiner.Art Unit 2438	11/27/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
713	186	H	0	4	L	63 / 0861						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											

/PHY ANH VU/ Examiner.Art Unit 2438 (Assistant Examiner)	11/25/2015 (Date)	**Total Claims Allowed:** 18	
/TAGHI ARANI/ Supervisory Patent Examiner.Art Unit 2438 (Primary Examiner)	11/27/2015 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 6

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2438

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1	15	17												
1	2	16	18												
2	3	17	19												
3	4	18	20												
4	5														
5	6														
6	7														
	8														
7	9														
8	10														
9	11														
10	12														
11	13														
12	14														
13	15														
14	16														

/PHY ANH VU/ Examiner.Art Unit 2438	11/25/2015	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/TAGHI ARANI/ Supervisory Patent Examiner.Art Unit 2438	11/27/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	2437
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	10001-4540 US

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
/P.V./	1	20040123127		2004-06-24	Teicher, et al.	
/P.V./	2	20070159301		2007-07-12	Hirt, et al.	
/P.V./	3	20070219926		2007-09-20	Korn, Stanley	
/P.V./	4	20070213048		2007-09-13	Trauberg, Markus	
/P.V./	5	20080008359		2008-01-10	Beenau, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-4540 US

/P.V./	6	20010026619		2001-05-30	Howard 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] 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]
/P.V./	1	Simon Liu and Mark Silverman. 2001. "A Practical Guide to Biometric Security Technology". IT Professional 3, 1 (January 2001). 27-32. DOI=10. 1109/6294.899930 http://dx.doi.org/10.1109/6294.899930	☐
/P.V./	2	Smart Card Alliance Report, "Contactless Technology for Secure Physical Access: Technology and Standards Choices", Smart Card Alliance, 10/2002, pg. 1-48.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Phy Anh Vu/	Date Considered	11/25/2015

*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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		device near4 ID or identification identifier) with third near4(party agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
L1	0	"14521982"	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:21
L2	0	"14521982"	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:21
L3	273	(biometric with authenticat$3) same (third with trust$4) near5 (agent or party)	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:33
L4	7	l3 and @ad<"20011220"	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:34
L5	676	g06f21/32.cpc. and (authenticat$3 same (third near5 (party or agent)))	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:37
L6	439	g06f21/32.cpc. and (authenticat$3 with (third near5 (party or agent)))	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:37
L7	196	g06f21/32.cpc. and (authenticat$3 with (third near5 (party or agent))) same (biometric)	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:37
L8	13	l7 and @ad<"20011220"	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:37
L9	134	h04l63/0861.cpc. and (authenticat$3 with (third near5 (party or agent))) same (biometric)	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:42
L10	4	l9 and @ad<"20011220"	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:42
L14	10	"34940790".FMID.	US-PGPUB; USPAT; FPRS	OR	OFF	2015/11/25 17:44
S1	549	(transmit$3 or send$3) with (ID or code identifier identification) with (agent employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:04
S2	33	(transmit$3 or send$3) with (ID or code identifier identification) with (third) with (agent employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:04
S3	560	(transmit$3 or send$3) with (ID or code identifier identification) with (third) with (party) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:13
S4	522	(transmit$3 or send$3) with (ID or code	US-	OR	OFF	2015/05/31

		identifier identification) with (third near4 party) with authenticat$3	PGPUB; USPAT			21:14
S5	549	(transmit$3 or send$3) with (ID or code identifier identification) with (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:14
S6	14	(transmit$3 or send$3) with (ID or code identifier identification) with third near5 (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:15
S7	1	(transmit$3 or send$3) with (device near4 ID) with third near5 (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:16
S8	21	(transmit$3 or send$3) with (device near4 ID) with (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:17
S9	1315	(device near4 ID or identification identifier) with third near4(party agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
S10	43	(device near4 ID or identification identifier) with third near4 (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
S11	39	(device near4 ID or identification identifier) with third near4 (agent) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:33
S12	4	transmit$4 with (ID or code or identifier identification) with (attendant or guard) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:25
S13	1	"20050074126".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:34
S14	1	"20040128162".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:46
S15	1	"6041410".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 10:01
S16	1	"13710109"	US-PGPUB; USPAT	OR	OFF	2015/06/01 10:32
S17	1140	("4759060" "4993068" "5187352" "5296641" "5416780" "5422632" "5450489")	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:38
S18	7	("4759060" "4993068" "5187352" "5296641" "5416780" "5422632" "5450489").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:38
S19	11	("5619251" "5629980" "5644354" "5666412" "5784464" "5825876" "5857020" "5892825" "5894551" "5894551" "5898880" "5917913").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:43
S20	10	("5928327" "5991399" "5991749" "6016476" "6018739" "6035329" "6038334" "6041410" "6042006" "6055314").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:45
S21	34	g06f21/32.cpc. and (authenticat$3 with biometric with fob)	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:51
S22	15	h04l63/0861.cpc. and (authenticat$3 with biometric with fob)	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:59

S23	76	(john near5 giobbi).in.	US-PGPUB; USPAT	OR	OFF	2015/06/01 13:00
S24	47	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT	OR	OFF	2015/06/01 13:00

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L11	253	g06f21/32.cpc. and (authenticat$3 same (third near5 (party or agent)))	USPAT	OR	OFF	2015/11/25 17:43
L12	79	g06f21/32.cpc. and (authenticat$3 same (third near5 (party or agent))) with biometric	USPAT	OR	OFF	2015/11/25 17:43
L13	57	g06f21/32.cpc. and (authenticat$3 with (third near5 (party or agent))) with biometric	USPAT	OR	OFF	2015/11/25 17:43
L15	35	(authenticat$3 with (third near5 (party or agent))) with biometric.clm.	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:45
L16	51	(authenticat$3 with (third near5 (party or agent))) with (ID).clm.	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:46
L17	7	(authenticat$3 with (third near5 (party or agent))) with (device near10 ID).clm.	US-PGPUB; USPAT	OR	OFF	2015/11/25 17:48
L18	145	h04l63/0861.cpc. and (authenticat$3 same (third near5 (party or agent)))	USPAT	OR	OFF	2015/11/25 17:50
L19	26	h04l63/0861.cpc. and (authenticat$3 same (third near5 (party or agent))).clm.	USPAT	OR	OFF	2015/11/25 17:50

11/25/2015 5:51:32 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14521982.wsp

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	2438
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	10001-04540 US

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
/P.V./	1	20020091646		2002-07-11	Lake et al.	
/P.V./	2	20020116615		2002-08-22	Nguyen et al	
/P.V./	3	20050054431		2005-03-10	Walker et al.	
/P.V./	4	20060058102		2006-03-16	Nguyen et al	
/P.V./	5	20060063575		2006-03-23	Gatto et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-04540 US

/P.V./	6	20060076401		2006-04-13	Frerking	
/P.V./	7	20070032288		2007-02-08	Nelson et al.	
/P.V./	8	20070060319		2007-03-15	Block 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] 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		☐

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

EXAMINER SIGNATURE

Examiner Signature	/Phy Anh Vu/	Date Considered	11/25/2015

*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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
G06F 21/32	6/1/2015; 11/25/2015	PVU
H04L 63/0861	6/1/2015; 11/25/2015	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor name search for double patening issuest	6/1/2015	PVU
Keywords search	6/1/2015; 11/25/2015	PVU
Consulted with SPE regarding allowable subject matters	11/25/2015	PVU

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
G06F	21/32	11/25/2015	PVU
H04L	63/0861	11/25/2015	PVU

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/01/2015	11/25/2015							
	1	-	-							
1	2	✓	=							
2	3	✓	=							
3	4	✓	=							
4	5	✓	=							
5	6	✓	=							
6	7	✓	=							
	8	✓	-							
7	9	✓	=							
8	10	✓	=							
9	11	✓	=							
10	12	✓	=							
11	13	✓	=							
12	14	✓	=							
13	15	✓	=							
14	16	✓	=							
15	17	✓	=							
16	18	✓	=							
17	19		=							
18	20		=							

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14521982
Filing Date	23-Oct-2014
First Named Inventor	John Giobbi
Attorney Docket Number	10001-04540 US
Title of Invention	Biometric Personal Data Key (PDK) Authentication

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Proxense, LLC	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8352730

8886954

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request. ○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ◉ Small Entity ○ Micro Entity ○ Regular Undiscounted I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 65160 ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this request	
Signature	/Matthew Holmes/
Name	Matthew Holmes

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14521982
Filing Date:	23-Oct-2014
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Matthew M. Holmes
Attorney Docket Number:	10001-04540 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or Terminal Disclaimer	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14521982

Filing Date: 23-Oct-2014

Applicant/Patent under Reexamination: Giobbi et al.

Electronic Terminal Disclaimer filed on November 23, 2015

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	24163190
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	23-NOV-2015
Filing Date:	23-OCT-2014
Time Stamp:	18:45:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$160
RAM confirmation Number	6341
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33447 db55097ba0af815baf377ab7d00877f1bac7374f	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30366 53292d2de3991b656884e16978f7d4a8108ad5b2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	63813		

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

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	2438
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	10001-04540 US

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	20020091646		2002-07-11	Lake et al.	
	2	20020116615		2002-08-22	Nguyen et al	
	3	20050054431		2005-03-10	Walker et al.	
	4	20060058102		2006-03-16	Nguyen et al	
	5	20060063575		2006-03-23	Gatto et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-04540 US

	6	20060076401		2006-04-13	Frerking	
	7	20070032288		2007-02-08	Nelson et al.	
	8	20070060319		2007-03-15	Block 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							☐

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-04540 US

[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	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2438
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-04540 US

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	/Paige Alsbury/	Date (YYYY-MM-DD)	2015-11-02
Name/Print	Paige M. Alsbury	Registration Number	72,965

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:	23963059
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	02-NOV-2015
Filing Date:	23-OCT-2014
Time Stamp:	17:30:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	04540US20151102_IDS.pdf	612456 f0ca54e7b856d0c3b1c5189b58db851c0a126a4a	no	5

Warnings:
Information:

Total Files Size (in bytes):	612456

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

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

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

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

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2438
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: September 14, 2015 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT A

Responsive to the Non-Final Office Action mailed on June 12, 2015, which sets a shortened statutory period for response that expires on September 12, 2015, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (Currently Amended) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on[[the]] an integrated device;

responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for ~~authentication by an agent that is~~ comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

responsive to receiving an access message from the third-party trusted authority ~~agent~~ indicating that the third-party trusted authority ~~agent~~ successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to ~~perform an action~~ complete a financial transaction.

3. (Currently Amended) The method of claim[[1]] 2, further comprising:

registering an age verification for the user in association with the ID code.

4. (Currently Amended) The method of claim[[1]] 2, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (Currently Amended) The method of claim[[1]] 2, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Currently Amended) The method of claim[[1]] 2, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Currently Amended) The method of claim[[1]] 2, wherein the action includes accessing an application.

8. (Cancelled).

9. (Currently Amended) The method of claim[[1]] 2, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

10. (Currently Amended) The method of claim[[1]] 2, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (Currently Amended) An integrated device comprising:

a persistent storage media that persistently stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for ~~authentication by a third party that operates a trusted authority~~ comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to ~~perform an action~~ complete a financial transaction.

12. (Currently Amended) The integrated device of claim 11, wherein the ID code is transmitted to the third-party trusted authority over a network.

13. (Previously Presented) The integrated device of claim 11, wherein an age verification is registered in association with the device ID code.

14. (Previously Presented) The integrated device of claim 11, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (Currently Amended) A system, comprising:

an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the ~~device~~ ID code;[[and]]

an authentication circuit that receives ~~the one or more codes and other data values~~ the ID code and sends ~~the one or more codes and other data values~~ the ID code to a third-party ~~that operates a~~ trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to ~~perform an action~~ complete a financial transaction; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the ~~device~~ ID code received and ~~the list~~ the legitimate codes included in the list of the legitimate codes.

16. (Currently Amended) The system of claim 15, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (Previously Presented) The system of claim 15, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (Previously Presented) The system of claim 15, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

19. (New) The system of claim 15, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (New) The system of claim 15, wherein the action includes accessing an application.

REMARKS

Claims 2-18 were presented for examination.[1] Claims 2-18 stand rejected in the Office Action dated June 12, 2015 (herein, "OA"). Claims 19 and 20 are new. Claim 8 is cancelled. Claims 2-12, 15 and 16 are amended without acquiescing to the propriety of the rejection. Support for these amendments can be found in at least paragraphs [0027], [0031], [0032], [0035], [0041], [0043] and [0052] of the original disclosure. Claims 2-7 and 9-20 are pending upon entry of this amendment. No new matter is added.

Summary of Office Action

1. Claims 3-10, and 15 are objected to because of alleged informalities.

2. Claims 11 and 15 are rejected on the ground of non-statutory double patenting as allegedly being unpatentable over claims 12 and 22 of U.S. Patent No. 8,886,954.

3. Claims 2-10 are rejected under 35 U.S.C. § 101 for allegedly being directed to non-statutory subject matter.

4. Claims 2-10 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over Hsu et al. (U.S. Patent No. 6,041,410, hereinafter "Hsu") and in view of Stanko (U.S. Publication No. 2005/0074126, hereinafter "Stanko").

5. Claims 3 and 13 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over Hsu, Stanko and further in view of Schlotterbeck (U.S. Publication No. 2004/0128162, hereinafter "Schlotterbeck").

---

[1] Preliminary Amendment included claims 2-21; however, because claims 19-21 were on the same page as the remarks, claims 19-21 do not appear to have been entered or considered. Accordingly, claims 19 and 20, which correspond to claims 19 and 21, respectively, in the preliminary amendment, are identified as new herein. Claim 1 is amended to include elements similar to claim 20 of the previous filed Preliminary Amendment.

6. Claims 11-12, and 14-18 are rejected under pre-AIA 35 U.S.C. § 103(a) as allegedly being unpatentable over Hsu, Stanko and further in view of Lake et al. (U.S. Publication No. 2002/0091646, hereinafter "Lake").

Response to Objections for Claims

Claims 3-10 and 15 are objected to because of alleged informalities.

In particular, claims 3-10 recite the limitation "The method of claim 1" which should be "The method of claim 2." Claims 3-10 are amended to recite "The method of claim 2" as suggested by the Examiner. Accordingly, Applicants respectfully request that the objection of claims 3-10 be withdrawn.

Claim 15 recites "the one or more codes and other data values" which should be "the ID code." Claim 15 is amended to recite "the ID code" as suggested by the Examiner. Accordingly, Applicants respectfully request that the objection of claim 15 be withdrawn.

Response to Double Patenting Rejection

Claims 11 and 15 are rejected on the ground of non-statutory double patenting as being allegedly unpatentable over claims 12 and 22 of U.S. Patent No. 8,886,954. Applicant respectfully requests that the double patenting rejection be held in abeyance until it is determined that there is allowable subject matter, at which time Applicant will respond to the rejection or file a terminal disclaimer.

Response to Rejections under 35 U.S.C. § 101

Claims 2-10 are rejected under 35 U.S.C. § 101 for allegedly being directed to non-statutory subject matter.

Here, the OA asserts that the independent claim 2 is directed to "*an abstract idea of biometric personal data key authentication. The steps of storing biometric data, receiving a request for biometric data, comparing the scan data, sending the ID code, receiving an access message, and allowing user to perform an action are all mental processes, that describe the abstract idea*."

Applicants respectfully disagree and submit that at least the following elements of claim 2, when considered with the other elements of claim 2, are not directed to an abstract idea.

> *... persistently storing biometric data of a legitimate user and an ID code on an integrated device;*
> *responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;*
> *... responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and*
> *responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction.*

In particular, the element of "*responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction*" is not merely an "abstract idea of biometric personal data key authentication" but rather "*authenticat[ing] the user as the legitimate user*" in a certain concrete way, which is dependent upon several concrete computer-implemented acts being performed

including "*persistently storing biometric data of a legitimate user and an ID code on an integrated device*," "*responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor*" and "*responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority*."

Accordingly, Applicant respectfully requests that the rejection under 35 U.S.C. § 101 of claim 2, and all claims depending therefrom, be withdrawn.

Response to Rejections under 35 U.S.C. § 103

The rejection of the claims will be addressed by reference to the independent claims.

Independent claim 2

As amended, independent claim 2 recites in part:

> *... persistently storing biometric data of a legitimate user and an ID code on an integrated device;*
> *responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor*
> *... responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and*
> *responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction.*

The cited portions of the references, and the proposed combination thereof, fail to disclose or render obvious, among other things, "*responsive to receiving an access message from*

the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction" as recited by amended claim 2.

The Examiner, on page 9 of the OA, cites Hsu at Figure 4, col. 5 line 65 – col. 6 line 9, and col. 6 lines 24-34 as disclosing "*wherein the action includes accessing an application*" and "*wherein the action includes completing a transaction*." In particular, on page 9 of the OA, the Examiner argues:

> Regarding claim 7, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the action includes accessing an application *(figure 4, column 5, line 65-colum 6, line 9, access to an application of a financial institution)*.
>
> Regarding claim 8, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the action includes completing a transaction *(Figure 4, column 6, 24-34, ATM)*.

Respectfully, Applicants disagree. Figure 4, col. 5 line 65 – col. 6 line 9, and col. 6 lines 24-34 of Hsu disclose:

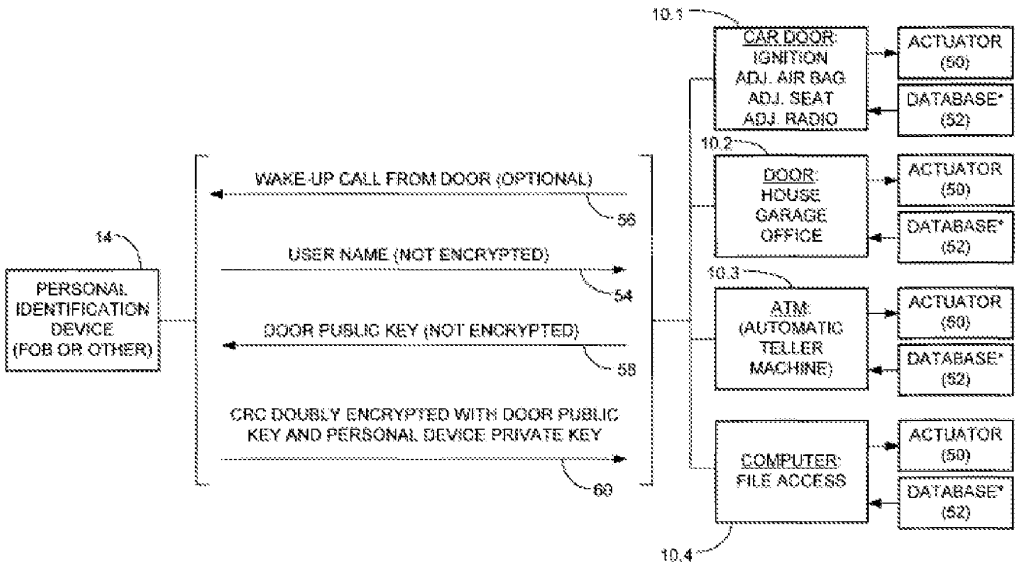


FIG. 4

CRC as derived from the user's reference fingerprint. If the door **10** provides access to a financial institution, for example, the user will register by bringing his or her fob **14** to the institution, and transmitting the fingerprint CRC from the fob to the door receiver **15**. In the registration mode, the door receiver **15** will store the user's CRC in association with the user's name or other identifying information. As part of the registration process, the user **12** will normally be required to present some form of identification other than the fob **14**, to prove to the institution that the user is, in fact, the one whose name or other identifying information is presented and will be stored in the door **10**.

FIG. **4** shows the communications that pass between the fob **14** or other personal identification device and a door **10**, four different forms of which are shown, including a car door **10.1**, a building door **10.2**, an automatic teller machine (ATM) **10.3**, and a computer **10.4**. Each door **10** has an actuator **50**, to perform some desired operation, such as opening the door, and each door also has a database **52** in which is stored the user name, the user fob public encryption key and the user CRC, for each user registered to use the door.

The cited portions of Hsu disclose at most that "[i]f the door 10 provides access to a financial institution … the user will register by bringing his or her fob 14 to the institution, and

transmitting the fingerprint CRC from the fob to the door receiver 15" at col. 5 line 65 – col. 6 line 2. "[O]pen[ing]" "the door for the user"[2] in which "the door 10 provides access to a financial institution" as disclosed by Hsu is not similar to "allowing the user to complete a transaction" much less "allowing the user to *complete a financial transaction*" as recited by amended claim 2.

The cited portions of Hsu also disclose at most that "[i]f there is a match, the door is opened for the user" and "a door 10, four different forms of which are shown, including a car door 10.1, a building door 10.2, an automatic teller machine (ATM) 10.3, and a computer 10.4." *See* Hsu, col. 6 lines 23-24 and lines 26-29. "[O]pen[ing]" "a door … different forms of which … including … an automatic teller machine (ATM)" "for the user" as disclosed by Hsu does not disclose "a financial transaction" much less "allowing the user to *complete a financial transaction*" as recited by amended claim 2. Accordingly, the cited portions of Hsu do not teach, disclose or suggest "*responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction*" as recited by amended claim 2.

The deficiencies of the cited portions of Hsu are not remedied by the cited portions of Stanko, Schlotterbeck and Lake. The cited portions of Stanko, Schlotterbeck and Lake do not teach, disclose or suggest, among other things, "*responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction,*" as recited by amended claim 2, nor does the

[2] Hsu, col. 6 lines 23-24.

Examiner contend that they do. Thus, Applicants respectfully submit that the proposed combinations of the cited portions of Hsu, Stanko, Schlotterbeck and Lake fail to disclose or render obvious each and every element of amended claim 2.

Claims 3-7, 9 and 10 depend from claim 2 and are therefore patentable for at least similar reasons as amended claim 2 as well as because of the additional features they recite.

Independent claim 11

As amended, independent claim 11 recites in part:

> "*... a persistent storage media that persistently stores biometric data of a user and an ID code;*
> *a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and*
> *a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to complete a financial transaction*."

Accordingly, the cited portions of Hsu, Stanko, Schlotterbeck and Lake in the proposed combinations set forth in the OA fail to disclose or render obvious each and every limitation of amended claim 11, and amended claim 11 is therefore patentable over the cited portions of the references for at least reasons analogous to those discussed above with reference to claim 2.

Claims 12-14 depend from claim 11 and are therefore patentable for at least similar reasons as amended claim 11 as well as because of the additional features they recite.

Independent claim 15

As amended, independent claim 15 recites in part:

"*...an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and responsive to scan data matches the stored biometric data, wirelessly sends the ID code;*

an authentication circuit that receives the ID code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

Accordingly, the cited portions of Hsu, Stanko, Schlotterbeck and Lake in the proposed combinations set forth in the OA fail to disclose or render obvious each and every limitation of amended claim 15, and amended claim 15 is therefore patentable over the cited portions of the references for at least reasons analogous to those discussed above with reference to claim 2.

Claims 16-20 depend from claim 15 and are therefore patentable for at least similar reasons as amended claim 15 as well as because of the additional features they recite.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: September 14, 2015 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

MMH:kkt

Electronic Acknowledgement Receipt	
EFS ID:	23480533
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	14-SEP-2015
Filing Date:	23-OCT-2014
Time Stamp:	18:37:25
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		04540US_AmendmentA.pdf	212665 bb6d7392009e7f5d7a0b202b83f6f1d6f555daff	yes	16

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	16
Warnings:			
Information:			
	Total Files Size (in bytes):	212665	

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/521,982	Filing Date 10/23/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	09/14/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PAMELA YOUNG/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US	8239

89194 7590 06/12/2015

Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
06/12/2015	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):

docketing@patentlawworks.net
patents@patentlawworks.net
mfurubayashi@patentlawworks.net

Office Action Summary	Application No. 14/521,982	Applicant(s) GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/12/2014*.

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

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *2-18* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *2-18* is/are rejected.

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

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

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

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *10/23/2014* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *02/12/2015*.

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

4) ☐ Other: _____.

DETAILED ACTION

The present application having Application No. 14/521,982 filed on 12/12/2014, is being presented for examination by the examiner.

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

Claim Objections

Claims 3-10 are objected to because of the following informalities:

Claim 3 recites "The method of claim 1…" which should be "The method of claim ~~1~~ **2**…"

Claims 4-10 are objected for the same rationale as claim 3 above.

an authentication circuit that receives the one or more codes and other data values and

Claim 15 recites "…an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values…" which should be "…..an authentication circuit that receives the **ID code** ~~**one or more codes and other data values**~~ and sends the **ID code** ~~**the one or more codes and other data values**~~…" Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent

and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 11 and 15 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 12 and 22 of U.S. Patent No. 8,886,954. Although the claims at issue are not identical, they are not patentably distinct from each other because the scopes of the claims are the same.

Application 14/521,982	Patent 8,886,954
Claims 11: An integrated device comprising: a persistent storage media that stores biometric data of a user and an ID code; a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for authentication by a third party that operates a trusted authority; and a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code sent to the third party and allowing the user to perform an action.	Claim 12: An integrated device comprising: **a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code** uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage media and not capable of being subsequently altered; a validation module, coupled to communicate with the persistent storage media, **that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority,** wherein the one or more codes and other data values includes the device ID code; and a radio frequency communication module that **receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.**

Claim 15: A system, comprising: an integrated hardware device that stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the device ID code; and an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code and allows the user to perform an action; and the trusted authority operated by a third party, the trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the device ID received and the list.	Claim 22: A system, comprising: **an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code** uniquely identifying the integrated hardware device and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered, **and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values,** wherein the one or more codes and other data values include the device ID code; and an authentication circuit that **receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.**

Claim Rejections - 35 USC § 101

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

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

Claims 2-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 2 is rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e: a law of nature, a natural phenomenon, or an abstract idea) without significant more. Claim 2 is an abstract idea of biometric personal data key authentication. The steps of storing biometric data, receiving a request for biometric data, comparing the scan data, sending the ID code, receiving an access message, and allowing user to perform an action are all mental processes, that describe the abstract idea.

The claim does not include additional elements that are sufficient to amount to significantly more than the judicial exception. Based upon consideration of all of the relevant factors with respect to the claim as a whole, the claim simply instructs the practitioner to implement the abstract idea with routine conventional activity.

Claims 3-10 depend on claim 2, thus inherit the same 101 rejection as their independent claim 2 above.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-10 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US Patent 6,041,410 B1-hereinafter Hsu) and in view of Stanko (US 2005/0074126 A1-hereinafter Stanko).

Regarding claim 2, Hsu discloses a method comprising:

persistently storing biometric data of a legitimate user and an ID code on the integrated device *(Figure 3, element 32; column 4, lines 15-25; column 7, lines 6-9, and 63-65, user's name, account number, fob's public and private key pair are stored in fob)*;

responsive to receiving a request for a biometric verification of a user, receiving scan data from a biometric scan *(column 4, lines 40-45, column 6, lines 29-41; column 7, lines 17-34, fingerprint from sensor is received)*;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data*(column 4, lines 40-45, received fingerprint is compared to a reference fingerprint image)* ;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for authentication by an agent that is a third-party trusted authority *(Figure 4, step 60; column 7, lines 20-30, account number and fob's key information are transmitted)*; and

successfully authenticated the user as the legitimate user based on the ID code, allowing the user to perform an action *(column 6, lines 16-24, column 7, lines 25-34, user's account number and key are successfully authenticated)*.

Hsu does not explicitly disclose receiving an access message from the agent indicating that the agent successfully authenticated the user.

However, Stanko discloses receiving a grant message after successful authentication *([0055][0069], grant message is sent)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Stanko into the method of Hsu to provide a clear and effective method of communication.

Regarding claim 4, Hsu and Stanko disclose the method of claim 2. Hsu further discloses an indication that the biometric verification was successful is sent with the ID code *(Figure 4, step 60; column 7, lines 20-30, at least account number, fob's key information and CRC are transmitted)*.

Regarding claim 5, Hsu and Stanko disclose the method of claim 2. Hsu further discloses wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition *(column 4, lines 31-39, print patter, iris patter)*;

Regarding claim 6, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob *(column 2, lines 15-29 and 27-40, fob)*.

Regarding claim 7, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the action includes accessing an application *(figure 4, column 5, line 65-colum 6, line 9, access to an application of a financial institution)*.

Regarding claim 8, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the action includes completing a transaction *(Figure 4, column 6, 24-34, ATM)*.

Regarding claim 9, Hsu and Stanko disclose the method of claim 1. Hsu further discloses wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account *(figure 4, column 5, line 65-column 6, lines 9, 24-34, car door, building door, ATM)*.

Regarding claim 10, Hsu and Stanko disclose the method of claim 1. Hsu further discloses responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification *(column 5, lines 60-65; column 6, lines 9-23, for subsequent use of fob, only user's account number and CRC are required)*; and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data *(column 6, lines 9-23, user's account number an CRC are transmitted)*.

Claims 3 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hsu, Stanko and further in view of Schlotterbeck et al. (US 2004/0128162 A1-hereinafter Schlotterbeck).

Regarding claim 3, Hsu and Stanko disclose the method of claim 2.

Hsu and Stanko do not disclose registering age verification for the user in association with the ID code.

However, Schlotterbeck discloses registering an age verification for a user in association with a patient ID card *([0057], age of patient).*

One of ordinary skill in the art the time the invention was made would have been motivated to incorporate the feature discloses by Schlotterbeck into the method Hsu and Stanko to include a wider selection of identifying information into the method.

Claim 13 is rejected for the same rationale as claim 3 above.

Claims 11-12 and 14-18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hsu, Stanko and further in view of Lake et al. (US 2002/0091646 A1-hereinafter Lake).

Regarding claim 11, Hsu discloses an integrated device comprising:

a persistent storage media that stores biometric data of a user and an ID code *(Figure 3, element 32; column 4, lines 15-25; column 7, lines 6-9, and 63-65, fob stores user's name, account number, and fob's public and private key pair)*;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data *(column 4, lines 40-45, column 6, lines 29-41; column 7, lines 17-34, fingerprint from sensor is received, received fingerprint is compared to a reference fingerprint image)*, and that sends the ID code for authentication by a trusted authority *(Figure 4, step 60; column 7, lines 20-30, account number and fob's key information are transmitted to the door)*; and

the trusted authority indicating that the trusted authority successfully authenticated the ID code sent to the third party and allowing the user to perform an action *(column 6, lines 16-24, column 7, lines 25-34, door is open after user's account number and key are successfully authenticated)*.

Hsu does not explicitly disclose authentication is done by a third party that operates the trusted authority and receiving an access message from the trusted authority indicating that the trusted authority successfully authenticated the user.

However, Lake discloses a concept of having a third party that works for a trusted server to authenticate users *([0006][0011], identity verification agent)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Lake into the method of Hsu to add another layer of protection to ensure users are who they claim to be.

Hsu and Lake do not disclose receiving an access message from the trusted authority indicating that the trusted authority successfully authenticated the user.

However, Stanko discloses receiving a grant message after successful authentication *([0055][0069], grant message is sent)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Stanko into the method of Hsu and Lake to provide a clear and effective method of communication.

Regarding claim 12, Hsu, Lake and Stank disclose the integrated device of claim 11. Hsu further discloses wherein the ID code is transmitted to the trusted authority over a network *(figure 4, column 7, lines 24-34, account number and key information are transmitted)*.

Claim 14 is rejected for the same rationale as claim 6 above.

Regarding claim 15, Hsu discloses a system, comprising:

an integrated hardware device that stores biometric data of a legitimate user and an ID code in the integrated hardware device *(Figure 3, element 32; column 4, lines 15-25; column 7, lines 6-9, and 63-65, fob stores user's name, account number, and fob's public and private key pair)*, and that wirelessly sends the device ID code *(Figure 4, step 60; column 7, lines 20-30, account number and fob's key information are transmitted to the door)*; and

an authentication circuit that receives the one or more codes and other data values *(column 4, lines 40-45, column 6, lines 29-41; column 7, lines 17-34, fingerprint*

from sensor is received, received fingerprint is compared to a reference fingerprint image) and sends the one or more codes and other data values to a trusted authority for authentication *(Figure 4, step 60; column 7, lines 20-30, account number and fob's key information are transmitted to the door)*, and allows the user to perform an action*(column 6, lines 16-24, column 7, lines 25-34, door is open after user's account number and key are successfully authenticated)*; and

the trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the device ID received and the list *(column 6, lines 2-9, and 16-34 user's registration information such as CRC and use's account number are stored, and the registration information will be used for authentication).*

Hsu does not disclose the trusted authority operated by a third party, and receiving an access message from the trusted authority indicating that the trusted authority successfully authenticated the user.

However, Lake discloses a concept of having a third party that works for a trusted server to authenticate users *([0006][0011], identity verification agent)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Lake into the method of Hsu to add another layer of protection to ensure users are who they claim to be.

Hsu and Lake do not disclose receiving an access message from the trusted authority indicating that the trusted authority successfully authenticated the user.

However, Stanko discloses receiving a grant message after successful authentication *([0055][0069], grant message is sent)*.

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature discloses by Stanko into the method of Hsu and Lake to provide a clear and effective method of communication.

Regarding claim 16, Hsu, Lake and Stanko discloses the system of claim 15. Hsu further discloses wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify scan data as being from the legitimate user, the integrated hardware device does not send the ID code *(column 5, lines 42-47, if the biometric comparison result in a no match, then no further processing is performed).*

Claim 17 is rejected for the same rationale as claims 6 and 14 above.

Claim 18 is rejected for the same rationale as claim 5 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHY ANH VU whose telephone number is (571)270-7317. The examiner can normally be reached on Wed 7:00-5:30, TH-F 7-5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PHY ANH VU/
Examiner, Art Unit 2438
/TAGHI ARANI/
Supervisory Patent Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/521,982	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0091646	07-2002	Lake et al.	705/67
*	B	US-2005/0074126	04-2005	Stanko, Joseph A.	380/279
*	C	US-6,041,410	03-2000	Hsu et al.	713/186
*	D	US-2004/0128162	07-2004	Schlotterbeck et al.	705/002
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	~~2437~~ 2438
Examiner Name	~~Not Yet Known~~ Phy Anh Vu
Attorney Docket Number	10001-04540 US

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	4759060		1988-07-19	Hayashi et al.	
	2	4993068		1991-02-12	Piosenka et al.	
	3	5187352		1993-02-16	Blair et al.	
	4	5296641		1994-03-22	Stelzl	
	5	5392433		1995-06-06	Hammersley et al.	
	6	5416780		1995-05-16	Patel	
	7	5422632		1995-06-06	Bucholtz et al.	
	8	5450489		1995-09-12	Ostrover et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	9	5619251		1997-04-08	Kuroiwa et al.	
	10	5629980		1997-05-13	Stefik et al.	
	11	5644354		1997-07-01	Thompson et al.	
	12	5666412		1997-09-09	Handelman et al.	
	13	5784464		1998-07-21	Akiyama et al.	
	14	5825876		1998-10-20	Peterson, Jr.	
	15	5857020		1999-01-05	Peterson, Jr.	
	16	5892825		1999-04-06	Mages et al.	
	17	5894551		1999-04-13	Huggins et al.	
	18	5898880		1999-04-27	Ryu	
	19	5917913		1999-06-29	Wang	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	20	5928327		1999-07-27	Wang et al.	
	21	5991399		1999-11-23	Graunke et al.	
	22	5991749		1999-11-23	Morril, Jr.	
	23	6016476		2000-01-18	Maes et al.	
	24	6018739		2000-01-25	McCoy et al.	
	25	6035038		2000-03-07	Campinos et al.	
	26	6035329		2000-03-07	Mages et al.	
	27	6038334		2000-03-14	Hamid	
	28	6041410		2000-03-21	Hsu et al.	
	29	6042006		2000-03-28	Van Tilburg et al.	
	30	6055314		2000-04-25	Spies et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	31	6070796		2000-06-06	Sirbu	
	32	6088730		2000-07-11	Kato et al.	
	33	6104334		2000-08-15	Allport	
	34	6121544		2000-09-19	Petsinger	
	35	6148142		2000-11-14	Anderson	
	36	6161179		2000-12-12	Seidel	
	37	6185316		2001-02-06	Buffam	
	38	6209089		2000-03-27	Selitrennikoff et al.	
	39	6219109		2001-04-17	Raynesford et al.	
	40	6219439		2001-04-17	Burger	
	41	6247130		2001-06-12	Fritsch	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	42	6256737		2001-07-03	Bianco et al.	
	43	6266415		2001-07-24	Campinos et al.	
	44	6295057		2001-09-25	Rosin et al.	
	45	6336121		2002-01-01	Lyson et al.	
	46	6336142		2002-01-01	Kato et al.	
	47	6363485		2002-03-26	Adams et al.	
	48	6367019		2002-04-02	Ansell et al.	
	49	6381747		2002-04-30	Wonfor et al.	
	50	6385596		2002-05-07	Wiser et al.	
	51	6392664		2002-05-21	White et al.	
	52	6397387		2002-05-28	Rosin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	53	6401059		2002-06-04	Shen et al.	
	54	6411307		2002-06-25	Rosin et al.	
	55	6424715		2002-07-23	Saito	
	56	6425084		2002-07-23	Rallis et al.	
	57	6434535		2002-08-13	Kupka et al.	
	58	6446130		2002-09-03	Grapes	
	59	6463534		2002-10-08	Geiger et al.	
	60	6480188		2002-11-12	Horsley	
	61	6490443		2002-12-03	Freeny, Jr.	
	62	6510350		2003-01-21	Steen III et al.	
	63	6523113		2003-02-18	Wehrenberg	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	64	6529949		2003-03-04	Getsin et al.	
	65	6546418		2003-04-08	Schena et al.	
	66	6550011		2003-04-15	Sims III	
	67	6563805		2003-05-13	Ma et al.	
	68	6564380		2003-05-13	Murphy	
	69	6628302		2003-09-30	White et al.	
	70	6632992		2003-10-14	Hasegawa	
	71	6647417		2003-11-11	Hunter et al.	
	72	6667684		2003-12-23	Waggamon et al.	
	73	6683954		2004-01-27	Searle	
	74	6697944		2004-02-24	Jones et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	75	6709333		2004-03-23	Bradford et al.	
	76	6711464		2004-03-23	Yap et al.	
	77	6775655		2004-08-10	Peinado et al.	
	78	6804825		2004-10-12	White et al.	
	79	6806887		2004-10-19	Chernock et al.	
	80	6850147		2005-02-01	Prokoski et al.	
	81	6873975		2005-03-29	Hatakeyama et al.	
	82	6950941		2005-09-27	Lee et al.	
	83	6963971		2005-11-08	Bush et al.	
	84	6973576		2005-12-06	Giobbi	
	85	6975202		2005-12-13	Rodriguez et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	86	6983882		2006-01-10	Cassone	
	87	7012503		2006-03-14	Nielsen	
	88	7090126		2006-08-15	Kelly et al.	
	89	7112138		2006-09-26	Hedrick et al.	
	90	7137012		2006-11-14	Kamibayshi et al.	
	91	7191466		2007-03-13	Hamid et al.	
	92	7218944		2007-05-15	Cromer et al.	
	93	7249177		2007-07-24	Miller	
	94	7305560		2007-12-04	Giobbi	
	95	7529944		2009-05-05	Hamid	
	96	7574734		2009-08-11	Fedronic et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	97	7587611		2009-09-08	Johnson et al.	
	98	7617523		2009-11-10	Das et al.	
	99	7644443		2010-01-05	Matsuyama et al.	
	100	7715593		2010-05-11	Adams et al.	
	101	7883417		2011-02-08	Bruzzese et al.	
	102	7904718		2011-03-08	Giobbi 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	20010044337		2001-11-22	Rowe et al.	
	2	20020007456		2002-01-17	Peinado et al.	
	3	20020013772		2002-01-31	Peinado	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	4	20020014954		2002-02-07	Fitzgibbon et al.	
	5	20020015494		2002-02-07	Nagai et al.	
	6	20020023032		2002-02-21	Pearson et al.	
	7	20020026424		2002-02-28	Akashi	
	8	20020071559		2002-06-13	Christensen et al.	
	9	20020073042		2002-06-13	Maritzen et al.	
	10	20020098888		2002-07-25	Rowe et al.	
	11	20020103027		2002-08-01	Rowe et al.	
	12	20020104006		2002-08-01	Boate et al.	
	13	20020108049		2002-08-08	Xu et al.	
	14	20020109580		2002-08-15	Shreve et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	15	20020129262		2002-09-12	Kutaragi et al.	
	16	20020138767		2002-09-26	Hamid et al.	
	17	20020140542		2002-10-03	Prokoski et al.	
	18	20020144117		2002-10-03	Faigle	
	19	20020150282		2002-10-17	Kinsella	
	20	20020152391		2002-10-17	Willins et al.	
	21	20020158750		2002-10-31	Almalik	
	22	20020174348		2002-11-21	Ting	
	23	20020178063		2002-11-28	Gravelle et al.	
	24	20020191816		2002-12-19	Maritzen et al.	
	25	20030036425		2003-02-20	Kaminkow et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	26	20030046552		2003-03-06	Hamid	
	27	20030054868		2003-03-20	Paulsen et al.	
	28	20030054881		2003-03-20	Hedrick et al.	
	29	20030055689		2003-03-20	Block et al.	
	30	20030079133		2003-03-24	Breiter et al.	
	31	20030115474		2003-06-19	Khan et al.	
	32	20030127511		2003-07-10	Kelly et al.	
	33	20030139190		2003-07-24	Steelberg et al.	
	34	20030149744		2003-08-07	Bierre et al.	
	35	20030172037		2003-09-11	Jung et al.	
	36	20030176218		2003-09-18	LeMay et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	37	20030186739		2003-10-02	Paulsen et al.	
	38	20040127277		2004-07-01	Walker et al.	
	39	20040128162		2004-07-01	Schlotterbeck et al.	
	40	20040129787		2004-07-08	Saito et al.	
	41	20040209690		2004-10-21	Bruzzese et al.	
	42	20040209692		2004-10-21	Schober et al.	
	43	20040215615		2004-10-28	Larsson et al.	
	44	20040230488		2004-11-18	Beenau et al.	
	45	20050074126		2005-04-07	Stanko	
	46	20050081040		2005-04-14	Johnson et al.	
	47	20050109836		2005-05-26	Ben-Aissa	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	48	20050229007		2005-10-13	Bolle et al.	
	49	20050251688		2005-11-10	Nanavati et al.	
	50	20050253683		2005-11-17	Lowe	
	51	20060022046		2006-02-02	Iwamura	
	52	20060113381		2006-06-01	Hochstein et al.	
	53	20060156027		2006-07-13	Blake	
	54	20070220272		2007-09-20	Campisi et al.	
	55	20080019578		2008-01-24	Saito et al.	
	56	20080188308		2008-08-07	Shepherd et al.	
	57	20090328182		2009-12-31	Malakapalli et al.	
	58	20100117794		2010-05-13	Adams et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	59	20110126188		2011-05-26	Bernstein 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	WO 00/62505	WO		2000-10-19	Thomson Multimedia		☐
	2	WO 01/22724	WO		2001-03-29	Thomson Multimedia		☐
	3	WO 01/75876	WO		2001-10-11	Thomson Multimedia		☐
	4	WO 01/77790	WO		2001-10-18	Thomson Multimedia		☐
	5	WO 05/050450	WO		2005-06-02	Margent Development, LLC		☐
	6	WO 05/086802	WO		2005-09-22	Margent Development, LLC		☐

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, Retrieved on January 7, 2007 from <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pgs.	☐
	2	Amr Farouk, Ahmed A. Abdelhafez, "Authentication Mechanisms in Grid Computing Environment: Comparative Study," IEEE, 2012, pgs. 1-6.	☐
	3	ANTONOFF, Michael, "Visiting Video Valley," Sound & Vision, November 2001, pgs 116, 118-119.	☐
	4	"Applying Biometrics to Door Access," Security Magazine, September 26, 2002, Retrieved on January 7, 2007, from <URL:http://www.securitymagazine.com/CDA/Articles/technologies/3ae610eaa34d8010VgnVCM100000f932a8c0____>, 5 pgs.	☐
	5	BioPay, LLC, "Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, Retrieved on January 7, 2007, from <URL:http://www.biopay.com/faqs-lowes.asp>, 5 pgs.	☐
	6	BLUM, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, October 2000, pgs. 24-27.	☐
	7	DEBOW, Yvette, "Credit/Debit Debuts in Midwest Smart Card Test," Computers in Banking, v6, n11, November 1989, 4 pgs.	☐
	8	DENNIS, Sylvia, "Digital Passports Need Not Infringe Civil Liberties," Newsbytes, December 2, 1999, 2 pgs.	☐
	9	FASCA, Chad, "The Circuit," Electronic News, Vol. 45 Iss. 45, November 8, 1999, 2 pgs.	☐
	10	"Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet," Computergram International, January 18, 1996, 2 pgs.	☐
	11	KONTZER, Tony, "Thomson Bets on Smart Cards For Video Encryption," www.informationweek.com, June 7, 2001, 1 pg	☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	12	LAKE, Matt, "Downloading for Dollars," Sound & Vision, November 2000, pgs. 137-138.	☐
	13	LEWIS, Peter H., "Sony and Visa in On-Line Entertainment Venture," New York Times, v145, November 16, 1995, 1 pg.	☐
	14	MCIVER, R. et al., "Identification and Verification Working Together," Bioscrypt, August 27, 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>, 5 pgs.	☐
	15	"Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, January 8, 2002, 3 pgs.	☐
	16	NILSSON, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, April 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>, 5 pgs.	☐
	17	NORDIN, B., "Match-On-Card Technology," Precise Biometrics, White Paper, April 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf>, 7 pgs.	☐
	18	PAGET, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, December 1999, 4 pgs.	☐
	19	PCT International Search Report, PCT/US04/38124, April 7, 2005, 10 pgs.	☐
	20	PCT International Search Report, PCT/US05/43447, February 22, 2007, 7 pgs.	☐
	21	PCT International Search Report, PCT/US05/46843, March 1, 2007, 10 pgs.	☐
	22	PCT International Search Report, PCT/US07/11102, October 3, 2008, 11 pgs.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	23	PCT International Search Report, PCT/US07/11103, April 23, 2008, 9 pgs.	☐
	24	PCT International Search Report, PCT/US07/11104, June 26, 2008, 9 pgs.	☐
	25	PCT International Search Report, PCT/US07/11105, October 20, 2008, 10 pgs.	☐
	26	POPE, "Oasis Digital Signature Services: Digital Signing without the Headaches," Internet Computing-IEEE, Vol. 10, October 2006, pgs. 81-84.	☐
	27	"SAFModuleTM: A Look Into Strong Authentication," saflink Corporation, Retrieved on January 7, 2007, from <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pgs.	☐
	28	SAPSFORD, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, August 14, 2000, 2 pgs.	☐
	29	"Say Hello to Bluetooth," Bluetooth Web site, June 2000, 4 pgs.	☐
	30	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, Retrieved on January 7, 2007, from <URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>, 7 pgs.	☐
	31	"Thomson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001, 2 pgs.	☐
	32	VAN WINKLE, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, January 2000, pgs. 148-153..	☐
	33	WADE, Will, "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, April 21, 2003, Retrieved on January 7, 2007, from <URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>, 3 pgs.	☐

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	34	WALLACE, Bob, "The Internet Unplugged," InformationWeek.com, December 13, 1999, pgs. 22-24.	☐
	35	WEBER, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, July 24, 2000, 3 pgs.	☐
	36	"What is a File?," April 30, 1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed March 11, 2010 via http://waybackmachine.org/1998061500000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html, 1 pg.	☐
	37	YOSHIDA, Junko, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002, 2 pgs.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/Phy Anh Vu/	Date Considered	06/01/2015

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.V./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		device near4 ID or identification identifier) with third near4(party agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
L1	1140	("4759060" "4993068" "5187352" "5296641" "5416780" "5422632" "5450489")	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:38
L2	7	("4759060" "4993068" "5187352" "5296641" "5416780" "5422632" "5450489").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:38
L3	11	("5619251" "5629980" "5644354" "5666412" "5784464" "5825876" "5857020" "5892825" "5894551" "5894551" "5898880" "5917913").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:43
L4	10	("5928327" "5991399" "5991749" "6016476" "6018739" "6035329" "6038334" "6041410" "6042006" "6055314").pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:45
L5	34	g06f21/32.cpc. and (authenticat$3 with biometric with fob)	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:51
L6	15	h04l63/0861.cpc. and (authenticat$3 with biometric with fob)	US-PGPUB; USPAT	OR	OFF	2015/06/01 12:59
L7	76	(john near5 giobbi).in.	US-PGPUB; USPAT	OR	OFF	2015/06/01 13:00
L8	47	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT	OR	OFF	2015/06/01 13:00
S1	549	(transmit$3 or send$3) with (ID or code identifier identification) with (agent employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:04
S2	33	(transmit$3 or send$3) with (ID or code identifier identification) with (third) with (agent employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:04
S3	560	(transmit$3 or send$3) with (ID or code identifier identification) with (third) with (party) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:13
S4	522	(transmit$3 or send$3) with (ID or code identifier identification) with (third near4 party) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:14
S5	549	(transmit$3 or send$3) with (ID or code identifier identification) with (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:14
S6	14	(transmit$3 or send$3) with (ID or code identifier identification) with third near5 (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:15
S7	1	(transmit$3 or send$3) with (device near4 ID)	US-	OR	OFF	2015/05/31

		with third near5 (agent or employee) with authenticat$3	PGPUB; USPAT			21:16
S8	21	(transmit$3 or send$3) with (device near4 ID) with (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:17
S9	1315	(device near4 ID or identification identifier) with third near4(party agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
S10	43	(device near4 ID or identification identifier) with third near4 (agent or employee) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:30
S11	39	(device near4 ID or identification identifier) with third near4 (agent) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/05/31 21:33
S12	4	transmit$4 with (ID or code or identifier identification) with (attendant or guard) with authenticat$3	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:25
S13	1	"20050074126".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:34
S14	1	"20040128162".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 09:46
S15	1	"6041410".pn.	US-PGPUB; USPAT	OR	OFF	2015/06/01 10:01
S16	1	"13710109"	US-PGPUB; USPAT	OR	OFF	2015/06/01 10:32

EAST Search History (Interference)

<This search history is empty>

6/1/2015 1:03:03 PM
C:\Users\pvu3\Documents\EAST\Workspaces\14521982.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/01/2015								
	1	-								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 8239

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/521,982	10/23/2014 RULE	713	2438	10001-04540 US

APPLICANTS
Proxense, LLC, Bend, OR

INVENTORS
John J. Giobbi, Bend, OR;

**** CONTINUING DATA ***************************
This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005
and claims benefit of 60/637,538 12/20/2004

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
10/31/2014

Foreign Priority claimed	☐ Yes ☑ No	☐ Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	☐ Yes ☑ No					
Verified and Acknowledged	/PHY ANH TRAN VU/ Examiner's Signature	Initials	OR	6	20	3

ADDRESS
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111
UNITED STATES

TITLE
Biometric Personal Data Key (PDK) Authentication

FILING FEE RECEIVED		
800	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14521982	GIOBBI, JOHN J.
	Examiner	Art Unit
	PHY ANH VU	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
G06F 21/32	6/1/2015	PVU
H04L 63/0861	6/1/2015	PVU

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor name search for double patening issues	6/1/2015	PVU
Keywords search	6/1/2015	PVU

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

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	2437
Examiner Name	Phy Anh Tran Vu
Attorney Docket Number	10001-4540 US

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	20040123127		2004-06-24	Teicher, et al.	
	2	20070159301		2007-07-12	Hirt, et al.	
	3	20070219926		2007-09-20	Korn, Stanley	
	4	20070213048		2007-09-13	Trauberg, Markus	
	5	20080008359		2008-01-10	Beenau, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-4540 US

	6	20010026619		2001-05-30	Howard 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] 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	Simon Liu and Mark Silverman. 2001. "A Practical Guide to Biometric Security Technology". IT Professional 3, 1 (January 2001). 27-32. DOI=10. 1109/6294.899930 http://dx.doi.org/10.1109/6294.899930	☐
	2	Smart Card Alliance Report, "Contactless Technology for Secure Physical Access: Technology and Standards Choices", Smart Card Alliance, 10/2002, pg. 1-48.	☐

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	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-4540 US

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	/Paige Alsbury/	Date (YYYY-MM-DD)	2015-06-07
Name/Print	Paige M. Alsbury	Registration Number	72965

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:	22557827
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	07-JUN-2015
Filing Date:	23-OCT-2014
Time Stamp:	20:08:01
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)	04540US_IDS.pdf	612358 188d592b901d4070dd90884a7eb88197c7e9ad9f	no	4

Warnings:	
Information:	

2	Non Patent Literature	04540_PracticalGuidetoBiometricSecurity.pdf	1011821 0479da4d7e51cc0b05071d0a60c30572fac09c83	no	6
Warnings:					
Information:					
3	Non Patent Literature	04540_SmartCardAllianceReport.pdf	2297926 ffb4067a429f5ceea29fee094d592d249f9aba1d	no	48
Warnings:					
Information:					
		Total Files Size (in bytes):	3922105		

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

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	14521982
Filing Date	2014-10-23
First Named Inventor	John J. Giobbi
Art Unit	2437
Examiner Name	Not Yet Known
Attorney Docket Number	10001-04540 US

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	4759060		1988-07-19	Hayashi et al.	
	2	4993068		1991-02-12	Piosenka et al.	
	3	5187352		1993-02-16	Blair et al.	
	4	5296641		1994-03-22	Stelzl	
	5	5392433		1995-06-06	Hammersley et al.	
	6	5416780		1995-05-16	Patel	
	7	5422632		1995-06-06	Bucholtz et al.	
	8	5450489		1995-09-12	Ostrover et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	9	5619251		1997-04-08	Kuroiwa et al.	
	10	5629980		1997-05-13	Stefik et al.	
	11	5644354		1997-07-01	Thompson et al.	
	12	5666412		1997-09-09	Handelman et al.	
	13	5784464		1998-07-21	Akiyama et al.	
	14	5825876		1998-10-20	Peterson, Jr.	
	15	5857020		1999-01-05	Peterson, Jr.	
	16	5892825		1999-04-06	Mages et al.	
	17	5894551		1999-04-13	Huggins et al.	
	18	5898880		1999-04-27	Ryu	
	19	5917913		1999-06-29	Wang	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	20	5928327		1999-07-27	Wang et al.	
	21	5991399		1999-11-23	Graunke et al.	
	22	5991749		1999-11-23	Morril, Jr.	
	23	6016476		2000-01-18	Maes et al.	
	24	6018739		2000-01-25	McCoy et al.	
	25	6035038		2000-03-07	Campinos et al.	
	26	6035329		2000-03-07	Mages et al.	
	27	6038334		2000-03-14	Hamid	
	28	6041410		2000-03-21	Hsu et al.	
	29	6042006		2000-03-28	Van Tilburg et al.	
	30	6055314		2000-04-25	Spies et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	31	6070796		2000-06-06	Sirbu	
	32	6088730		2000-07-11	Kato et al.	
	33	6104334		2000-08-15	Allport	
	34	6121544		2000-09-19	Petsinger	
	35	6148142		2000-11-14	Anderson	
	36	6161179		2000-12-12	Seidel	
	37	6185316		2001-02-06	Buffam	
	38	6209089		2000-03-27	Selitrennikoff et al.	
	39	6219109		2001-04-17	Raynesford et al.	
	40	6219439		2001-04-17	Burger	
	41	6247130		2001-06-12	Fritsch	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	42	6256737		2001-07-03	Bianco et al.	
	43	6266415		2001-07-24	Campinos et al.	
	44	6295057		2001-09-25	Rosin et al.	
	45	6336121		2002-01-01	Lyson et al.	
	46	6336142		2002-01-01	Kato et al.	
	47	6363485		2002-03-26	Adams et al.	
	48	6367019		2002-04-02	Ansell et al.	
	49	6381747		2002-04-30	Wonfor et al.	
	50	6385596		2002-05-07	Wiser et al.	
	51	6392664		2002-05-21	White et al.	
	52	6397387		2002-05-28	Rosin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	53	6401059		2002-06-04	Shen et al.	
	54	6411307		2002-06-25	Rosin et al.	
	55	6424715		2002-07-23	Saito	
	56	6425084		2002-07-23	Rallis et al.	
	57	6434535		2002-08-13	Kupka et al.	
	58	6446130		2002-09-03	Grapes	
	59	6463534		2002-10-08	Geiger et al.	
	60	6480188		2002-11-12	Horsley	
	61	6490443		2002-12-03	Freeny, Jr.	
	62	6510350		2003-01-21	Steen III et al.	
	63	6523113		2003-02-18	Wehrenberg	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	64	6529949		2003-03-04	Getsin et al.	
	65	6546418		2003-04-08	Schena et al.	
	66	6550011		2003-04-15	Sims III	
	67	6563805		2003-05-13	Ma et al.	
	68	6564380		2003-05-13	Murphy	
	69	6628302		2003-09-30	White et al.	
	70	6632992		2003-10-14	Hasegawa	
	71	6647417		2003-11-11	Hunter et al.	
	72	6667684		2003-12-23	Waggamon et al.	
	73	6683954		2004-01-27	Searle	
	74	6697944		2004-02-24	Jones et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	75	6709333		2004-03-23	Bradford et al.	
	76	6711464		2004-03-23	Yap et al.	
	77	6775655		2004-08-10	Peinado et al.	
	78	6804825		2004-10-12	White et al.	
	79	6806887		2004-10-19	Chernock et al.	
	80	6850147		2005-02-01	Prokoski et al.	
	81	6873975		2005-03-29	Hatakeyama et al.	
	82	6950941		2005-09-27	Lee et al.	
	83	6963971		2005-11-08	Bush et al.	
	84	6973576		2005-12-06	Giobbi	
	85	6975202		2005-12-13	Rodriguez et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	86	6983882		2006-01-10	Cassone	
	87	7012503		2006-03-14	Nielsen	
	88	7090126		2006-08-15	Kelly et al.	
	89	7112138		2006-09-26	Hedrick et al.	
	90	7137012		2006-11-14	Kamibayshi et al.	
	91	7191466		2007-03-13	Hamid et al.	
	92	7218944		2007-05-15	Cromer et al.	
	93	7249177		2007-07-24	Miller	
	94	7305560		2007-12-04	Giobbi	
	95	7529944		2009-05-05	Hamid	
	96	7574734		2009-08-11	Fedronic et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	97	7587611		2009-09-08	Johnson et al.	
	98	7617523		2009-11-10	Das et al.	
	99	7644443		2010-01-05	Matsuyama et al.	
	100	7715593		2010-05-11	Adams et al.	
	101	7883417		2011-02-08	Bruzzese et al.	
	102	7904718		2011-03-08	Giobbi 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	20010044337		2001-11-22	Rowe et al.	
	2	20020007456		2002-01-17	Peinado et al.	
	3	20020013772		2002-01-31	Peinado	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	4	20020014954		2002-02-07	Fitzgibbon et al.	
	5	20020015494		2002-02-07	Nagai et al.	
	6	20020023032		2002-02-21	Pearson et al.	
	7	20020026424		2002-02-28	Akashi	
	8	20020071559		2002-06-13	Christensen et al.	
	9	20020073042		2002-06-13	Maritzen et al.	
	10	20020098888		2002-07-25	Rowe et al.	
	11	20020103027		2002-08-01	Rowe et al.	
	12	20020104006		2002-08-01	Boate et al.	
	13	20020108049		2002-08-08	Xu et al.	
	14	20020109580		2002-08-15	Shreve et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	15	20020129262		2002-09-12	Kutaragi et al.	
	16	20020138767		2002-09-26	Hamid et al.	
	17	20020140542		2002-10-03	Prokoski et al.	
	18	20020144117		2002-10-03	Faigle	
	19	20020150282		2002-10-17	Kinsella	
	20	20020152391		2002-10-17	Willins et al.	
	21	20020158750		2002-10-31	Almalik	
	22	20020174348		2002-11-21	Ting	
	23	20020178063		2002-11-28	Gravelle et al.	
	24	20020191816		2002-12-19	Maritzen et al.	
	25	20030036425		2003-02-20	Kaminkow et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	26	20030046552		2003-03-06	Hamid	
	27	20030054868		2003-03-20	Paulsen et al.	
	28	20030054881		2003-03-20	Hedrick et al.	
	29	20030055689		2003-03-20	Block et al.	
	30	20030079133		2003-03-24	Breiter et al.	
	31	20030115474		2003-06-19	Khan et al.	
	32	20030127511		2003-07-10	Kelly et al.	
	33	20030139190		2003-07-24	Steelberg et al.	
	34	20030149744		2003-08-07	Bierre et al.	
	35	20030172037		2003-09-11	Jung et al.	
	36	20030176218		2003-09-18	LeMay et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	37	20030186739		2003-10-02	Paulsen et al.	
	38	20040127277		2004-07-01	Walker et al.	
	39	20040128162		2004-07-01	Schlotterbeck et al.	
	40	20040129787		2004-07-08	Saito et al.	
	41	20040209690		2004-10-21	Bruzzese et al.	
	42	20040209692		2004-10-21	Schober et al.	
	43	20040215615		2004-10-28	Larsson et al.	
	44	20040230488		2004-11-18	Beenau et al.	
	45	20050074126		2005-04-07	Stanko	
	46	20050081040		2005-04-14	Johnson et al.	
	47	20050109836		2005-05-26	Ben-Aissa	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	48	20050229007		2005-10-13	Bolle et al.	
	49	20050251688		2005-11-10	Nanavati et al.	
	50	20050253683		2005-11-17	Lowe	
	51	20060022046		2006-02-02	Iwamura	
	52	20060113381		2006-06-01	Hochstein et al.	
	53	20060156027		2006-07-13	Blake	
	54	20070220272		2007-09-20	Campisi et al.	
	55	20080019578		2008-01-24	Saito et al.	
	56	20080188308		2008-08-07	Shepherd et al.	
	57	20090328182		2009-12-31	Malakapalli et al.	
	58	20100117794		2010-05-13	Adams et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	59	20110126188		2011-05-26	Bernstein 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	WO 00/62505	WO		2000-10-19	Thomson Multimedia		☐
	2	WO 01/22724	WO		2001-03-29	Thomson Multimedia		☐
	3	WO 01/75876	WO		2001-10-11	Thomson Multimedia		☐
	4	WO 01/77790	WO		2001-10-18	Thomson Multimedia		☐
	5	WO 05/050450	WO		2005-06-02	Margent Development, LLC		☐
	6	WO 05/086802	WO		2005-09-22	Margent Development, LLC		☐

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	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, Retrieved on January 7, 2007 from <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pgs.	☐
	2	Amr Farouk, Ahmed A. Abdelhafez, "Authentication Mechanisms in Grid Computing Environment: Comparative Study," IEEE, 2012, pgs. 1-6.	☐
	3	ANTONOFF, Michael, "Visiting Video Valley," Sound & Vision, November 2001, pgs 116, 118-119.	☐
	4	"Applying Biometrics to Door Access," Security Magazine, September 26, 2002, Retrieved on January 7, 2007, from <URL:http://www.securitymagazine.com/CDA/Articles/technologies/3ae610eaa34d8010VgnVCM100000f932a8c0____>, 5 pgs.	☐
	5	BioPay, LLC, "Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, Retrieved on January 7, 2007, from <URL:http://www.biopay.com/faqs-lowes.asp>, 5 pgs.	☐
	6	BLUM, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, October 2000, pgs. 24-27.	☐
	7	DEBOW, Yvette, "Credit/Debit Debuts in Midwest Smart Card Test," Computers in Banking, v6, n11, November 1989, 4 pgs.	☐
	8	DENNIS, Sylvia, "Digital Passports Need Not Infringe Civil Liberties," Newsbytes, December 2, 1999, 2 pgs.	☐
	9	FASCA, Chad, "The Circuit," Electronic News, Vol. 45 Iss. 45, November 8, 1999, 2 pgs.	☐
	10	"Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet," Computergram International, January 18, 1996, 2 pgs.	☐
	11	KONTZER, Tony, "Thomson Bets on Smart Cards For Video Encryption," www.informationweek.com, June 7, 2001, 1 pg	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	12	LAKE, Matt, "Downloading for Dollars," Sound & Vision, November 2000, pgs. 137-138.	☐
	13	LEWIS, Peter H., "Sony and Visa in On-Line Entertainment Venture," New York Times, v145, November 16, 1995, 1 pg.	☐
	14	MCIVER, R. et al., "Identification and Verification Working Together," Bioscrypt, August 27, 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>, 5 pgs.	☐
	15	"Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, January 8, 2002, 3 pgs.	☐
	16	NILSSON, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, April 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>, 5 pgs.	☐
	17	NORDIN, B., "Match-On-Card Technology," Precise Biometrics, White Paper, April 2004, Retrieved on January 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf>, 7 pgs.	☐
	18	PAGET, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, December 1999, 4 pgs.	☐
	19	PCT International Search Report, PCT/US04/38124, April 7, 2005, 10 pgs.	☐
	20	PCT International Search Report, PCT/US05/43447, February 22, 2007, 7 pgs.	☐
	21	PCT International Search Report, PCT/US05/46843, March 1, 2007, 10 pgs.	☐
	22	PCT International Search Report, PCT/US07/11102, October 3, 2008, 11 pgs.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	23	PCT International Search Report, PCT/US07/11103, April 23, 2008, 9 pgs.	☐
	24	PCT International Search Report, PCT/US07/11104, June 26, 2008, 9 pgs.	☐
	25	PCT International Search Report, PCT/US07/11105, October 20, 2008, 10 pgs.	☐
	26	POPE, "Oasis Digital Signature Services: Digital Signing without the Headaches," Internet Computing-IEEE, Vol. 10, October 2006, pgs. 81-84.	☐
	27	"SAFModuleTM: A Look Into Strong Authentication," saflink Corporation, Retrieved on January 7, 2007, from <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pgs.	☐
	28	SAPSFORD, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, August 14, 2000, 2 pgs.	☐
	29	"Say Hello to Bluetooth," Bluetooth Web site, June 2000, 4 pgs.	☐
	30	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, Retrieved on January 7, 2007, from <URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>, 7 pgs.	☐
	31	"Thomson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001, 2 pgs.	☐
	32	VAN WINKLE, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, January 2000, pgs. 148-153..	☐
	33	WADE, Will, "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, April 21, 2003, Retrieved on January 7, 2007, from <URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>, 3 pgs.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

	34	WALLACE, Bob, "The Internet Unplugged," InformationWeek.com, December 13, 1999, pgs. 22-24.	☐
	35	WEBER, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, July 24, 2000, 3 pgs.	☐
	36	"What is a File?," April 30, 1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed March 11, 2010 via http://waybackmachine.org/1998061500000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html, 1 pg.	☐
	37	YOSHIDA, Junko, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002, 2 pgs.	☐

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	14521982
	Filing Date	2014-10-23
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Not Yet Known
	Attorney Docket Number	10001-04540 US

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	/Paige Alsbury/	Date (YYYY-MM-DD)	2015-02-12
Name/Print	Paige M. Alsbury	Registration Number	72,965

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.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, 12/28

A1

(11) International Publication Number: WO 00/62505

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/EP00/02918

(22) International Filing Date: 31 March 2000 (31.03.00)

(30) Priority Data:
99/04767 13 April 1999 (13.04.99) FR

(71) Applicant *(for all designated States except US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F–92100 Boulogne–Billancourt (FR).

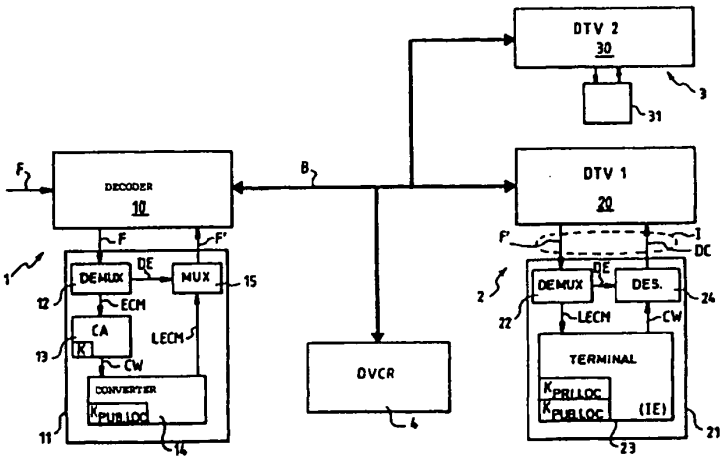
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: QUES, Florence [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR). ANDREAUX, Jean–Pierre [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR). FURON, Teddy [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR).

(74) Agent: KOHRS, Martin; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DIGITAL HOME NETWORK AND METHOD FOR CREATING AND UPDATING SUCH A NETWORK



(57) Abstract

The local digital network comprises: access devices (1), for receiving data originating from outside the network and transmitting them at a point of the network; and presentation devices (2, 3) for receiving the data flowing in the network and presenting them at a point of the network. The data flow in the network in encrypted form and all the devices of the network use a single key, the local key of the network, for the encryption and decryption of the data. Preferably, the local key of the network is formed by a pair of public and private keys. The purpose of this network is to make it possible to copy data in the local network whilst preventing pirate copies destined for other local networks.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

DIGITAL HOME NETWORK AND METHOD FOR CREATING AND UPDATING SUCH A NETWORK

The present invention relates generally to the field of local digital networks and more particularly to the field of digital home networks.

Such a network consists of a set of devices interlinked by a digital bus, for example a bus according to the IEEE 1394 standard. It comprises two main types of devices:

- access devices capable of receiving data originating from outside the local network and of transmitting them at a point of the network to which the devices are connected, and
- presentation devices, adapted to receive the data flowing in the network so as to present them at another point of the network to which these devices are connected. This second type of device has no link with the outside of the local network.

Thus, if one takes the example of a digital home network intended for conveying audio and/or video data into various rooms of a house, the access devices are for example digital decoders or set-top boxes receiving video programmes from outside the network, via a satellite antenna or via a cable connection, or else readers of optical disks broadcasting on the network, in digital form, data (audio and/or video) read from a disk (in this case the disk contains data originating from outside the network). The presentation devices are for example television receivers making it possible to view video programmes received from the network or, more generally, any type of apparatus capable of converting digital information received into an analogue signal so as to broadcast this signal to an end user.

A home network of the type mentioned hereinabove can also comprise a third type of device having no link

with the outside of the network and having the function of recording the data flowing in the network. By way of example of apparatuses of this third type, mention may in particular be made of digital video recorders or apparatuses capable of recording optical disks, of the DVD type (the abbreviation "DVD" standing for "Digital Versatile Disk").

It should be noted that one and the same apparatus can belong to two, or even three different categories of devices mentioned hereinabove. For example, an apparatus for recording optical disks can also be capable of reading commercial prerecorded disks and thus of belonging at the same time to the first and to the third categories of devices mentioned above.

If one considers the viewpoint of the content providers who provide the data originating from outside the local network, especially providers of services broadcasting pay-televised programmes or else publishers of optical disks for example, it is necessary to prevent these transmitted data from being copied and from being able to flow easily (for example by being copied onto an optical disk or any other recording medium) from one local network to the other.

To do this, it is known practice to transmit the data in secret form by encrypting them with the aid of cryptography algorithms using keys which are known beforehand to the devices authorized to receive these data or else which are exchanged according to particular secure protocols between the content provider and these devices.

If one now considers the viewpoint of a user who possesses a digital home network, it is desirable for these data to be able to be transmitted to all the other devices of the network when one of the devices of the network is authorized to receive data from a content provider. Thus, a user who is a subscriber to a pay-television service and receives programmes (transmitted

in encrypted form) on a set-top box located in his lounge (authorized to decrypt them), will wish to be able to watch these programmes for example on a television located in his bedroom. Moreover, the user is interested in recording programmes received and in being able subsequently to view them on several devices of the network even when he no longer subscribes to the pay-television service.

To take into account the wishes of content providers and also of users, it is an object of the invention to provide a means such that data received by a local digital network can flow freely between the various devices of the network whilst preventing them from flowing from one local network to another.

To this end, the invention proposes a local digital network, in particular a digital home network, comprising at least one access device, capable of receiving data originating from outside the network and of transmitting them at a point of the network; and at least one presentation device, adapted to receive data flowing in the network so as to present them at a point of the network; in which the data are adapted to flow only in encrypted form. According to the invention, all the devices of the network use for the encryption and decryption of the data flowing in the network a single encryption key specific to the network: the local key of the network.

Since each local network possesses its own local key which is different from that of the other local networks, any information which enters the said network will be readable equally by all the devices of the network but will not be copiable for being read onto another local network. More exactly, the information will be copiable, in its encrypted form, but it will not be possible to replay it in a local network different from that to which it was copied. Thus, the invention meets the wishes of content providers and also of users.

According to a preferred aspect of the invention, the data are encrypted using a cryptographic system with public keys, also known as asymmetric cryptographic system. The local key of the network is in this case formed by a pair of public and private keys: the local public key and the local private key of the network.

Preferably, only the presentation devices connected to the network know the local private key.

According to a particular embodiment, at a given instant, a single presentation device of the network is authorized to transmit the local private key to a new presentation device apt to be connected to the network. This device will subsequently be referred to as the genitor of the network.

Thus, if this genitor is removed from the local network, especially to create a pirate local network possessing the same local key as the initial local network, the latter will no longer be able to alter since no device of the initial network will any longer be capable of transmitting the local private key of the network to a new presentation device apt to be connected to the initial local network.

According to another aspect of the invention, at a given instant, a presentation device can be in only one of the following states:

i) a first state, the virgin state, when the presentation device is connected for the first time to the network;

ii) a second state, the genitor state, in which the presentation device is authorized to transmit the local private key of the network to any new presentation device apt to be connected to the network;

iii) a third state, the sterile state, in which the presentation device is no longer authorized to transmit the local private key of the network to any new presentation device apt to be connected to the said network.

A presentation device can change state only so as to pass to a state of higher rank, that is to say from the virgin state to the genitor state or from the genitor state to the sterile state, or else from the virgin state to the sterile state.

According to a preferred aspect of the invention, a single presentation device of the network is in the second state, the genitor state: the genitor of the network.

According to a particular embodiment, at a given instant, the genitor of the network is the presentation device which was connected last to the network.

Thus, the title of "genitor" of the network is transmitted to each new apparatus connected to the local network. This prevents a pirate from being able, starting from a single genitor presentation device, to create in series local networks all having the same local keys.

The invention also relates to a presentation device adapted to be connected to a digital network such as described hereinabove and which, at a given instant, can be in only one of the states which were mentioned above, namely: the virgin state, the genitor state or the sterile state, the said presentation device being adapted to change state only so as to go to a state of higher rank.

According to one aspect of the invention, when the presentation device is in the virgin state, it possesses its own pair of public and private keys and it is authorized to receive the pair of local keys of a network to which it is apt to be connected so as to store them instead of its own pair of keys.

According to another aspect of the invention, when the presentation device is in the sterile state, it is no longer authorized to receive the pair of local keys of a network to which it is apt to be connected.

According to another aspect of the invention, the presentation device comprises a means for storing the

state which said presentation device occupies, this storage means being integrated into a smart card.

According to yet another aspect of the invention, the pair of local keys of the network is contained in a smart card with which said device is furnished.

The invention also relates to a process for creating and for updating a network such as hereinabove, which will be described subsequently.

Other characteristics and advantages of the invention will become apparent on reading the following description of a particular, nonlimiting embodiment of the invention, given with reference to the appended drawings in which:

- Figure 1 represents a local digital network according to the invention;
- Figure 2 illustrates a process for creating a digital network such as that of Figure 1; and
- Figure 3 illustrates a process for connecting a new presentation device to a local digital network created according to the process of Figure 2 for example.

In the figures, only the elements which are vital to the understanding of the invention and of the particular embodiment which will be described have been represented.

Represented in Figure 1 is a digital home network comprising an access device 1, two presentation devices 2 and 3 as well as a digital video recorder 4, commonly referred to as a DVCR (the abbreviation DVCR standing for "Digital Video Cassette Recorder"). The assembly of devices 1, 2, 3 and 4 is connected to a domestic digital bus B which is for example a bus according to the IEEE 1394 standard.

The access device 1 comprises a digital decoder 10 equipped with a smart card reader furnished with a smart card 11. This digital decoder 10 is connected, either to a satellite antenna, or to a cable network, so as to receive video programmes distributed by a service

provider. These programmes are received in a stream F of data for example in the MPEG-2 format. In a manner known per se, they are transmitted in scrambled form, the content being scrambled by control words CW. These control words are themselves transmitted, in the data stream F, in a form encrypted using a key K according to a given enciphering algorithm in such a way as to remain secret during transmission.

Thus, only the users authorized by the service provider are empowered to descramble the data transmitted (against payment of a subscription for example). To do this, the provider supplies the authorized users with the key K serving to decrypt the control words CW. Very often, authorization to receive the programmes is only temporary, so long as the user pays his subscription. The key K is therefore modified regularly by the service provider.

By virtue of the invention, and as will be seen hereinbelow, the user will nevertheless be able to record programmes transmitted while he is subscribing and to replay them as often as he wishes on his own network, even if he is no longer a subscriber. On the other hand, since the data are recorded in scrambled form, it will only be possible to replay them on the network of the user who recorded them.

In Figure 1, the network is represented in the state which it occupies when all the apparatuses have been connected according to the processes which will be described subsequently in conjunction with Figures 2 and 3.

We shall now describe how the data which are transmitted in the stream F received by the decoder 10 are processed. As is known to the person skilled in the art, in the case of data transmitted according to the MPEG-2 format, the data stream F comprises a succession of video data packets, of audio data packets and of management data packets. The management data packets

comprise in particular control messages denoted ECM (the abbreviation "ECM" standing for "Entitlement Control Message") in which are transmitted, in a form encrypted using a key K, the control words CW which served to scramble the data transmitted in the video and audio data packets.

This data stream F is transmitted to the smart card 11 so as to be processed therein. It is received by a demultiplexer circuit (DEMUX) 12, which circuit transmits, on the one hand to an access control circuit (CA) 13 the ECMs and, on the other hand, to a multiplexing circuit (MUX) 15 the packets, denoted DE, of scrambled video and audio data. The circuit CA contains the key K and can thus decrypt the control words CW which are contained in the ECMs. The circuit CA transmits these control words CW to a converter circuit 14 which contains, according to the invention, the local public key of the network $K_{PUB.LOC}$. The converter 14 uses the key $K_{PUB.LOC}$ to encrypt the control words CW and transmits these control words, encrypted using the local public key, to the multiplexing circuit 15 in control messages denoted LECM. These messages LECM have the same function as the messages ECM received in the initial data stream F, namely of transmitting the control words CW, but in the messages LECM, the control words CW are encrypted therein using the local public key $K_{PUB.LOC}$ instead of being encrypted using the key K of the service provider.

The multiplexing circuit 15 then transmits the data packets DE and the converted control messages LECM in a data stream F' which is received by the decoder 10. It is this data stream F' which will then flow around the domestic bus B so as to be received, either by one of the presentation devices 2 or 3, or by the digital video recorder 4 so as to be recorded. According to the invention, the data therefore always flow in encrypted form in the bus B, and only the apparatus containing the private local key $K_{PRI.LOC}$ of the network are capable of

decrypting the control words CW and hence of decrypting the data DE. This therefore prevents the broadcasting to other local networks of any copy made in the domestic network of Figure 1.

In the example of Figure 1, the circuits 12 to 15 are integrated into the smart card 11 but in a variant embodiment, it is possible to place the circuits DEMUX and MUX in the decoder 10, only the circuits 13 and 14 remaining integrated into the smart card. Specifically, since the circuit CA 13 and the converter 14 contain decryption and encryption keys, they must be integrated into a secure medium such as a smart card.

The presentation device 2 comprises a digital television receiver (DTV1) 20 equipped with a smart card reader furnished with a smart card 21. The receiver 20 receives the data stream F' originating, either from the decoder 10, or from the digital video recorder 4, through the bus B. The data stream F' is transmitted to the smart card 21. It is received by a demultiplexer circuit (DEMUX) 22, which transmits, on the one hand the scrambled video and audio data packets DE to a descrambling circuit (DES.) 24, and on the other hand the converted control messages LECM to a terminal module 23. The terminal module contains the pair of public ($K_{PUB.LOC}$) and private ($K_{PRI.LOC}$) keys of the network. Since the control messages LECM contain the control words CW which have been encrypted using the local public key $K_{PUB.LOC}$ of the network, the terminal module can decrypt these control words using the local private key $K_{PRI.LOC}$ so as to obtain the control words CW in clear. These control words CW are then transmitted to the descrambling circuit 24 which uses them to descramble the data packets DE and to output clear data packets DC to the television receiver 20.

In order to secure the transmission lastly of the clear data DC between the smart card 21 and the display circuits of the television receiver 20, the interface I

between said smart card and the card reader of the receiver 20 is for example made secure according to the American NRSS standard (NRSS being the acronym for National Renewable Security Standard) for securing smart cards.

The second presentation device 3, comprising a digital television receiver (DTV2) 30 equipped with a smart card reader furnished with a smart card 31 operates in exactly the same way as the presentation device 2 and will not be described further.

By virtue of the local digital network just described, the data stream F originating from a content provider is transformed by the access device which receives it into a data stream F' by virtue of the local public key of the network $K_{PUB.LOC}$. This data stream F' thus contains data having a format specific to the local network, which data cannot be decrypted other than by the presentation devices of the local network which all contain the local private key of the network.

We shall now describe how the local digital network of Figure 1 is created and how the connecting of new apparatuses to the said network is managed so as to guarantee that all the apparatuses of the network all share the unique local pair of keys of the network.

In Figure 2, the process for creating the digital network represented in Figure 1 is illustrated diagrammatically.

To create a digital network according to the invention, it is necessary to connect together an access device and a presentation device.

In Figure 2, it is assumed that at the outset the network is created by connecting the access device 1 and the presentation device 2 by way of the digital bus B. The various steps of the process for creating the network have been represented along a time axis t which is doubled up in such a way as to illustrate the exchanges which take place between the two devices.

In the first step 100 of the process, when the two devices are connected together, the presentation device contains a pair of public K_{PUB2} and private K_{PRI2} keys and is, according to the invention, in the virgin state.

The state of the device is stored preferably by a state indicator IE which is a 2-bit register located in the terminal module 23 (Figure 1) of the presentation device. By convention, it is assumed that when the device is in the virgin state, the state indicator IE is equal to 00; when the device is in the genitor state, IE = 01 and when the device is in the sterile state, IE = 10.

The state indicator IE is contained in an integrated circuit in a smart card so as to guarantee that it is tamper-proof.

When a presentation device is sold by a manufacturer, it must be able to be connected to any existing local digital network, of the type of the invention. It must also be capable of being connected to an access device so as to create a new network. This is why any presentation device which is manufactured according to the invention routinely comprises a pair of public and private keys, this pair of keys being unique and different from one device to another, so as to guarantee the fact that each local network created according to the invention also possesses a unique pair of keys. Moreover, to guarantee the security of the exchanges, all the pairs of private/public keys used are certified according to a method known to the person skilled in the art.

The access devices, on the other hand, are manufactured and sold without containing any encryption/decryption key. They nevertheless preferably contain a converter circuit (contained in a smart card) according to the invention and such as described previously in conjunction with Figure 1, which is capable

of storing a local key of a network to which they are apt to be connected.

Referring again to Figure 2, step 101 of the process consists, for the presentation device 2, in dispatching over the bus B its public key K_{PUB2} destined for all the access devices apt to be connected to the bus B, in this instance the access device 1.

Step 102 consists, for the access device 1, in receiving the public key K_{PUB2} and in storing it as the new local public key of the network ($K_{PUB.LOC} = K_{PUB2}$).

In step 103, the access device 1 dispatches over the bus B a change of state signal destined for the presentation device 2. This step has the objective of indicating to the presentation device 2 that it is the first to be connected to the network and that it must therefore become the genitor of the network, that is to say the only presentation device authorized to transmit its private key K_{PRI2} (which becomes the local private key of the network $K_{PRI.LOC}$) to any new presentation device apt to be connected to the network.

Step 104 therefore consists, for the presentation device 2, in receiving the change of state signal and modifying its state indicator so as to pass to the genitor state (IE = 01).

At the end of the process, one therefore has a local digital network in accordance with the invention which comprises a unique local public key $K_{PUB.LOC}$ (equal to the initial public key K_{PUB2} of the presentation device 2) which is known to both devices of the network, and a unique local private key $K_{PRI.LOC}$ which is known only to the presentation device 2. The network also comprises, in accordance with the invention, a genitor presentation device which is capable of altering it by allowing the connection of new presentation devices.

The process for connecting a new presentation device, in this instance the presentation device 3, to the network created in accordance with the process of

Figure 2, will now be described in conjunction with Figure 3.

In the first step 200, 200' 200" of the process, which consists in connecting the presentation device 3 to the existing local network by way of the digital bus B, the presentation device 3 contains its own pair of public K_{PUB3} and private K_{PRI3} keys and it is in the virgin state (IE = 00). The access device 1 and presentation device 2 are respectively in the same state as at the end of the process of Figure 2, that is to say the access device 1 contains the local public key of the network $K_{PUB.LOC}$ and the presentation device is the genitor of the network (IE = 01) and contains the pair of local keys ($K_{PUB.LOC}$, $K_{PRI.LOC}$) of the network.

The second step 201 consists, for the presentation device 3, in dispatching over the bus B its public key K_{PUB3} destined for all the access devices apt to be connected to the bus B, in this instance the access device 1. This step is the same as step 101 (Figure 2) of the creation process.

Step 202 consists, for the access device 1, in receiving the public key K_{PUB3} and in verifying whether it already contains a public key or not (VERIF. PRESENCE $K_{PUB.LOC}$).

In the event of a positive verification, this being the case in this instance, the next step 203 consists, for the access device 1, in dispatching the local public key $K_{PUB.LOC}$ over the bus B destined for the new presentation device 3.

In step 204, the presentation device 3 receives the local public key $K_{PUB.LOC}$ and stores it, preferably in its terminal module.

The next step 205 consists, for the presentation device 3, in dispatching a signal over the bus B, addressed to all the presentation devices of the network, in the form of a message (GENITOR?) requesting the genitor device of the network to respond to it.

In step 206, the genitor device of the network, in this instance the presentation device 2, receives this message and, once the communication has been established in a dependable manner between the presentation devices 2 and 3, it changes state so as to pass to the sterile state (IE = 10).

Step 207 then consists, for the presentation device 2, in dispatching the local private key of the network in encrypted form ($E(K_{PRI.LOC})$) which can be decrypted by the presentation device 3. In particular, this secure transmission of the local private key between the presentation devices 2 and 3 can be performed using the initial public key K_{PUB3} of the presentation device 3 to encrypt the local private key, the presentation device 3 being capable of decrypting this message using its private key K_{PRI3}. The key K_{PUB3} is for example transmitted to the presentation device 2 during step 205.

In step 208, the presentation device 3 receives and decrypts the local private key and stores it, preferably in its terminal module, integrated into the smart card 31 (Figure 1).

Step 209 consists, for the presentation device 3, in dispatching a signal acknowledging receipt of the local private key (ACKNOWLEDGE-RECEIPT ($K_{PRI.LOC}$)) over the bus B destined for the presentation device 2.

In step 210, the presentation device 2 receives this acknowledgement of receipt signal and dispatches, in response, a change of state signal to the new presentation device 3 and in step 211, the presentation device 3 receives this signal and changes state so as to become the new genitor of the network (IE = 01).

Since the presentation device 2 is henceforth in the sterile state, it is no longer authorized to transmit the local public key of the network to another presentation device. This makes it possible to prevent this device 2 from being removed from the network so as

to create another pirate local network possessing the same pair of local keys as the network just described.

At the end of the process, there are therefore two presentation devices 2 and 3 and one access device 1 which are connected to the local network. They all share the local key pair of the network $K_{PUB.LOC}$, $K_{PRI.LOC}$. There is always a unique genitor in the network which is the presentation device which was connected last to the network.

The connecting of a new access device to the local network is for its part much simpler since any access device in accordance with the invention is sold without containing a key. It is in particular possible to envisage that when a new access device is plugged into the network, it dispatches a message over the bus B requesting to receive the public key of the network. It is then possible to make provision for either the first network device which receives this message, or only the genitor device, to dispatch, in response to this message, the public key of the network to the new access device.

CLAIMS

1. Local digital network, in particular digital home network, comprising:

- at least one access device (1), capable of receiving data originating from outside said network and of transmitting them at a point of said network; and
- at least one presentation device (2, 3), adapted to receive data flowing in the network so as to present them at a point of the network;

in which the data are adapted to flow only in encrypted form, characterized in that all the devices of said network use for the encryption and decryption of the data flowing in the network a single encryption key specific to the network: the local key ($K_{PUB.LOC}$, $K_{PRI.LOC}$) of the network.

2. Digital network according to Claim 1, in which the data are encrypted using a public keys cryptographic system, characterized in that said local key of the network is formed by a pair of public and private keys: the local public key ($K_{PUB.LOC}$) and the local private key ($K_{PRI.LOC}$) of the network.

3. Digital network according to Claim 2, characterized in that only the presentation devices (2, 3) connected to the said network contain the local private key ($K_{PRI.LOC}$).

4. Digital network according to Claim 3, characterized in that at a given instant, a single presentation device of the network is authorized to transmit the local private key ($K_{PRI.LOC}$) to a new presentation device apt to be connected to said network.

5. Digital network according to Claim 3, characterized in that at a given instant, a presentation device can be in only one of the following states:

i) a first state, the virgin state (IE = 00), when the presentation device is connected for the first time to said network;

ii) a second state, the genitor state (IE = 01), in which the presentation device is authorized to transmit the local private key of the network to any new presentation device apt to be connected to said network;

iii) a third state, the sterile state (IE = 10), in which the presentation device is no longer authorized to transmit the local private key of the network to any new presentation device apt to be connected to the said network,

a presentation device being adapted to change state only so as to pass to a state of higher rank.

6. Digital network according to Claim 5, characterized in that a single presentation device of the network is in the second state, the genitor state: the genitor of the network.

7. Digital network according to Claim 6, characterized in that at a given instant, the genitor of the network is the presentation device which was connected last to the said network.

8. Presentation device adapted to be connected to a digital network according to one of Claims 2 to 7, characterized in that at a given instant, said presentation device can be in only one of the following states:

i) a first state, the virgin state (IE = 00), when the presentation device is connected for the first time to a network;

ii) a second state, the genitor state (IE = 01), in which the presentation device is authorized to transmit the local private key of the network to any new presentation device apt to be connected to said network;

iii) a third state, the sterile state (IE = 10), in which the presentation device is no longer authorized to transmit the local private key of the network to any new presentation device apt to be connected to said network,

said presentation device being adapted to change state only so as to pass to a state of higher rank.

9. Presentation device according to Claim 8, characterized in that when said presentation device is in the virgin state, it contains its own pair of public and private keys and it is authorized to receive the pair of local keys of a network to which it is apt to be connected so as to store them instead of its own pair of keys.

10. Presentation device according to one of Claims 8 or 9, characterized in that when said presentation device is in the sterile state, it is no longer authorized to receive the pair of local keys of a network to which it is apt to be connected.

11. Presentation device according to one of Claims 8 to 10, characterized in that it comprises a means (IE) for storing the state which said presentation device occupies, this storage means being integrated into a smart card (21, 31).

12. Presentation device according to one of Claims 8 to 11, characterized in that the pair of local keys of the network is contained in a smart card (21, 31) with which said device is furnished.

13. Process for creating a local digital network according to one of Claims 5 to 7, characterized in that it comprises the steps consisting successively:

a) in connecting together by way of a digital bus (B) an access device (1) and a presentation device (2) in the virgin state and containing a pair of public (K_{PUB2}) and private (K_{PRI2}) keys;

b) for the presentation device (2), in dispatching over said bus (B) its public key (K_{PUB2});

c) for the access device (1), in receiving said public key (K_{PUB2}), in storing it as a new local public key of the network ($K_{PUB.LOC} = K_{PUB2}$) and in dispatching over said bus a signal of change of state of the presentation device;

d) for the presentation device (2), in receiving said change of state signal and in passing to the genitor state (IE = 01).

14. Process for connecting a new presentation device (3) in the virgin state (IE = 00) and containing a pair of public (K_{PUB3}) and private (K_{PRI3}) keys to a local digital network according to one of Claims 5 to 7, characterized in that it comprises the steps consisting successively:

e) in connecting the new presentation device (3) to the said local network by way of a digital bus (B);

f) for the new presentation device (3), in dispatching over said bus its public key (K_{PUB3});

g) for at least one of the access devices (1) of said network, in receiving the public key (K_{PUB3}) of the new presentation device, in verifying that said access device already contains a public key, the local public key ($K_{PUB.LOC}$) of the network, and, in the event of a positive verification, in dispatching over the bus (B) the local public key of the network;

h) for the new presentation device (3), in receiving the local public key ($K_{pub,LOC}$) of the network, in storing it and in dispatching over said bus a signal, addressed to all the presentation devices of the network, requesting response from the presentation device in the genitor state;

i) for the genitor presentation device of the network (2), in receiving said response request signal, in passing to the sterile state (IE = 10), and in dispatching in response to the new presentation device (3) the local private key ($K_{PRI.LOC}$) of the network in an encrypted form which can be decrypted by the new presentation device (3);

j) for the new presentation device (3), in receiving said local private key ($K_{PRI.LOC}$) of the network, in storing it and in dispatching an acknowledgement of

receipt signal to the presentation device which was formerly the genitor of the network (2);

k) for the presentation device which was formerly the genitor of the network (2), in receiving said acknowledgement of receipt signal and in dispatching to the new presentation device (3) a change of state signal;

l) for the new presentation device (3), in receiving said change of state signal and in passing to the genitor state (IE = 01).

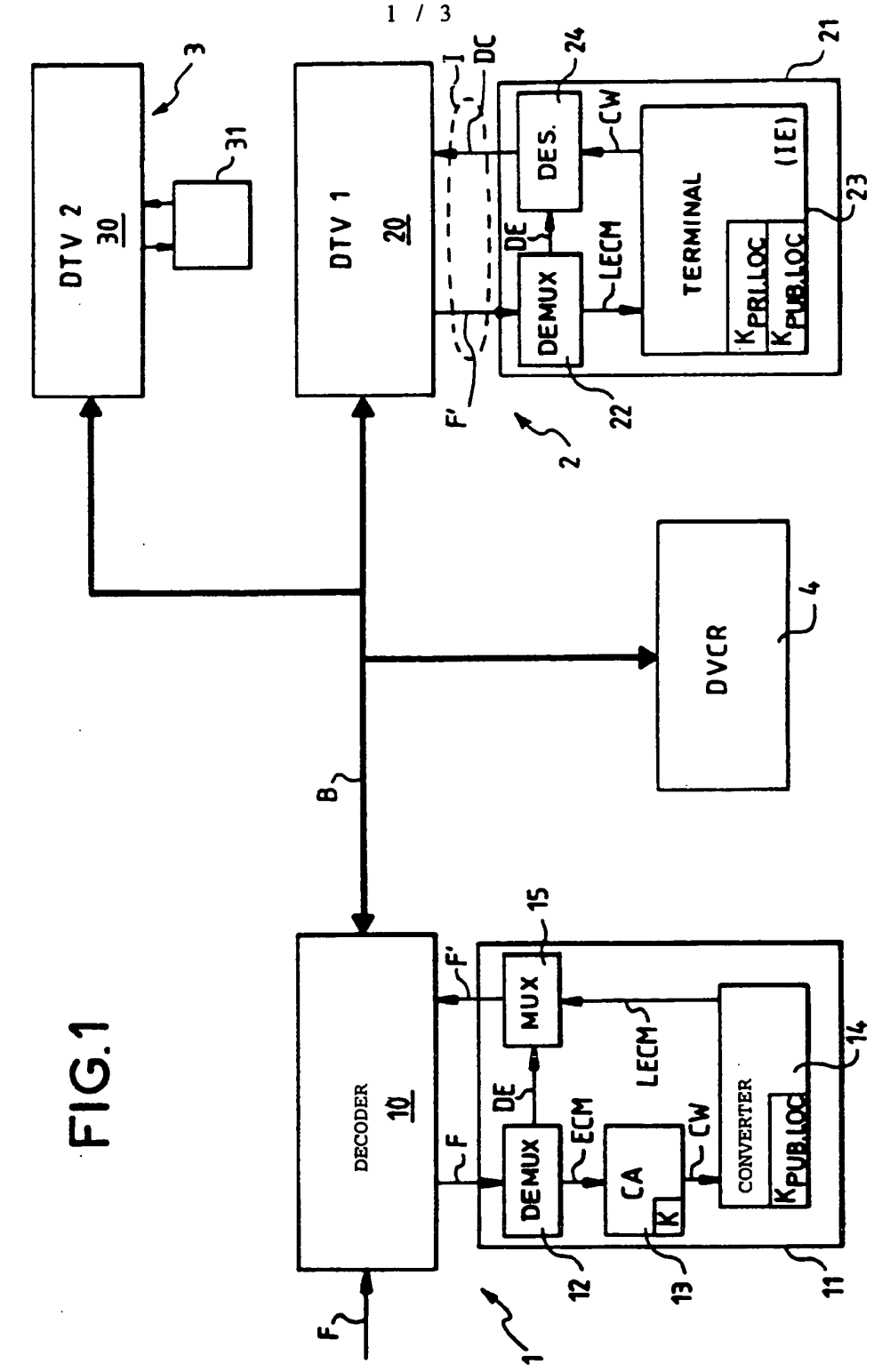

DTV 2
30
31
3
DTV 1
20
I
DC
F'
DES.
24
CW
DE
DEMUX
LECM
TERMINAL
(IE)
K PRI.LOC
K PUB.LOC
21
23
22
2
DVCR
4
B
DECODER
10
F
F'
MUX
15
DE
DEMUX
ECM
CA
K
CW
LECM
CONVERTER
K PUB.LOC
14
12
13
11
1

FIG.1

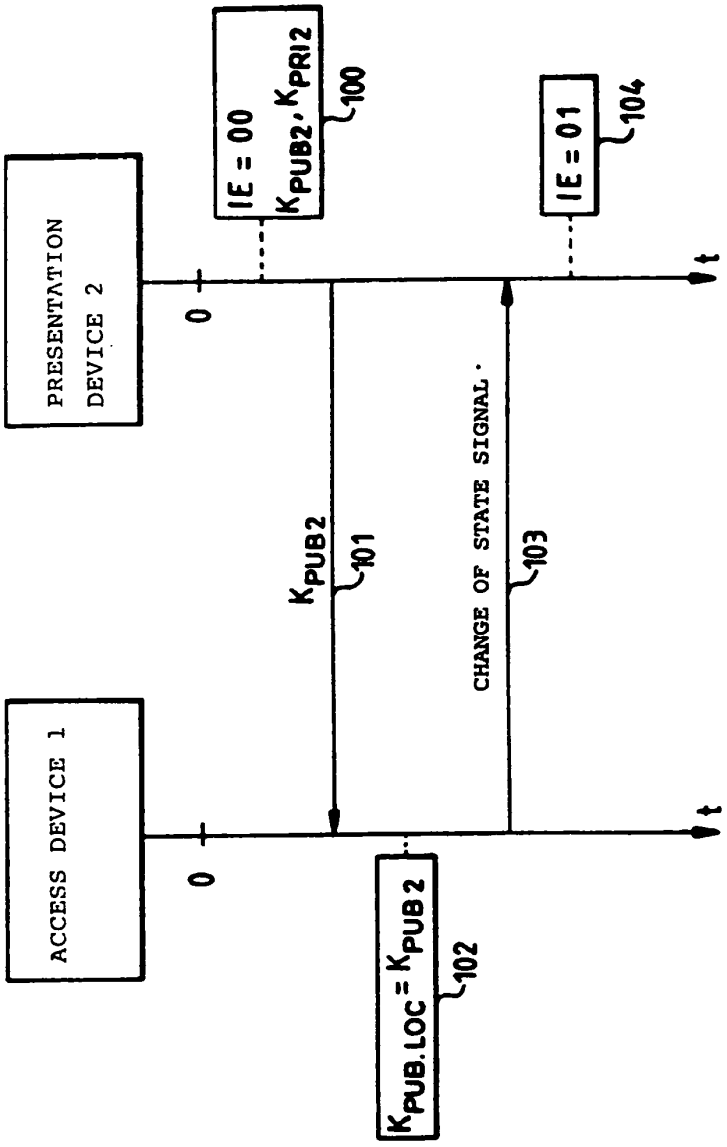

PRESENTATION DEVICE 2
ACCESS DEVICE 1
0
0
t
t
IE = 00
K_{PUB2}, K_{PRI2}
100
IE = 01
104
K_{PUB2}
101
CHANGE OF STATE SIGNAL
103
$K_{PUB.LOC} = K_{PUB2}$
102

FIG. 2

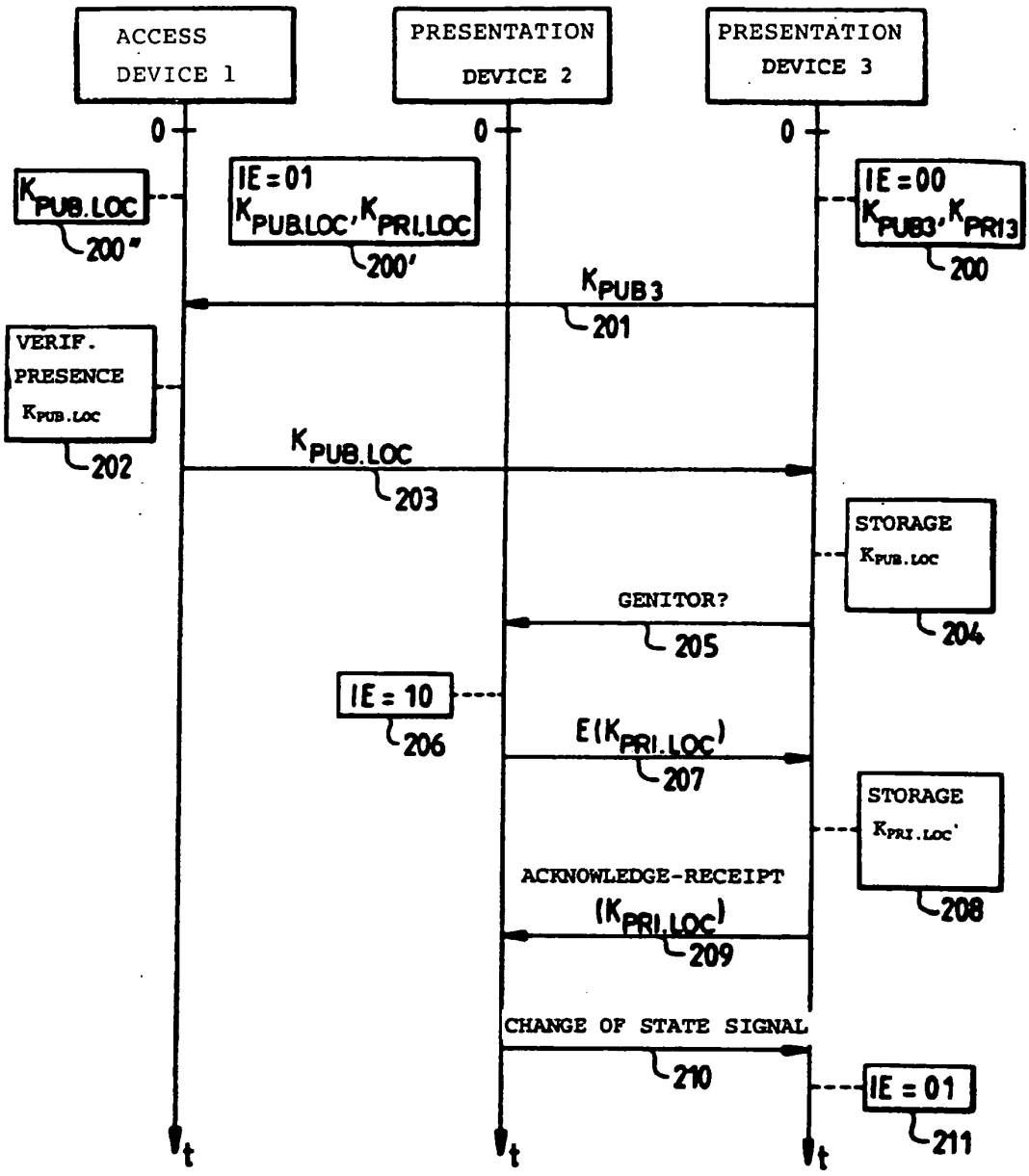

ACCESS DEVICE 1
PRESENTATION DEVICE 2
PRESENTATION DEVICE 3
0
0
0
$K_{PUB.LOC}$
200"
IE = 01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE = 00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
VERIF. PRESENCE $K_{PUB.LOC}$
202
$K_{PUB.LOC}$
203
STORAGE $K_{PUB.LOC}$
204
GENITOR?
205
IE = 10
206
$E(K_{PRI.LOC})$
207
STORAGE $K_{PRI.LOC}$
208
ACKNOWLEDGE-RECEIPT ($K_{PRI.LOC}$)
209
CHANGE OF STATE SIGNAL
210
IE = 01
211
t
t
t

FIG.3

INTERNATIONAL SEARCH REPORT

Inter xnal Application No
PCT/EP 00/02918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 382 296 A (N.V. PHILIPS GLOEILAMPENFABRIEKEN) 16 August 1990 (1990-08-16)	1
A	column 2, line 2-37 column 3, line 12-29 column 4, line 40-44 column 4, line 55 -column 5, line 34 column 6, line 57 -column 7, line 5 column 8, line 56 -column 9, line 42	2-14
A	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 (1995-10-25) page 2, line 22-41 page 3, line 31-34 page 3, line 47-50 page 7, line 34-57 page 9, line 46-57	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2000	21/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter nal Application No
PCT/EP 00/02918

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0679029 A	25-10-1995	US 5237610 A	17-08-1993
		EP 0683614 A	22-11-1995
		AT 144670 T	15-11-1996
		AT 181196 T	15-06-1999
		AT 180373 T	15-06-1999
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		BR 9201106 A	24-11-1992
		CN 1066950 A,B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		DE 69229235 D	24-06-1999
		DE 69229235 T	23-09-1999
		DE 69229408 D	15-07-1999
		DE 69229408 T	11-11-1999
		EP 0506435 A	30-09-1992
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22724 A1

(51) International Patent Classification[7]: H04N 5/00, 7/16, 7/167

(21) International Application Number: PCT/EP00/08439

(22) International Filing Date: 30 August 2000 (30.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99/11901 23 September 1999 (23.09.1999) FR

(71) Applicant *(for all designated States except US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: MORCEL, Stéphane [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(74) Agent: KOHRS, Martin; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

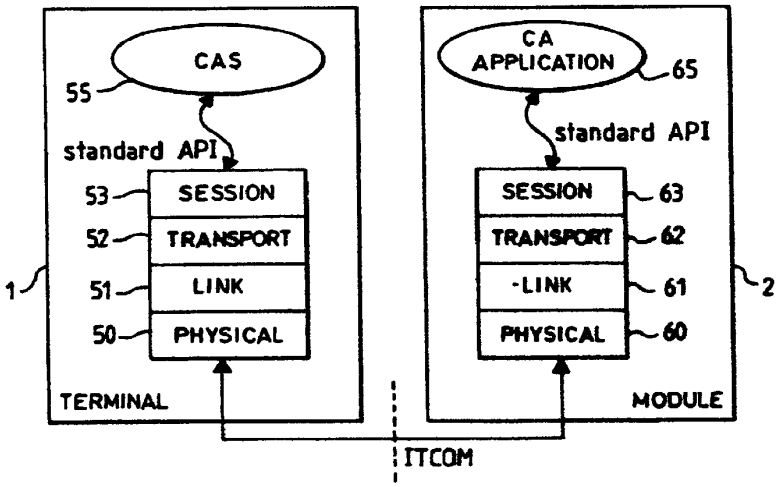
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTIMEDIA DIGITAL TERMINAL AND DETACHABLE MODULE COOPERATING WITH THE TERMINAL COMPRISING AN INTERFACE PROTECTED AGAINST COPYING



(57) Abstract: The terminal (1) receives a scrambled data stream (TS(D.EMB.)) in which the control words (CW) having served to scramble the data are transmitted in encrypted form. It transmits, via a first interface (ITTS), this stream to a detachable module (2) containing the conditional access system specific to the service provider supplying the data. The module (2) extracts from the stream and decrypts the control words (CW) before transmitting them to the terminal, via a second interface (ITCOM). These control words are used by a descrambler (16) of the terminal to descramble the data. The data stream leaving the module (TS'(D.EMB.)) contains only scrambled data, thus guaranteeing better protection against copying.

WO 01/22724 A1

Multimedia digital terminal and detachable module cooperating with the terminal comprising an interface protected against copying

The present invention relates to the field of conditional access systems for multimedia digital terminals. It relates more particularly to a multimedia digital terminal as well as to a detachable module associated with this terminal for implementing a conditional access system, in which the interface between the terminal and the module is protected against illicit copying.

The invention has been embodied within the context of the so-called DVB-CI interface (the initials standing for "Digital Video Broadcasting - Common Interface" which is described in particular in European Standard EN 50221 published by CENELEC (Comité Européen de Normalisation Electrotechnique).

This DVB-CI common interface has been defined by the DVB group so as to allow standardization of digital receiving equipment whilst allowing service providers supplying the data, (for example suppliers of Pay TV programmes) to remain proprietors of the conditional access system and of the corresponding security elements. This is because a conditional access system must be envisaged whenever it is necessary to control access to broadcast data. However, the service providers supplying the data wish to preserve a specific conditional access system. By virtue of the DVB-CI interface, the specific proprietary elements can be integrated into a module which is separate from the standardized parts of the terminal which receive and decode the digital video data or the service data. Thus, the proprietary elements can be manufactured and sold separately from the terminals, thereby making their distribution easier. The module is referred to as a "DVB-CI module" by extension.

The aforesaid European standard describes in particular the hardware and software architecture of the common interface between a server (the host) and one or more DVB-CI modules connected to the server.

We have represented this architecture in Figure 1. The host server 1 is a multimedia digital terminal such as a decoder of programmes broadcast by satellite or by cable, a video recorder or a personal computer, to which may be connected one or more modules 2. The module 2 is a detachable device which cannot operate alone but which is intended to execute certain specific tasks in association with the host server, in particular the implementation of a conditional access system or of an electronic programme guide. To do this, the module can access resources, that is to say software or hardware functional units, of the host server. The aforesaid common interface standard defines for this purpose a certain number of objects able to be exchanged between the module and the host server and allowing the module to use the resources of the host server.

Within the framework of the standards defined by the DVB group, the digital data are transmitted in the form of an information stream coded according to the MPEG 2 standard (ISO/IEC 13818-1), but naturally any other data transport standard can be used within the framework of the invention.

The digital terminal 1 of Figure 1 comprises a tuner/demodulator 10 which receives a signal S, emanating from a satellite antenna or from a cable network, and which outputs a digital data stream transmitted in the form of packets, and referred to as the TS (standing for "Transport Stream") in the aforesaid MPEG 2 standard, and containing the services supplied by providers.

The data stream TS comprises, in a known manner, packets of data supplied by various service providers and, so as to guarantee that the data reach only those users having acquired the right to receive them (for

example by means of a subscription to the service), these data are transmitted whilst being scrambled by control words CW.

In order to descramble the data, the service provider also supplies the users with the control words having served to scramble the data. So as to keep the control words secret, they are supplied after having been encrypted with an algorithm with key K. The various encrypted control words are sent to the users in control messages, commonly denoted ECMs (the abbreviation ECM standing for "Entitlement Control Message") transmitted in the data stream TS. The control words are thereafter decrypted in a secure processor containing the key K, the secure processor being included within a security element, for example a smart card, which is supplied to the users.

Returning to Figure 1, TS(D.EMB.) therefore denotes the data stream TS containing the data in scrambled form. In accordance with the principle defined in the aforesaid standard EN 50221, all the elements of the conditional access system which are specific to the service provider are contained in the detachable module 2 which receives the data stream TS(D.EMB.) from the digital terminal 1 across the DVB-CI common interface.

The module 2 comprises a microcontroller 21, in which the access control software application CA specific to the service provider is executed. It furthermore comprises a component 22 referred to as demultiplexer which receives the data stream TS(D.EMB.) so as to extract therefrom the video or audio data packets corresponding to a service which the user wishes to view or so as to extract therefrom data packets containing so-called "service" information, such as control messages ECM. The video or audio data packets are sent to a descrambler 23 contained in the module 2 whilst the messages ECM are sent to a smart card 3 which has been inserted into the module 2 and which contains, in a

secure processor 30, the key K having served to encrypt the control words. The decryption of the control words contained in the messages ECM is performed by the secure processor 30 which outputs the control words CW unenciphered to the descrambler 23 situated in the module 2. The descrambler 23 is thus in a position to descramble the video or audio data packets received from the demultiplexer 22 by virtue of the control words CW which it receives from the smart card 3. It outputs a digital data stream TS(D.DES.) in which the data packets corresponding to the service which has been selected by the user are descrambled.

The data stream TS(D.DES.) is transmitted to the digital terminal 1 via the DVB-CI common interface. It is more particularly transmitted to an MPEG decoder 14 of the terminal which supplies the audio and video outputs of the terminal which can be read directly by an apparatus such as a television.

The terminal 1 also comprises a microcontroller 11 in which the various software applications of the terminal are executed.

The DVB-CI common interface in fact comprises two logic interfaces:

- the first, the interface of the data stream ITTS, constitutes a bi-directional bus and transports the digital data packets of the TS stream in both directions between the terminal 1 and the module 2 according to the MPEG 2 transport standard. From the terminal to the module, the stream TS(D.EMB.) transmitted via the ITTS interface is a scrambled data stream whilst in the other direction stream TS(D.DES)), and on condition that the module 2 allows access to the data selected by the user (that is to say that it contains the elements of the conditional access system of the service provider which are necessary for descrambling the said data), the packets containing the selected data are returned

descrambled whilst the remainder of the TS stream remains unchanged;

- the second, the command interface ITCOM, transmits commands in both directions between the terminal 1 and the module 2 (more particularly between the microcontrollers 11 and 21) by way of the objects (or primitive functionalities) defined in the standard and which were mentioned above.

A notable drawback of the system just described is that certain data flow unenciphered at the DVB-CI common interface level (in the stream TS(D.DES.). In actual fact, data broadcasters are becoming increasingly preoccupied by illicit copies which may be made from the data which these broadcasters transmit, all the more so when these data are transmitted in digital form as is the case in the present instance, and they are asking for means of protection against copying to be set in place.

The current DVB-CI common interface cannot guarantee this protection against copying since, the module 2 being detachable, it is possible for a pirate to connect a digital recorder to a connection port across which the stream TS(D.DES.) travels and to record the data packets which flow unenciphered.

A purpose of the present invention is to solve the aforesaid problems by providing means of ensuring protection against copying at the level of the common interface between a digital terminal and a module which are linked together by an interface of the DVB-CI type.

The invention therefore relates to a multimedia digital terminal intended for receiving a stream of digital data scrambled by control words, the control words being contained in the stream in encrypted form, and intended to cooperate with a detachable module for descrambling the data stream. The terminal is able to transmit the scrambled data stream to the detachable module. According to the invention, the terminal is furthermore capable of receiving from the detachable

module the decrypted control words, and it comprises a descrambler capable of descrambling the digital data stream by using the control words received from the detachable module.

The descrambling of the data is therefore performed solely in the decoder and no data item now travels unenciphered at the level of the interface between the terminal and the detachable module. The risks of illicit copies are therefore considerably reduced by virtue of the invention.

According to a preferred embodiment of the invention, the digital terminal is furthermore able to receive from the detachable module the scrambled digital data stream, wherein the data stream received by the terminal is not modified relative to the data stream transmitted by the terminal.

According to another embodiment, the digital terminal is able to receive from the detachable module the scrambled digital data stream from which, relative to the data stream transmitted by the terminal, the data packets containing the control words have been removed.

According to another aspect of the invention, the terminal is able to transmit the scrambled data stream to the detachable module across a first interface with the detachable module, and it is furthermore capable of receiving from the detachable module the decrypted control words across a second interface with said module.

According to another particular characteristic of the invention, the terminal is furthermore able to receive from the detachable module, across the first interface, the scrambled digital data stream.

The invention also relates to a multimedia digital terminal intended for receiving a stream of digital data scrambled by control words, the stream of data containing the control words encrypted using a first key, and intended to cooperate with a detachable module for descrambling the data stream. The terminal is able to

transmit the scrambled data stream to the detachable module across a first interface with the detachable module. According to the invention, the terminal is furthermore capable of receiving from the detachable module the decrypted control words which are encrypted using a second key before being transmitted across a second interface with the module. The terminal also comprises means for decrypting the control words received from the detachable module using the second key; and a descrambler capable of descrambling the digital data stream by using the decrypted control words.

Thus, in addition to the data which travel at the level of the first interface between the module and the terminal only in scrambled form, the control words are also encrypted so as to travel at the level of the second interface, thereby further increasing the security of the assembly.

The invention also relates to a module intended for cooperating with a digital terminal as described above, this module being able to receive from the terminal a scrambled digital data stream. According to another aspect of the invention, the module is furthermore capable of extracting from the data stream the control words having served to scramble the digital data; of decrypting the control words; and of transmitting the decrypted control words (CW) to the terminal.

According to another aspect of the invention, the module is furthermore adapted for returning the scrambled digital data stream to the terminal without modifying the stream.

According to yet another aspect of the invention, the module is furthermore adapted for returning the scrambled digital data stream to the terminal by removing, relative to the data stream transmitted by the terminal, the data packets containing the control words.

According to another characteristic of the invention, the module is able to receive the digital data stream across a first interface with the terminal, and it is furthermore capable of transmitting the decrypted control words to the terminal across a second interface with the terminal.

According to a particular embodiment of the invention, the module is able to cooperate with a detachable security element for decrypting the control words, the module being capable of extracting from the digital data stream messages containing the encrypted control word; of transmitting the messages to a security element inserted into the module; of receiving from the security element the decrypted control words; and of transmitting the decrypted control words to the digital terminal with which it cooperates.

The invention also relates to a module intended for cooperating with a digital terminal as described above, the module being able to receive from the terminal a scrambled digital data stream across a first interface with the terminal. According to the invention, the module is furthermore capable of extracting from the data stream the control words having served to scramble the digital data; of decrypting the control words and encrypting the control words using a second key; and of transmitting the encrypted control words to the terminal across a second interface with said terminal.

The invention also relates to a method for descrambling a stream of digital data, scrambled by control words, which is received by a multimedia digital terminal, the control words being contained in the stream in encrypted form. The method comprises a first step consisting in transmitting the scrambled data stream to a detachable module. It furthermore comprises the steps consisting, for the detachable module, in extracting from the data stream the control words having served to scramble the digital data; in decrypting said control

words; and in transmitting the decrypted control words to the terminal.

The invention also relates to a method for descrambling a stream of digital data, scrambled by control words, which is received by a multimedia digital terminal, the stream of data containing the control words encrypted using a first key. The method comprises a first step consisting in transmitting the scrambled data stream to a detachable module. According to the invention, it furthermore comprises the steps consisting, for the detachable module, in extracting from the data stream the control words having served to scramble the digital data; in decrypting the control words; in encrypting the control words with using a second key; and in transmitting the encrypted control words to the terminal. The method furthermore comprises the steps consisting, for the terminal, in decrypting the control words using the second key; and in descrambling the digital data stream by using said decrypted control words.

The invention also relates to a method for transferring control words between a module as described above and a digital terminal also described above. This method consists essentially:

- for the module, in sending a first identification object to the terminal;
- for the terminal, in sending, in response to the first object, a second identification object indicating whether the terminal is or is not able to receive the control words from the module; and
- for the module, in the event of a positive response with the second object, in sending the control words enclosed in a third object.

Other characteristics and advantages of the invention will become apparent on reading a particular, non-limiting embodiment of the invention given with reference to Figures 1 to 4, among which:

- Figure 1, described above, represents a digital terminal into which is plugged a DVB-CI module according to the prior art;
- Figure 2 represents a digital terminal into which is plugged a module according to the principle of the invention;
- Figure 3 diagrammatically represents a part of the common interface between a digital terminal and a module such as those of Figure 2;
- Figure 4 illustrates a protocol for communication across the part of the common interface represented in Figure 3.

Represented in Figure 2 are a digital terminal 1 together with a module 2 connected to the terminal via an interface which is improved relative to the DVB-CI interface so as ensure better protection against copying at the level of this interface.

The elements which are similar to those of Figure 1 described earlier bear the same reference numbers and will not be described further.

In the embodiment of the invention illustrated in Figure 2, it will be considered that the digital terminal 1 is a decoder receiving programmes from various service providers via cable or via a satellite antenna.

A module 2 containing the specific elements of the conditional access system of a first service provider is connected to this decoder.

According to the principle of the invention, the data stream TS'(D.EMB.) leaving the module 2 via the interface ITTS contains only data in scrambled form. The module 2 extracts only the control words CW from the stream TS(D.EMB.) received so as to transmit them, once decrypted, to the decoder. The descrambling of the data is performed only in the decoder 1 by virtue of a descrambler 16 contained in the decoder. Thus, the digital data are no longer available unenciphered at the level of the ITTS interface and illicit copying is, if

not eliminated, at least made much more complex than in the prior art.

To do this, as in the prior art, the module 2 comprises a demultiplexer 22 which extracts the ECM control messages from the data stream TS(D.EMB.) received and which transmits them to a smart card 3 inserted into the module. The secure processor 30 of the smart card decrypts the control words CW contained in the ECM messages and it transmits them to the module 2.

According to a preferred embodiment of the invention, the control words CW are transmitted from the module 2 to the decoder 1 across the control interface ITCOM. The details of the transmission of the control words via the ITCOM interface will be explained later in conjunction with Figures 3 and 4.

Preferably, the data stream TS(D.EMB.) which is received by the module 2 is retransmitted as is to the decoder (link 29) without being modified (TS'(D.EMB) = TS(D.EMB.)). It is received in the decoder by a demultiplexer 15 which extracts the video or audio data packets corresponding to the programme which the user wishes to view and which transmits them to the descrambler 16 so as to be descrambled before being transmitted to the MPEG decoder 14. For this purpose the descrambler 16 receives the control words CW from the module 2 via the ITCOM interface.

According to a first variant embodiment, the module 2 extracts the ECM control messages from the data stream TS(D.EMB.) and replaces them, in the data stream TS'(D.EMB.) transmitted to the decoder, with stuffing packets. This variant is represented diagrammatically via the link 28 shown dashed.

According to a second variant embodiment, the demultiplex 22, contained in the module 2, extracts the video or audio data packets corresponding to the programme which the user wishes to view and it transmits them in the data stream TS'(D.EMB.) so that they are

received directly by the descrambler 16 of the decoder. This variant is represented diagrammatically by the link 27 shown dashed.

Also represented dashed in Figure 2 is a smart card 4 which can be inserted into the decoder 1 and which belongs to the conditional access system of a second service provider. Indeed, the decoder can comprise an integrated conditional access system for accessing the services of the second provider and furthermore comprise several connectors for modules 2 so as to access the services of several other providers.

It is for this reason that the decoder comprises a demultiplexer 15 and a descrambler 16. The access control software application CA' of the second provider is executed in the microcontroller 11. When the user selects a service of the second provider, the stream TS(D.EMB.) is transmitted directly to the demultiplexer 15 via a link 19. This demultiplexer extracts the control messages ECM' and transmits them to the secure processor 40 of the smart card 4 which, with the aid of the key K', decrypts the control words CW' contained in the messages ECM' and sends them unenciphered to the descrambler 16, so as to descramble the services selected by the user.

According to a third variant embodiment of the invention, the data stream TS(D.EMB.) is transmitted from the decoder 1 to the module 2 so that the latter extracts the control words CW and retransmits them unenciphered to the decoder, but unlike the variants mentioned earlier, the stream TS(D.EMB.) is not returned via the ITTS interface to the decoder. Only the control words are transmitted to the decoder after having been decrypted by the module. The stream TS(D.EMB.) is for its part sent directly to the demultiplexer 15 of the decoder via the link 19 inside the decoder.

According to a fourth variant embodiment of the invention, the control words CW are not transmitted unenciphered across the ITCOM interface. They are

encrypted by the microcontroller 21 of the module 2 using a second key, different from the key K used to encrypt the control words upon their transmission in the data stream TS(D.EMB.), before being transmitted over the ITCOM interface. This variant thus offers increased security since now no element travels unenciphered via the interface between the module and the decoder.

The microcontroller 11 of the decoder 1 will therefore have to decrypt, using this second key, the control words received by the ITCOM interface before transmitting them to the descrambler 16.

In a first embodiment of this variant, the module 2 and the decoder 1 generate, before a single control word travels through the ITCOM interface, a session key SSK by using the Diffie Hellman protocol, which is well known to the person skilled in the art. Thereafter, all the control words are encrypted in the module using the session key SSK, then are transmitted to the decoder in this encrypted form across the ITCOM interface before being decrypted, using the session key, in the decoder.

In this embodiment, a different session key is generated each session, that is to say each time the user selects a programme which needs to be descrambled in the module 2.

In a second embodiment of this variant, the decoder 1 and the module 2 each contain a secret key K2 which is stored in a secure area of the decoder or of the module, for example in a secure processor. This secret key is unique for each decoder and if several modules are plugged into the decoder, they all contain the secret key of the decoder.

In this embodiment, the control words are therefore encrypted with the secret key K2 in the module before being transmitted to the decoder via the ITCOM interface; they are then decrypted in the decoder using the key K2.

The principle of the invention is particularly advantageous since it makes it possible to harness the demultiplexer and the descrambler which are already contained in the decoder so as to use them even when the conditional access system of another provider, contained in a detachable module, is used.

It should be stated in this regard that the demultiplexer and the descrambler components have been standardized within the framework of the DVB digital broadcasting standard in particular. Only the conditional access system (access control software, decryption algorithm and key, smart card, etc.) remains a proprietary system of the service provider.

We shall now describe in greater detail, in conjunction with Figures 3 and 4, how the control words CW are transmitted via the command interface ITCOM.

The ITCOM interface between the terminal (decoder) 1 and the module 2 uses a communication protocol which is represented diagrammatically in Figure 3 and which comprises several layers:

- a "Physical" layer (50, 60) which comprises the physical connector and low-level software for initializing the communication;
- a "Link" layer (51, 61) which forms the link between the Physical layer which deals only with bytes (8 bits of data) and the higher layer which can deal with much larger packets of data;
- a "Transport" layer (52, 62) which optimizes the occupation of the data stream by the various session in progress and which conveys the messages from the higher layer to the "Link" layer;
- a "Session" layer (53, 63) which opens, closes and manages the sessions in which the messages of the applications using the ITCOM interface are transmitted.

Represented in Figure 3 are on the one hand the access control application CA 65 which is executed in the microcontroller 21 (cf. Fig. 2) of the module 2 and on

the other hand a software resource 55 called CAS (standing for "Conditional Access Support") of the terminal 1.

This resource CAS defines a certain number of specific objects intended for use by the access control applications of the modules connected to the terminal. It communicates with the four layers of the ITCOM interface across a " Standard API " (the abbreviation API standing for "Application Programming Interface"), the standard API defining other objects which are used by all the resources of the system.

Likewise, the access control application 65 of the module uses the objects defined by the resources of the terminal through a standard API.

It was seen earlier that, according to the principle of the invention, the control words which are decrypted in the module 2 are thereafter transmitted to the terminal 1 across the ITCOM interface. In order that the control words may "cross" the various layers of the ITCOM interface, they must be enclosed in specific objects, comprehensible both to the application CA and to the resource CAS, which will be called "CPTS_CW()" hereinafter. Of course, when the control words are transmitted encrypted with the aid of a second key (SSK or K2) as in the fourth variant set forth above, they are enclosed, in this encrypted form, in the objects CPTS_CW().

Figure 4 illustrates the protocol for communication between the access control application CA of the module and the resource CAS of the terminal which allows, according to the invention, protection against copying.

The time scale has been represented by two downward vertical arrows.

After a first session-opening phase (not represented), the application CA of the module checks that the resource CAS of the terminal does indeed support

protection against copying over the ITCOM interface. To do this, the application CA sends during a step 100 an object "CPTS_identification()" which will be defined later. The resource CAS responds by sending, in step 101, an object "CPTS_identification_answer()" which indicates whether the resource CAS does or does not support protection, against copying. In the event of a positive response, the application CA of the module then regularly sends (steps 102a, 102b, 102i) the control words enclosed in the objects "CPTS_CW()" as and when they are decrypted by the module.

Conversely, in the event of a negative response, the terminal is not considered reliable. Consequently, the control words are not sent to the terminal and the data of the stream TS(D.EMB.) are not descrambled in the terminal. Any appropriate action can be envisaged at that moment (displaying of a message destined for the user by way of the User Interface resource of the terminal for example).

As seen above, it is necessary, in order to implement the protocol of Figure 4, to define additional objects over and above those already envisaged in the existing standards.

Identification objects

The function of the identification objects is to allow an access control application CA of a module supporting protection against copying to check whether the terminal to which the module is connected also supports protection against copying. That is to say, whether the resource CAS of the terminal possesses the functionality of protection against copying.

The first object used is the following:

```
CPTS_identification() {
    CPTS_identification_tag        24 bits   uimsbf
    Length_field() = 0             8 bits    uimsbf
    }
```

The notation used here corresponds to that used in the aforesaid standard EN 50221 in which the objects are generally defined by means of a tag (here the "CPTS_identification_tag"), of a length field ("Length_field()") and of parameters which can take various values.

The CPTS_identification_tag tag is a number defined on 24 bits and the notation "uimsbf" (stemming from "unsigned integer most significant bit first") signifies that this pertains to an unsigned integer whose most significant bits (highest order bits) are always situated first.

The "Length_field()" field defines the length in terms of number of bytes of the parameters forming part of the object. Since here the object "CPTS_identification()" contains no parameter, the length field is equal to zero.

The second object used is the following:

```
CPTS_identification_answer() {
     CPTS_identification_answer_tag     24 bitsuimsbf
     Length_field() = 1
     Identification_result               8 bits  uimsbf
}
```

This "CPTS_identification_answer()" object is used to indicate whether the resource CAS of the terminal does or does not support protection against copying according to the invention. It comprises a "CPTS_identification_answer_tag()" tag and a length field which is equal to 1 since the object also comprises an "Identification_result" parameter defined on 8 bits. This parameter is for example a Boolean indicating whether or not protection against copying is supported by the resource CAS.

Other parameters can be envisaged, for example to indicate a version number of the copy protection.

Contro- word transmission objects

These objects enclose the control words which are decrypted in the module. They allow the access control application CA of the module to send them, across the various layers of the ITCOM interface, to the resource CAS of the terminal which can thereafter utilize them by transmitting them to the descrambler 16 (Fig. 2).

These objects have the following format:

```
CPTS_CW()  {
    CPTS_CW_tag                  24 bits uimsbf
    Length_field()
    MPEG2_stream_type             8 bits uimsbf
    MPEG2_pid                    16 bits uimsbf
    Odd_CW                      128 bits uimsbf
    Even_CW                     128 bits uimsbf
}
```

They comprise a "CPTS_CW_tag" tag, a length field "Length_field()" and parameters identifying:

- the type of data packet transported (video, audio or other data), in "MPEG2_stream_type" defined on 8 bits;
- the PID (standing for "Programme Identifier"), that is to say the programme identifier associated with the packet transported in "MPEG2_pid", defined on 16 bits;
- the odd ("Odd_CW") and even ("Even_CW") control words defined on 128 bits each.

Indeed, it is well known that a succession of even and odd control words is transmitted in the TS data stream, each control word being transmitted in advance relative to the data packets which are scrambled with this control word. The descrambler therefore continuously memorizes the even control word serving to descramble the

current data packet and the odd control word serving to descramble the next packet (or vice versa).

The "CPTS_CW()" object comprises, in a first embodiment, parameters making it possible to send both an even control word (in "Even_CW") and an odd control word (in "Odd_CW"). It can also comprise, in another embodiment, a parameter "CW", on 128 bits, containing the control word and a parameter "Type_CW" on 8 bits, defining the type, even or odd, of the control word transmitted.

Of course, the invention is not limited to the exemplary embodiments which are mentioned hereinabove. In particular, the person skilled in the art will be able to introduce any variant into the definition of the identification objects and control-word transmission objects by adding other parameters to these objects.

Moreover, although the invention has been described with reference to the DVB-CI standard it is not limited to the framework of this standard. The invention can in particular be advantageously applied within the framework of the American NRSS (standing for "National Renewable Security Standard") standard.

CLAIMS

1. Multimedia digital terminal (1) intended for receiving a stream (TS(D.EMB.)) of digital data scrambled by control words (CW), said control words being contained in said stream (TS(D.EMB.)) in encrypted form, and intended to cooperate with a detachable module (2) for descrambling said data stream,

said terminal being able to transmit the scrambled data stream (TS(D.EMB.)) to the detachable module,

characterized in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW), and

in that it comprises a descrambler (16) capable of descrambling the digital data stream by using the control words (CW) received from the detachable module (2).

2. Digital terminal according to Claim 1, characterized in that it is furthermore able to receive from the detachable module (2) the scrambled digital data stream (TS'(D.EMB.)), said data stream received by the terminal not being modified relative to the data stream (TS(D.EMB.)) transmitted by the terminal.

3. Digital terminal according to Claim 1, characterized in that it is furthermore able to receive from the detachable module (2) the scrambled digital data stream (TS'(D.EMB.)) from which, relative to the data stream (TS(D.EMB.)) transmitted by the terminal, the data packets containing the control words (CW) have been removed.

4. Digital terminal according to one of Claims 1 to 3, characterized in that said terminal is able to transmit the scrambled data stream (TS(D.EMB.)) to the

detachable module across a first interface (ITTS) with said detachable module, and

in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW) across a second interface (ITCOM) with said module.

5. Terminal according to Claim 4, in combination with Claims 2 and 3, characterized in that it is furthermore able to receive from the detachable module (2), across said first interface (ITTS), the scrambled digital data stream (TS'(D.EMB.)).

6. Multimedia digital terminal (1) intended for receiving a stream (TS(D.EMB.)) of digital data scrambled by control words (CW), said stream of data (TS(D.EMB.)) containing the control words encrypted using a first key (K), and intended to cooperate with a detachable module (2) for descrambling said data stream,

said terminal being able to transmit the scrambled data stream (TS(D.EMB.)) to the detachable module across a first interface (ITTS) with said detachable module,

characterized in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW) which are encrypted using a second key (SSK, K2) before being transmitted across a second interface (ITCOM) with the module (2), and

in that it comprises:

- means for decrypting said control words received from the detachable module using said second key (SSK, K2); and
- a descrambler (16) capable of descrambling the digital data stream (TS(D.EMB.)) by using said decrypted control words (CW).

7. Module (2) intended for cooperating with a digital terminal according to Claim 1, said module being

able to receive from the terminal a scrambled digital data stream (TS(D.EMB.)), characterized in that said module is furthermore capable of:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- transmitting the decrypted control words (CW) to said terminal.

8. Module according to Claim 7, characterized in that it is furthermore adapted for returning the scrambled digital data stream (TS'(D.EMB.)) to the terminal without modifying said stream.

9. Module according to Claim 7, characterized in that it is furthermore adapted for returning the scrambled digital data stream (TS'(D.EMB.)) to the terminal by removing, relative to the data stream (TS(D.EMB.)) transmitted by the terminal, the data packets containing the control words.

10. Module according to one of Claims 7 to 9, characterized in that it is able to receive the digital data stream (TS(D.EMB.)) across a first interface (ITTS) with said terminal (1), and

in that it is furthermore capable of transmitting the decrypted control words to said terminal across a second interface (ITCOM) with said terminal.

11. Module according to one of Claims 7 to 10, characterized in that it is able to cooperate with a detachable security element (3) for decrypting the control words, said module being capable of:

- extracting from the digital data stream (TS(D.EMB.)) messages (ECM) containing the encrypted control words;

- transmitting said messages (ECM) to a security element (3) inserted into said module;
- receiving from said security element (3) the decrypted control words (CW); and
- transmitting the decrypted control words to the digital terminal (1) with which it cooperates.

12. Module (2) intended for cooperating with a digital terminal according to Claim 6, said module being able to receive from the terminal a scrambled digital data stream (TS(D.EMB.)) across a first interface (ITTS) with the terminal (1), characterized in that said module is furthermore capable of:
- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- encrypting said control words using the second key (SSK, K2); and
- transmitting said encrypted control words (CW) to the terminal across a second interface (ITCOM) with said terminal.

13. Module according to one of Claims 10 or 12, characterized in that it pertains to a module according to the DVB-CI standard and in that the first interface (ITTS) of the module is the interface of the transport stream according to the MPEG-2 standard and the second interface (ITCOM) is the control interface.

14. Method for descrambling a stream (TS(D.EMB.)) of digital data, scrambled by control words (CW), which is received by a multimedia digital terminal (1), said control words (CW) being contained in said stream in encrypted form, the method comprising a first step consisting in:

transmitting the scrambled data stream (TS(D.EMB.)) to a detachable module (2),

characterized in that it furthermore comprises the steps consisting, for the detachable module (2), in:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- transmitting the decrypted control words (CW) to said terminal.

15. Method for descrambling a stream (TS(D.EMB.)) of digital data, scrambled by control words (CW), which is received by a multimedia digital terminal (1), said stream of data containing said control words (CW) encrypted using a first key (K), the method comprising a first step consisting in:

transmitting the scrambled data stream (TS(D.EMB.)) to a detachable module (2),

characterized in that it furthermore comprises the steps consisting, for the detachable module (2), in:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words;
- encrypting said control words using a second key (SSK, K2); and
- transmitting the encrypted control words (CW) to said terminal; and,

for the terminal (1), in:

- decrypting said control words using the second key (SSK, K2); and
- descrambling the digital data stream by using said decrypted control words.

16. Method for transferring control words (CW) between a module according to one of Claims 7 to 13 and a

digital terminal according to one of Claim 1 to 6, characterized in that it comprises the steps consisting:

- for the module (2), in sending (100) a first identification object ("CPTS_identification()") to the terminal (1);
- for the terminal (1), in sending (101), in response to said first object, a second identification object ("CPTS_identification_answer()") indicating whether the terminal is or is not able to receive the control words from the module (2); and
- for the module (2), in the event of a positive response with said second object, in sending (102a, 102b, 102i) said control words (CW) enclosed in a third object ("CPTS_CW()").

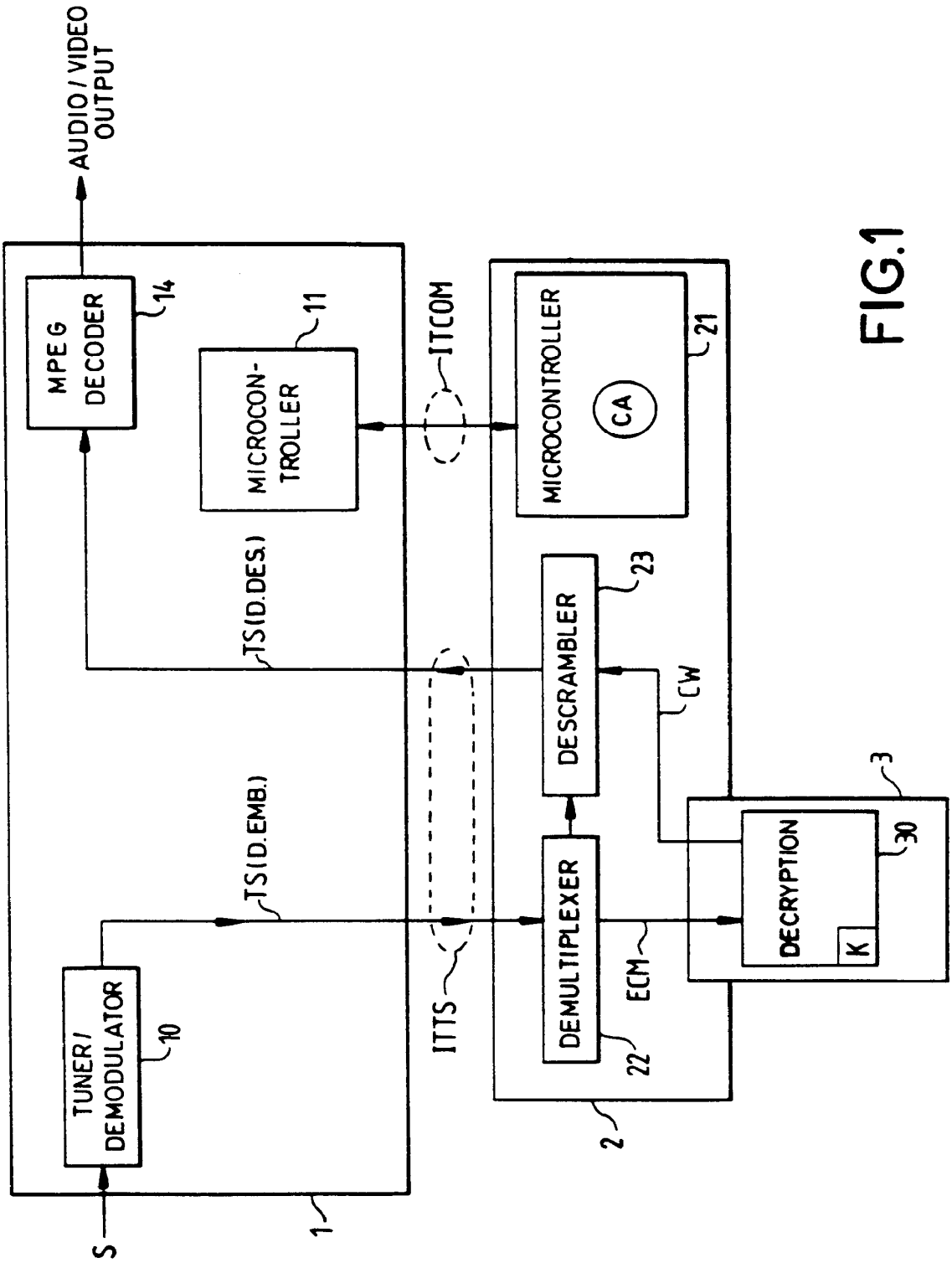

AUDIO / VIDEO OUTPUT
MPEG DECODER
14
MICROCON-TROLLER
11
ITCOM
MICROCONTROLLER
CA
21
TS(D.DES.)
DESCRAMBLER
23
CW
TS(D.EMB.)
DEMULTIPLEXER
ECM
DECRYPTION
K
30
3
ITTS
22
TUNER / DEMODULATOR
10
S
1
2

FIG.1

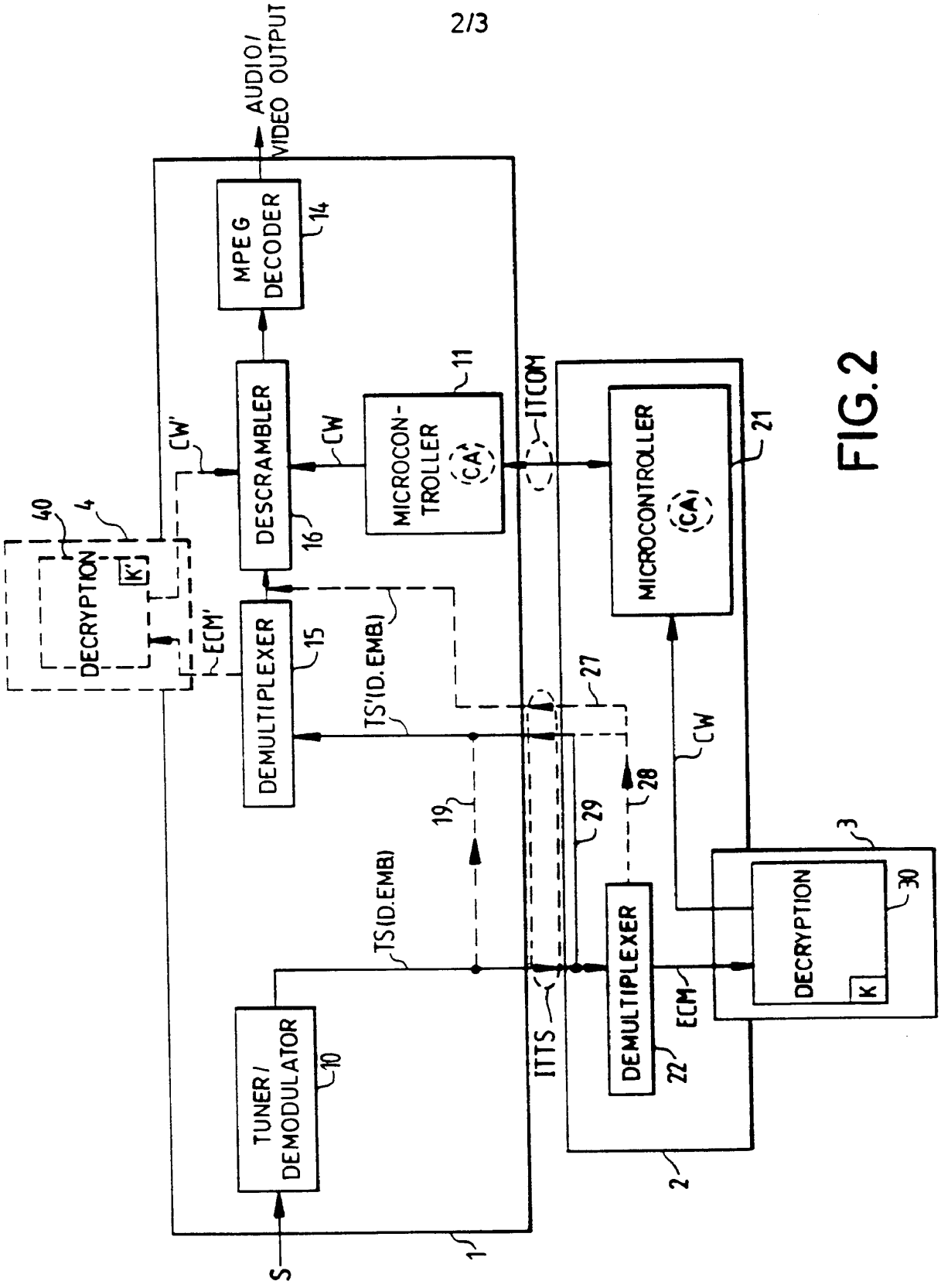

AUDIO/
VIDEO OUTPUT
MPEG
DECODER
14
DESCRAMBLER
16
CW'
CW
MICROCON-
TROLLER
(CA)
11
ITCOM
MICROCONTROLLER
(CA)
21
DECRYPTION
K'
40
4
ECM'
DEMULTIPLEXER
15
TS'(D.EMB)
27
CW
28
29
19
TS(D.EMB)
DEMULTIPLEXER
22
ECM
DECRYPTION
K
30
3
ITTS
TUNER/
DEMODULATOR
10
S
1
2

FIG.2

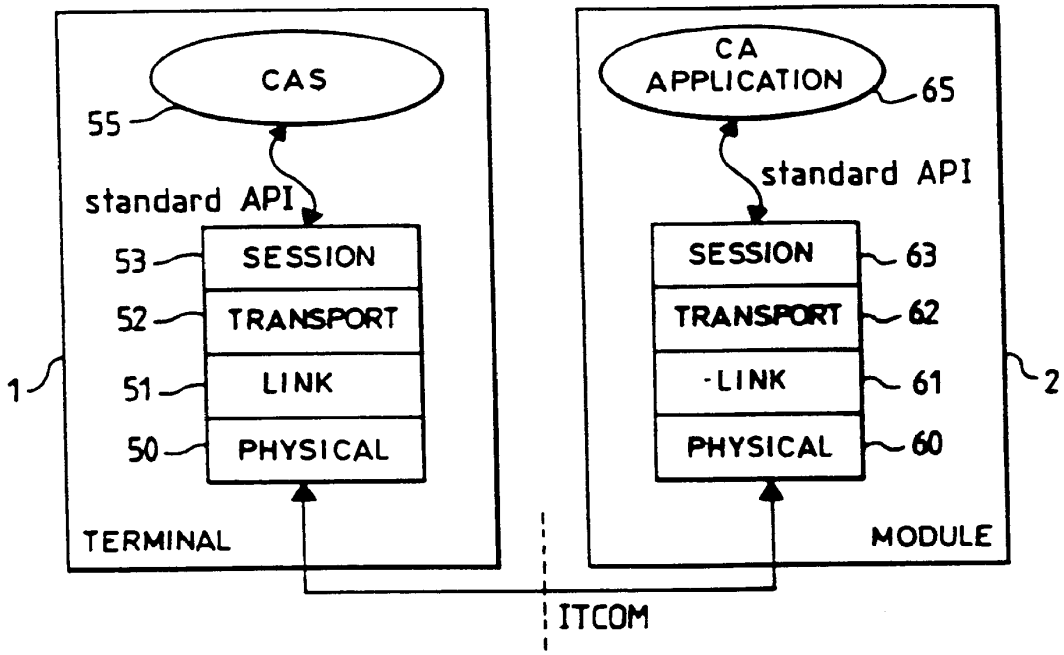

CAS
55
standard API
53
SESSION
52
TRANSPORT
51
LINK
50
PHYSICAL
1
TERMINAL
CA APPLICATION
65
standard API
SESSION
63
TRANSPORT
62
LINK
61
PHYSICAL
60
2
MODULE
ITCOM

FIG.3

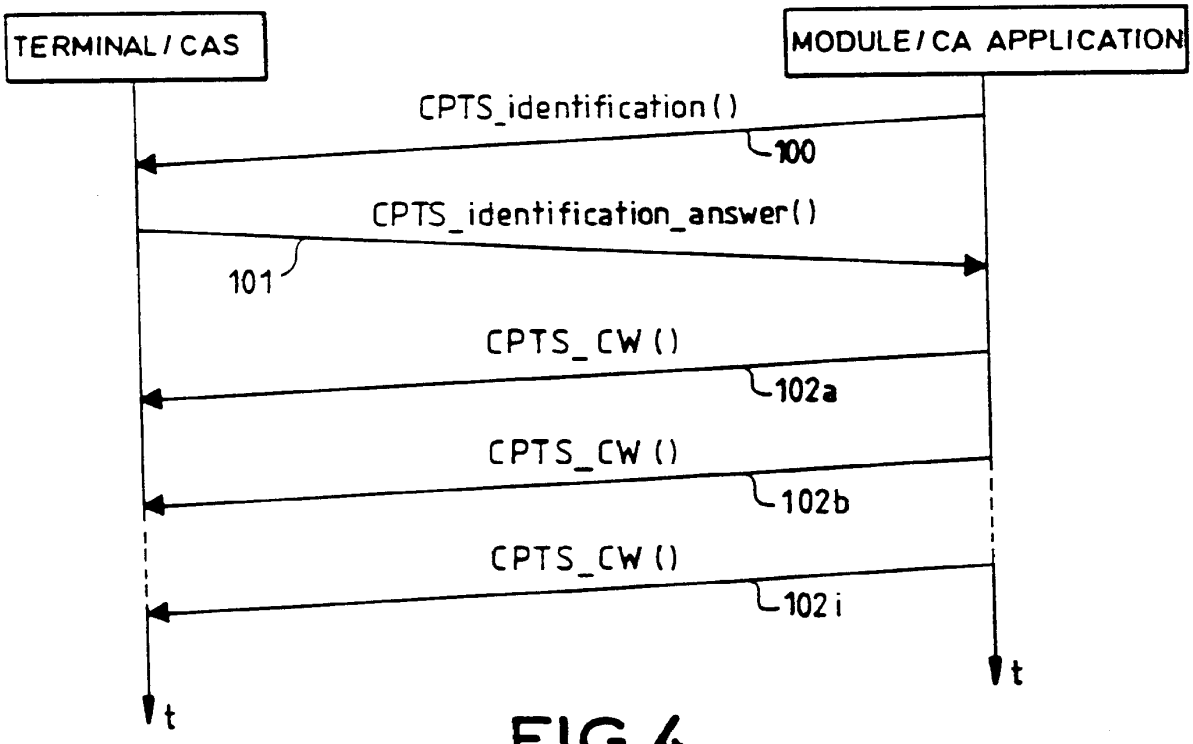

TERMINAL / CAS
MODULE / CA APPLICATION
CPTS_identification()
100
CPTS_identification_answer()
101
CPTS_CW()
102a
CPTS_CW()
102b
CPTS_CW()
102i
t
t

FIG.4

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/EP 00/08439

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/00 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 923 245 A (SONY UK LTD) 16 June 1999 (1999-06-16) page 3, column 4, line 19 -page 7, column 11, line 10 figures 1-7	1-15
A	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 (1996-02-29) page 6, line 1 -page 19, line 16 figures 1-4	1-15

-/--

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

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 December 2000	14/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/EP 00/08439

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 706 291 A (NEWS DATACOM LTD) 10 April 1996 (1996-04-10) page 2, column 2, line 47 -page 3, column 3, line 19 page 5, column 8, line 12 - line 50 page 6, column 9, line 47 -column 10, line 30 figures 1-3	1,6,7, 14,15

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Interr. nal Application No
PCT/EP 00/08439

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0923245 A	16-06-1999	GB 2332345 A	16-06-1999
		JP 11331801 A	30-11-1999
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		DE 69514843 D	02-03-2000
		DE 69514843 T	18-05-2000
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		ES 2141371 T	16-03-2000
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
EP 0706291 A	10-04-1996	IL 111151 A	24-09-1998
		AU 696725 B	17-09-1998
		AU 3303695 A	18-04-1996
		CA 2159779 A	04-04-1996
		JP 8214278 A	20-08-1996
		US 5666412 A	09-09-1997
		US 5774546 A	30-06-1998
		US 5878134 A	02-03-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
11 octobre 2001 (11.10.2001)

PCT

(10) Numéro de publication internationale
WO 01/75876 A1

(51) Classification internationale des brevets[7] : G11B 20/00, H04L 29/06

(21) Numéro de la demande internationale : PCT/FR01/00572

(22) Date de dépôt international : 28 février 2001 (28.02.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/04222 31 mars 2000 (31.03.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THOMSON MULTIMEDIA** [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventeurs; et

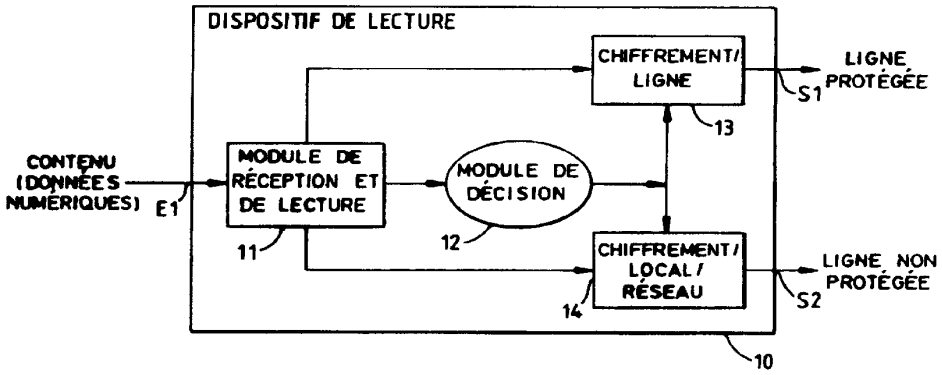
(75) Inventeurs/Déposants *(pour US seulement)* : **DIEHL, Eric** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **ANDREAUX, Jean-Pierre** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **FURON, Teddy** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **CHEVREAU, Sylvain** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Mandataire : **KOHRS, Martin**; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

[Suite sur la page suivante]

(54) Title: DEVICE FOR READING, RECORDING AND RESTORING DIGITAL DATA IN A COPY-PROTECTION SYSTEM FOR SAID DATA

(54) Titre : DISPOSITIFS DE LECTURE, D'ENREGISTREMENT ET DE RESTITUTION DE DONNEES NUMERIQUES DANS UN SYSTEME DE PROTECTION CONTRE LA COPIE DESDITES DONNEES



10...READING DEVICE
13...LINE ENCRYPTION
S1...PROTECTED LINE
S2...UNPROTECTED LINE
14...LOCAL NETWORK ENCRYPTION
12...DECISION MODULE
11...RECEIVING AND READING MODULE
E1...CONTENTS (DIGITAL DATA)

(57) Abstract: The invention concerns a device for reading digital data (10) receiving data representing a content designed to be connected to a digital home network. It comprises: first means for encrypting (13) data in accordance with a protection mode specific to a line whereby the device is to be connected to another digital network device, the encrypted data being in that case supplied to a first output (S1); and second means for encrypting (14) data in accordance with a mode specific to the home network, the encrypted data being in that case supplied to a second output (S2). The invention also concerns a device for recording and restoring digital data designed to be connected to said reading device (10).

[Suite sur la page suivante]

WO 01/75876 A1

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le dispositif de lecture de données numériques (10) recevant des données représentant un contenu est destiné à être raccordé à un réseau numérique domestique. Il comporte: un premier moyen de chiffrement (13) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie (S1); et un deuxième moyen de chiffrement (14) des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie (S2). L'invention concerne également un dispositif d'enregistrement et un dispositif de restitution de données numériques destinés à être raccordés à ce dispositif de lecture (10).

Dispositifs de lecture, d'enregistrement et de restitution de données numériques dans un système de protection contre la copie desdites données

Domaine de l'invention

L'invention se rapporte d'une manière générale au domaine de la protection contre la copie de données numériques, plus particulièrement dans un environnement de réseau numérique domestique.

Etat de la technique

Un réseau numérique domestique peut véhiculer des données numériques issues de différentes sources extérieures au réseau. Il peut s'agir de données stockées sur des supports détachables tels que des disques optiques, par exemple des disques DVD (de l'anglais "*Digital Versatile Disc*" signifiant littéralement "*Disque Numérique Polyvalent*"), ou des bandes magnétiques, les supports étant soit pré-enregistrés, soit enregistrables.

Il peut aussi s'agir de données diffusées puis injectées sur le réseau numérique domestique, par exemple des signaux de télévision numérique diffusés par satellite, par le câble ou encore par des réseaux numériques hertziens. Les données peuvent également être téléchargées en provenance de l'Internet.

Enfin, un réseau numérique domestique peut en outre être amené à gérer des données numériques stockées localement, par exemple dans un disque dur relié au réseau domestique.

Ces données numériques peuvent être séparées en deux grandes catégories: d'une part les données qui ne nécessitent pas de protection particulière (par exemple, celle qui relèvent d'une création personnelle de l'utilisateur du réseau domestique) et d'autre part les données qui doivent être protégées contre la copie pour garantir les intérêts de leur créateur (film, musique, jeux, etc.).

Divers mécanismes et possibilités existent actuellement pour protéger des données numériques contre une copie illégitime.

Les deux principales techniques de protection sont actuellement:

- le chiffrement des données, qui consiste à transformer des données intelligibles (ou "claires") en données chiffrées ou embrouillées à l'aide d'une clé, cette clé étant soit une clé secrète partagée par le dispositif qui chiffre les données et par celui qui est autorisé à les déchiffrer, soit dans les systèmes de cryptographie asymétrique une clé privée ou publique;

- le tatouage des données, qui consiste à insérer de manière non perceptible un tatouage (communément appelé "Watermark") attaché aux données à protéger. Le tatouage doit être non-modifiable et non effaçable même en cas de transformation des données à protéger.

Les deux techniques ci-dessus peuvent naturellement être associées en combinant le tatouage et le chiffrement des données.

Par ailleurs, les données numériques diffusées sont le plus souvent protégées dans le cadre d'un système à accès conditionnel. Dans ce type de système, les données fournies par différents prestataires de services sont transmises sous forme embrouillée par des mots de contrôle CW (de l'anglais "*Control Word*") afin de garantir que les données ne parviennent qu'aux utilisateurs ayant acquis le droit de les recevoir (par exemple moyennant un abonnement au service). Les mots de contrôle sont eux-mêmes transmis dans le flux de données diffusées après avoir été chiffrés avec un algorithme de clé K, cette clé K étant contenue dans un processeur sécurisé, par exemple inclus dans une carte à puce, qui est fournie aux utilisateurs par le prestataire de service pour leur permettre de déchiffrer les mots de contrôle et donc de désembrouiller les données.

Dans les réseaux numériques domestiques, deux grandes méthodes ont été proposées jusqu'à présent pour utiliser et combiner ces techniques de protection:

- la première méthode consiste à protéger les données qui doivent l'être en les chiffrant / embrouillant localement d'un bout à l'autre du réseau (on parle en général de "*end-to-end protection*" – signifiant littéralement "protection d'un bout à l'autre"), c'est à dire dès leur entrée en un point du réseau jusqu'au moment où elle sont restituées à l'utilisateur (affichage de vidéo sur un écran de téléviseur, diffusion de musique par un haut-parleur, etc.), tous les appareils du réseau utilisant le même type de protection, spécifique au réseau domestique. Les données ne sont donc jamais disponibles en clair dans le réseau, que ce soit sur le bus numérique reliant les appareils entre eux ou dans les appareils eux-même, sauf au moment ultime de leur restitution, généralement sous forme analogique, à l'utilisateur ;

- la seconde méthode consiste à associer une protection locale à chaque type d'appareil du réseau (un type de chiffrement particulier, un système d'accès conditionnel, etc.) avec une "protection de ligne" (ou protection "point-à-point"); dans ce type de méthode, les données sont disponibles en clair à l'intérieur des appareils mais ne sont jamais disponibles en clair sur le bus

numérique reliant les différents appareils du réseau entre eux; les données sont en effet re-chiffrées avant d'être transmises sur le bus.

Exposé de l'invention

Un but de la présente invention est de proposer un système permettant de concilier les différentes méthodes de protection qui ont été proposées jusque là.

L'invention concerne à cet effet un dispositif de lecture de données numériques destiné à être raccordé à un réseau numérique domestique et susceptible de recevoir des données représentant un contenu. Celui-ci comporte, selon l'invention :

- un premier moyen de chiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie; et

- un deuxième moyen de chiffrement des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie.

Selon une caractéristique avantageuse de l'invention, le dispositif comporte en outre un module de décision adapté à délivrer une permission ou une interdiction de copie et/ ou de lecture desdites données numériques, lesdites données numériques étant fournies au premier ou au deuxième moyen de chiffrement lorsque ledit module de décision délivre une interdiction de copie ou une permission de copie unique.

Selon une autre caractéristique avantageuse de l'invention, lesdites données numériques sont fournies directement à la première et/ou à la deuxième sortie sans être chiffrées lorsque ledit module de décision délivre une permission de copie illimitée.

Selon une autre caractéristique particulière de l'invention, le dispositif ne fournit aucune données numérique à la première ni à la deuxième sortie lorsque ledit module de décision délivre une interdiction de lecture.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une permission de copie illimitée lorsque lesdites données numériques reçues ne sont pas chiffrées.

Selon une caractéristique préférée de l'invention, le module de décision délivre une permission de copie illimitée lorsqu'en outre lesdites données numériques reçues ne sont pas tatouées.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de lecture lorsque à la fois lesdites données numériques reçues ne sont pas chiffrées et sont tatouées.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de copie lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type enregistrable; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de lecture lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type enregistrable; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une permission de copie unique lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type non-enregistrable ou que ce sont des données diffusées ou téléchargées; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de copie lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type non-enregistrable ou que ce sont des données diffusées ou téléchargées; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

Selon encore une autre caractéristique avantageuse de l'invention, les informations de permission ou d'interdiction de copie et/ ou de lecture desdites données numériques délivrées par le module de décision sont attachées aux données fournies à la première ou à la deuxième sortie.

Selon un mode de réalisation particulier de l'invention, la première et la deuxième sortie sont reliées respectivement à un unique connecteur pour raccorder le dispositif à un bus numérique du réseau domestique, ledit bus fonctionnant dans un premier mode protégé lorsque les données sont issues de la première sortie et dans un second mode non protégé lorsque les données sont issues de la deuxième sortie.

Avantageusement, le choix de la première ou de la deuxième sortie pour fournir les données est déterminé par le dispositif raccordé au réseau

numérique domestique destiné à recevoir lesdites données émises par le dispositif de lecture sur le réseau domestique.

L'invention concerne également un dispositif d'enregistrement de données numériques destiné à être raccordé à un dispositif de lecture tel que ci-dessus par l'intermédiaire d'un réseau numérique domestique. Selon l'invention, ce dispositif d'enregistrement comporte :

- une première entrée destinée à recevoir des données qui ont été fournies à la première sortie du dispositif de lecture; et
- une seconde entrée destinée à recevoir des données qui ont été fournies à la deuxième sortie du dispositif de lecture.

Selon une caractéristique particulière de l'invention, le dispositif d'enregistrement comporte un moyen de déchiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture, ledit moyen de déchiffrement étant relié à la première entrée du dispositif d'enregistrement.

Selon une autre caractéristique particulière de l'invention, le dispositif d'enregistrement comporte en outre un module de décision adapté à analyser les informations de permission ou d'interdiction de copie et/ou de lecture attachées aux données à enregistrer. Le dispositif d'enregistrement délivre les données à enregistrer à une sortie lorsque le module de décision détecte une permission de copie. Par contre, le dispositif d'enregistrement ne délivre aucune donnée à enregistrer à ladite sortie lorsque le module de décision détecte une interdiction de copie.

L'invention concerne aussi un dispositif de restitution de données numériques destinés à être raccordés à un dispositif de lecture tel que ci-dessus par l'intermédiaire d'un réseau numérique domestique. Selon l'invention, ce dispositif comporte :

- une première entrée destinée à recevoir des données qui ont été fournies à la première sortie du dispositif de lecture et qui est reliée à un premier moyen de déchiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture ; et
- une seconde entrée destinée à recevoir des données qui ont été fournies à la deuxième sortie dudit dispositif de lecture et qui est reliée à un deuxième moyen de déchiffrement des données selon un mode de protection spécifique au réseau domestique.

Brève description des dessins

L'invention sera mieux comprise à la lecture de la description suivante d'un mode de réalisation particulier, non limitatif, de celle-ci faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente un réseau numérique domestique servant à illustrer le principe de l'invention ;
- la figure 2 représente un dispositif de lecture de données numériques selon l'invention destiné à être raccordé à un réseau domestique;
- la figure 3 représente un dispositif d'enregistrement de données numériques selon l'invention destiné à être raccordé à un réseau domestique;
- la figure 4 représente un dispositif de restitution de données numériques destiné à être raccordé à un réseau domestique;
- la figure 5 illustre un procédé mis en œuvre dans le dispositif de la figure 2 ; et
- la figure 6 illustre un procédé mis en œuvre dans le dispositif de la figure 3.

Description détaillée de modes de réalisation de l'invention

Sur la figure 1, on a représenté un exemple de réseau numérique domestique. Celui-ci se compose d'un certain nombre de dispositifs reliés entre eux par un bus numérique B, par exemple un bus selon la norme IEEE 1394. Ces dispositifs peuvent être divisés en trois catégories :

- les dispositifs de lecture qui sont capables de recevoir des données numériques en provenance de différentes sources de données; sur la figure 1, deux exemples de ces dispositifs sont représentés: le décodeur 1 recevant des données d'une antenne satellite 6, notamment des programmes de télévision numérique, et le lecteur DVD 2 capable de lire des disques DVD 5 ;
- les dispositifs d'enregistrement de données, tel le dispositif 3, qui sont capables d'enregistrer le contenu des données lues par les dispositifs de lecture sur des supports d'enregistrement persistants ; et
- les dispositifs de restitution, tel le téléviseur numérique 4 de la figure 1, qui sont prévus pour restituer le contenu de données lues par un dispositif de lecture.

Bien entendu, cette séparation entre les trois catégories de dispositifs est faite pour les besoins de simplification de l'explication et un appareil d'électronique grand public réel peut très bien regrouper deux catégories de dispositifs décrits ci-dessus, voire les trois. Par exemple, un

téléviseur numérique peut contenir aussi le dispositif de lecture des émissions diffusées sous forme numérique ou bien un lecteur de DVD peut aussi contenir un dispositif d'enregistrement.

Sur la figure 2, on a représenté un dispositif de lecture 10 selon l'invention. Celui-ci reçoit sur son entrée E1 des données numériques représentant un contenu. Ce contenu peut être un contenu pré-enregistré, un contenu enregistré dans le réseau, un contenu diffusé ou un contenu téléchargé. Les données numériques sont reçues par un module de réception et de lecture 11 qui est capable d'interpréter le format des données reçues. En fait ce module est différent selon le type d'appareil appartenant à la première catégorie. Ce module a des fonctions dédiées selon le type de contenu qu'il reçoit: ainsi, si le dispositif de lecture est un lecteur de DVD Vidéo, le module 11 reconnaîtra le format de données embrouillées selon le système CSS (de l'anglais "*Content Scramble System*" signifiant littéralement "*Système d'Embrouillage de Contenu*") utilisé habituellement pour protéger le contenu des disques DVD et sera capable de désembrouiller les données; si le dispositif de lecture est un décodeur numérique, le module 11 reconnaîtra le format de flux de données diffusées protégées par un système d'accès conditionnel et sera capable de désembrouiller les données si l'utilisateur possède les droits nécessaires.

Le dispositif de lecture comprend en outre un module de décision 12 qui effectue un contrôle sur la lecture des données, c'est à dire qu'il détermine si les données lues en entrée peuvent être copiées librement (statut "*Copy-Free*"), ne peuvent être copiées qu'une seule fois (statut "*Copy-Once*"), ne peuvent plus être copiées (statut "*Copy-No-More*"), ne peuvent jamais être copiées (statut "*Copy-Never*") ou bien si ces données lues représentent une copie illégale et ne doivent donc pas être restituées sur un dispositif de restitution. Pour déterminer ces différents statuts, le module de décision utilise un procédé qui sera décrit plus bas en liaison avec la figure 5, à partir, soit de l'ensemble du flux de données qu'il reçoit du module de réception et de lecture 11, soit de seulement certaines informations extraites de ce flux de données, selon le type d'implémentation choisie par l'homme du métier.

Il génère en sortie des informations de gestion de génération de copie, par exemple des informations au format CGMS (de l'anglais "*Copy Generation Management Status*" signifiant littéralement "*Statut pour la Gestion des Générations de Copies*"), qui sont ensuite utilisées par les dispositifs d'enregistrement ou de restitution pour déterminer si les données peuvent être enregistrées ou copiées.

En pratique, ces informations sont transmises à deux modules de chiffrement de sortie 13 et 14 qui, en fonction des informations de gestion de génération de copie reçues, fournissent les données respectivement aux sorties S1 ou S2 sous forme protégée ou non, les informations concernant le statut des données étant également transmises en sortie dans le flux de données.

Si l'information de gestion de génération de copie indique que les données lues représentent une copie illégale, les modules de chiffrement 13 ou 14 ne fourniront aucune donnée en sortie. Il ne sera ainsi pas possible de visualiser le contenu, par exemple s'il s'agit d'un film, ou de l'enregistrer.

Si ces informations indiquent que les données ont un statut "*Copy-Free*", c'est à dire qu'elles peuvent être copiées librement, les données seront transmises sur l'une ou l'autre des sorties S1 ou S2 ou sur les deux sans être chiffrées.

Par contre si ces information indiquent que les données ont un statut "*Copy-No-More*" ou "*Copy-Never*" ou "*Copy-Once*", elles seront transmises aux sorties S1 ou S2 sous forme chiffrée.

Selon l'invention, le dispositif de lecture comprend deux modules de chiffrement de sortie différents. Les sorties S1 et S2 du dispositif sont des sorties numériques, c'est à dire qu'elles sont destinées à être reliées à un bus numérique. Par contre, elles utilisent chacune un mode de protection différent.

Pour la sortie S1, les données sont protégées au niveau de la ligne, par exemple selon la proposition de protection "DTCP" pour un bus numérique selon la norme IEEE 1394 ("DTCP" est un acronyme de "*Digital Transmission Content Protection*", aussi connu sous le nom de "5C", pour laquelle on pourra se référer pour plus de détails à la publication *"5C Digital Transmission Content Protection White Paper", Rev. 1.0, 14 juillet 1998*, disponible à l'adresse Internet suivante *http://www.dtcp.com/*). Lorsque cette sortie est utilisée, les données sont chiffrées par le module de chiffrement 13 de manière spécifique pour la ligne.

La sortie S2 conduit quant à elle à une ligne non protégée. Dans ce cas, les données sont chiffrées selon un mode de protection local du réseau domestique, de manière à ce que le contenu soit protégé. On pourra notamment utiliser le mode de chiffrement local des données conforme à la proposition XCA (acronyme de "eXtended Conditional Access", pour laquelle on pourra se référer pour plus de détails à la publication "*XCA, A Global Copy Protection System for Home Networks, White Paper v. 1.2*" publiée le 6 janvier 2000). Dans le cas où cette sortie S2 est utilisée, les données sont chiffrées par le module de chiffrement local 14.

Les sorties S1 et S2 du dispositif de lecture ont été représentées de manière séparée à la figure 1 mais il peut en réalité s'agir d'un seul connecteur de sortie permettant de connecter le dispositif au bus B du réseau domestique. Dans ce cas, le bus numérique pourra comporter deux modes distincts de fonctionnement: le mode protégé dans lequel les données sont chiffrées pour une liaison spécifique entre deux appareils du réseau et le mode non protégé dans lequel les données sont chiffrées de manière globale au niveau du réseau.

Le choix du type de sortie dépend en fait de l'appareil destiné à recevoir les données lues par le dispositif de lecture. En effet, le dispositif de lecture de l'invention est destiné à pouvoir être utilisé en liaison avec d'autres dispositifs qui ne supportent qu'un seul mode de protection: soit celui au niveau de la ligne, soit celui au niveau du réseau local. Entre le dispositif qui reçoit les données et celui qui les émet sur le bus à son intention, il existe de manière connue un échange lors duquel le dispositif de lecture connaît le type de protection supporté par l'appareil destinataire et peut ainsi déterminer quelle sortie S1 ou S2 sera choisie pour transmettre les données. Si l'appareil destiné à recevoir les données supporte les deux modes de protection tout comme le dispositif de lecture, le choix de la sortie S1 ou S2 sera prédéterminé selon l'implémentation choisie par l'homme du métier. Il est également possible dans ce cas d'utiliser les deux sorties, c'est à dire de transmettre les données à la fois sur la ligne protégée et sur la ligne non protégée, si celles-ci sont physiquement séparées.

En liaison avec la figure 5, nous allons maintenant décrire le procédé mis en œuvre par le module de décision 12 pour déterminer le statut des données pour la gestion de génération de copie.

Le premier test 100 consiste à vérifier si les données reçues sont chiffrées. Si ce n'est pas le cas (sortie "*N*"), cela signifie que l'on a affaire à un contenu qui est une création de l'utilisateur ou bien à un contenu qui a été piraté. C'est pourquoi un test supplémentaire 101 peut être effectué de manière préférentielle mais non obligatoire, pour déterminer si le contenu est tatoué. Si la réponse est positive (sortie "*O*"), cela signifie que le contenu a été piraté et le dispositif de lecture doit refuser de le lire (sortie "*STOP!*"). Si par contre, le contenu n'est pas tatoué (sortie "*N*" au test 101), alors le contenu est effectivement libre de copie et le statut "*Copy-Free*" lui est attribué.

Si la réponse au premier test 100 est positive (sortie "*O*"), c'est à dire si les données reçues sont chiffrées, le test suivant 102 consiste à détecter le type de support du contenu. Ceci s'applique en particulier pour les supports

détachables tels que les DVD qui peuvent être du type "*Enregistrable*" (par exemple les formats DVD-RAM, DVD-RW, DVD-R) ou du type "*Non enregistrable*" (par exemple DVD-ROM ou DVD vidéo pré-enregistré). Les données diffusées ou téléchargées seront par convention du type "*Non enregistrable*".

Si le support du contenu est du type "*Enregistrable*", le test suivant 103 consiste à détecter si le fournisseur du contenu a donné le droit d'effectuer une copie unique (statut "*Copy-Once*") ou aucune copie (statut "*Copy-Never*") de son contenu. Ces informations de contrôle de la copie communément notées CCI (acronyme de l'anglais "*Copy Control Information*") ou encore CGMS (acronyme de l'anglais "*Copy Generation Management System*" signifiant "système de gestion de la génération de copie") sont présentes dans les données sous une forme déterminée par le fournisseur du contenu et qui est bien connue de l'homme du métier. Si un support du type "*Enregistrable*" a un statut "*Copy-Once*", cela signifie que le support est lui-même la copie unique et qu'il ne doit plus être autorisé de copie. Par conséquent le statut de sortie sera "*Copy-No-More*". Par contre, si celui-ci a un statut "*Copy-Never*", cela signifie qu'il s'agit d'une copie pirate et celle-ci ne doit pas être lue par le dispositif de lecture (sortie "*STOP!*").

Il est à noter que le statut "*Copy-No-More*" signifie qu'il est interdit d'effectuer une génération supplémentaire de copie des données reçues. Ce statut signifie également, dans le cas où nous avons une protection locale au niveau du réseau (par exemple selon la proposition XCA), qu'il est possible d'effectuer une copie locale des données, cette copie n'étant lisible par aucun autre dispositif que ceux du réseau dans lequel elle a été copiée, ou en d'autres termes qu'il n'est pas possible d'effectuer une génération supplémentaire de copie pour un autre réseau domestique.

Si le support du contenu est du type "*Non-enregistrable*" ou si les données reçues sont des données diffusées ou téléchargées, le même test que le test 103 est effectué (test 104) et le statut détecté ("*Copy-Once*" ou "*Copy-Never*") correspond au statut de sortie attribué aux données.

Le statut "*Copy-Once*" autorise également la copie locale au niveau du réseau domestique lorsque nous avons un mode de protection local au réseau.

Nous allons maintenant décrire un dispositif d'enregistrement 20 selon l'invention tel que représenté schématiquement à la figure 3.

Celui-ci comporte deux entrées numériques E2 et E3, la première E2 recevant les données par une ligne protégée et la seconde E3 par une ligne non protégée. Comme on l'a vu plus haut, il peut s'agir en réalité d'une seule connexion physique avec un bus numérique capable de fonctionner dans un mode "protégé" ou dans un mode "non protégé". Le choix de l'entrée dépend du type d'appareil avec lequel le dispositif d'enregistrement est relié et des modes de protection supportés par cet appareil.

Dans le cas où les données sont reçues sur l'entrée E2, elles sont transmises à un module de déchiffrement 21 qui effectue un déchiffrement en utilisant une clé spécifique de la ligne, qui a par exemple été échangée avec le dispositif de lecture ayant envoyé les données sur la ligne.

Les informations concernant le statut des données, c'est à dire les informations de gestion de génération de copie des données, sont extraites du flux de données et analysées par un module de décision 22 selon le procédé qui sera décrit en liaison avec la figure 6 ci-dessous. Celui-ci effectue le contrôle de la copie au niveau du dispositif d'enregistrement.

Si le statut détecté est du type "*Copy-No-More*" ou "*Copy-Never*", l'enregistrement est stoppé et le module de décision 22 donne l'instruction au module de mise en forme pour l'enregistrement 23 de ne transmettre aucune donnée en sortie pour l'enregistrement.

Si en revanche le statut détecté est du type "*Copy-Once*", le module de décision 22 donne l'instruction au module 23 d'effectuer une mise en forme pour l'enregistrement de manière à ce que les données ne soient pas enregistrées en clair. Il peut s'agir par exemple d'un chiffrement selon la proposition CPRM (acronyme de "*Content Protection for Recordable Media*" signifiant littéralement "*Protection de Copie pour Support Enregistrable*" pour laquelle on pourra trouver plus de détails à l'adresse Internet suivante : *http://www.4centity.com/4centity/tech/cprm/*). Les données mises en forme sont ensuite transmises en sortie S3 pour être stockées sur un support d'enregistrement 24.

Lorsque le statut détecté par le module de décision 22 est du type "*Copy-Free*", l'enregistrement des données peut être effectué en clair, c'est à dire sans que les données ne soient mises en forme par le module 23.

Dans le cas où les données sont reçues sur l'entrée E3, elles sont déjà protégées par un chiffrement local au niveau du réseau. Dans ce cas, le dispositif d'enregistrement n'effectue aucun traitement et se contente d'enregistrer les données sous forme chiffrée.

En liaison avec la figure 6, nous allons maintenant décrire le procédé mis en œuvre dans le module de décision 22 du dispositif d'enregistrement.

Le module 22 a deux sources d'informations pour connaître le statut des données vis à vis de la gestion des générations de copie: les informations définies par le système de protection au niveau de la ligne – ces informations étant analysées à l'étape 110 – et les informations intégrées dans le contenu même des données transmises sur la ligne non protégée – informations analysées à l'étape 111. En principe, les deux sources doivent fournir les mêmes statuts de données mais, de manière préférentielle, et pour améliorer la sécurité du système, un test supplémentaire 112 est effectué pour définir le statut le plus restrictif parmi les informations reçues.

L'ordre de restriction parmi les statuts est le suivant:

"*Copy-Never*" = "*Copy-No-More*" > "*Copy-Once*" > "*Copy-Free*" ;

">" signifiant "est plus restrictif que".

Par exemple, si une information analysée à l'étape 110 indique un statut "*Copy-Once*" tandis que celle analysée à l'étape 111 indique un statut "*Copy-Free*", le statut retenu à l'étape 112 sera "*Copy-Once*".

Ensuite, selon le statut défini à l'étape 112, le module de décision 22 du dispositif d'enregistrement autorisera l'enregistrement (statuts "*Copy-Free*" ou "*Copy-Once*") ou bien n'autorisera pas l'enregistrement (statuts "*Copy-No-More*" ou "*Copy-Never*").

Il est à noter que les données reçues sur la ligne non protégée pourront toujours être enregistrées puisque celles-ci bénéficient déjà d'une protection spécifique au réseau local, c'est à dire qu'elles sont chiffrées de telle sorte qu'elles ne peuvent être lues (et restituées) que par un appareil du réseau.

Nous allons maintenant décrire un dispositif de restitution de données 30 selon l'invention tel que représenté à la figure 4.

Celui-ci comporte, comme le dispositif d'enregistrement 20, deux entrées numériques E4 et E5, reliées respectivement à une ligne protégée et à une ligne non protégée. Lorsque les données sont reçues sur l'entrée E4, celles-ci sont déchiffrées par le module de déchiffrement 31 spécifique à la ligne. Elles sont ensuite transmises en sortie S4 pour être restituées. Par exemple, s'il s'agit d'un téléviseur numérique, les données sont transmises au moyen d'affichage (tube cathodique, écran plasma, etc.) pour être visualisées.

Lorsque les données sont reçues sur l'entrée E5, elles sont transmises à un module de déchiffrement local 32 spécifique au réseau dans

lequel se trouve le dispositif. Ce module constitue la fin de la protection "d'un bout à l'autre" du réseau puisque les données ne sont déchiffrées, dans ce mode de protection, que pour être restituées en sortie S4 du dispositif.

Les dispositifs de lecture, d'enregistrement et de restitution de l'invention sont ainsi compatibles avec les différents modes de protection existants dans les réseaux numériques domestiques et permettent ainsi une meilleure interopérabilité des systèmes de protection contre la copie illicite.

Il est à noter que le terme "ligne" tel qu'employé dans toute la description s'entend de tout canal de communication dans un réseau numérique, que ce canal soit constitué par une ligne physique ou par une voie de communication dite "sans fil".

REVENDICATIONS

1. Dispositif de lecture de données numériques (1, 2, 10) destiné à être raccordé à un réseau numérique domestique et susceptible de recevoir des données représentant un contenu, caractérisé en ce qu'il comporte :

- un premier moyen de chiffrement (13) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie (S1) ; et
- un deuxième moyen de chiffrement (14) des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie (S2).

2. Dispositif selon la revendication 1, caractérisé en ce qu'il comporte en outre un module de décision (12) adapté à délivrer une permission ou une interdiction de copie et/ ou de lecture desdites données numériques,

lesdites données numériques étant fournies au premier (13) ou au deuxième (14) moyen de chiffrement lorsque ledit module de décision (12) délivre une interdiction de copie ("Copy-Never"; "Copy-No-More") ou une permission de copie unique ("Copy-Once").

3. Dispositif selon la revendication 2, caractérisé en ce que lesdites données numériques sont fournies directement à la première (S1) et/ou à la deuxième (S2) sortie sans être chiffrées lorsque ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free").

4. Dispositif selon l'une des revendications 2 ou 3, caractérisé en ce qu'il ne fournit aucune données numérique à la première (S1) ni à la deuxième (S2) sortie lorsque ledit module de décision (12) délivre une interdiction de lecture ("STOP!").

5. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free") lorsque lesdites données numériques reçues ne sont pas chiffrées.

6. Dispositif selon la revendication 5, caractérisé en ce que ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free") lorsqu'en outre lesdites données numériques reçues ne sont pas tatouées.

7. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de lecture ("STOP!") lorsque:

- lesdites données numériques reçues ne sont pas chiffrées ; et
- lesdites données numériques reçues sont tatouées.

8. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de copie ("Copy-No-More") lorsque :

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type enregistrable; et
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

9. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de lecture ("STOP!") lorsque:

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type enregistrable; et
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

10. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une permission de copie unique ("Copy-Once") lorsque:

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type non-enregistrable ou sont des données diffusées ou téléchargées;
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

11. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de copie ("Copy-Never") lorsque :

- lesdites données numériques reçues sont chiffrées;
- lesdites données numériques reçues sont stockées sur un support de type non-enregistrable ou sont des données diffusées ou téléchargées;
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

12. Dispositif selon l'une des revendications précédentes, caractérisé en ce que les informations de permission ou d'interdiction de copie et/ ou de lecture desdites données numériques délivrées par le module de décision (12) sont attachées aux données fournies à la première (S1) ou à la deuxième (S2) sortie.

13. Dispositif selon l'une des revendications précédentes, caractérisé en ce que la première (S1) et la deuxième (S2) sortie sont reliées respectivement à un unique connecteur pour raccorder ledit dispositif à un bus numérique (B) du réseau domestique, ledit bus fonctionnant dans un premier mode protégé lorsque les données sont issues de la première sortie (S1) et dans un second mode non protégé lorsque les données sont issues de la deuxième sortie (S2).

14. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le choix de la première (S1) ou de la deuxième (S2) sortie pour fournir les données est déterminé par le dispositif raccordé audit réseau numérique domestique destiné à recevoir lesdites données émises par ledit dispositif de lecture sur ledit réseau domestique.

15. Dispositif d'enregistrement de données numériques (3, 20) destiné à être raccordé à un dispositif de lecture (1, 2, 10) selon l'une des revendications 1 à 14 par l'intermédiaire d'un réseau numérique domestique, caractérisé en ce qu'il comporte :

- une première entrée (E2) destinée à recevoir des données qui ont été fournies à la première sortie (S1) dudit dispositif de lecture (10); et
- une seconde entrée (E3) destinée à recevoir des données qui ont été fournies à la deuxième sortie (S2) dudit dispositif de lecture (10).

16. Dispositif selon la revendication 15, caractérisé en ce qu'il comporte un moyen de déchiffrement (21) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture, ledit moyen de déchiffrement (21) étant relié à la première entrée (E2) dudit dispositif d'enregistrement.

17. Dispositif selon l'une des revendications 15 ou 16 prises dans leur dépendance de la revendication 12, caractérisé en ce qu'il comporte en outre un module de décision (22) adapté à analyser les informations de permission ou d'interdiction de copie et/ou de lecture attachées aux données à enregistrer,

ledit dispositif d'enregistrement délivrant lesdites données à enregistrer à une sortie (S3) lorsque ledit module de décision (22) détecte une permission de copie ("Copy-Once"; "Copy-free") ;

ledit dispositif d'enregistrement ne délivrant aucune donnée à enregistrer à ladite sortie (S3) lorsque ledit module de décision (22) détecte une interdiction de copie ("Copy-No-More"; "Copy-Never").

18. Dispositif de restitution de données numériques (4, 30) destiné à être raccordé à un dispositif de lecture (1, 2, 10) selon l'une des revendications 1 à 14 par l'intermédiaire d'un réseau numérique domestique, caractérisé en ce qu'il comporte:

- une première entrée (E4) destinée à recevoir des données qui ont été fournies à la première sortie (S1) dudit dispositif de lecture (10) et qui est reliée à un premier moyen de déchiffrement (31) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture ;

- une seconde entrée (E5) destinée à recevoir des données qui ont été fournies à la deuxième sortie (S2) dudit dispositif de lecture (10) et qui est reliée à un deuxième moyen de déchiffrement (32) des données selon un mode de protection spécifique au réseau domestique ; et

- une sortie (S4) pour la restitution des données, reliée au premier et au deuxième moyen de déchiffrement.

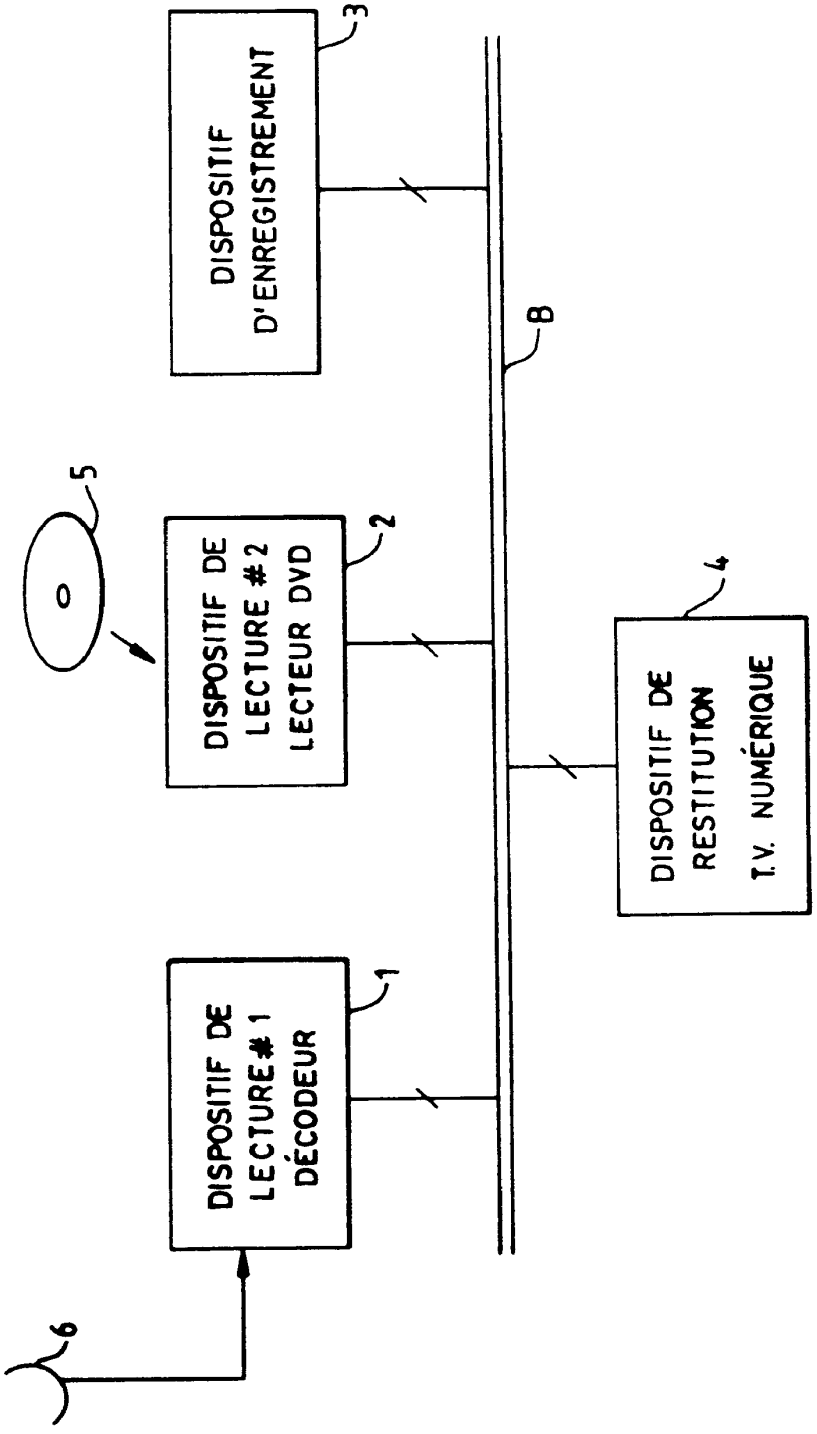

DISPOSITIF D'ENREGISTREMENT
3
8
5
DISPOSITIF DE LECTURE #2 LECTEUR DVD
2
4
DISPOSITIF DE RESTITUTION T.V. NUMÉRIQUE
DISPOSITIF DE LECTURE # 1 DÉCODEUR
1
6

FIG.1

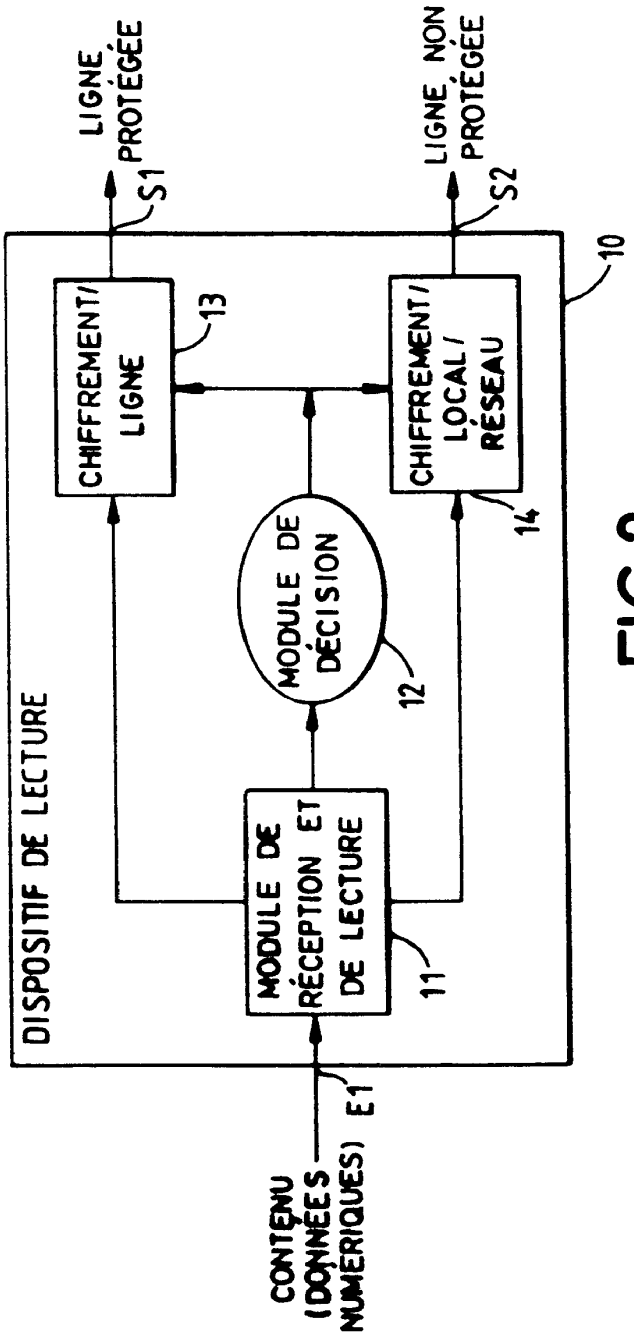

LIGNE PROTÉGÉE
S1
LIGNE NON PROTÉGÉE
S2
10
CHIFFREMENT/ LIGNE
13
CHIFFREMENT/ LOCAL/ RÉSEAU
14
MODULE DE DÉCISION
12
MODULE DE RÉCEPTION ET DE LECTURE
11
DISPOSITIF DE LECTURE
E1
CONTENU (DONNÉES NUMÉRIQUES)

FIG.2

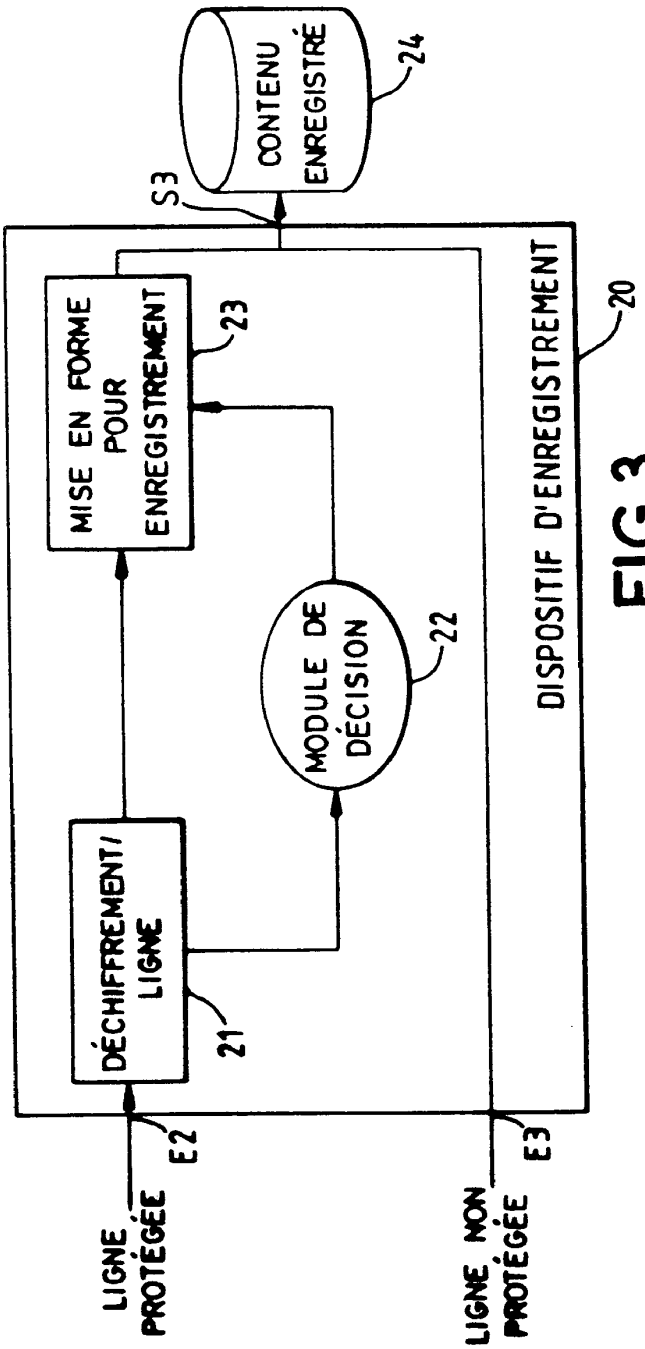

CONTENU ENREGISTRÉ
24
S3
MISE EN FORME POUR ENREGISTREMENT
23
MODULE DE DÉCISION
22
DÉCHIFFREMENT/ LIGNE
21
DISPOSITIF D'ENREGISTREMENT
20
E2
E3
LIGNE PROTÉGÉE
LIGNE NON PROTÉGÉE

FIG.3

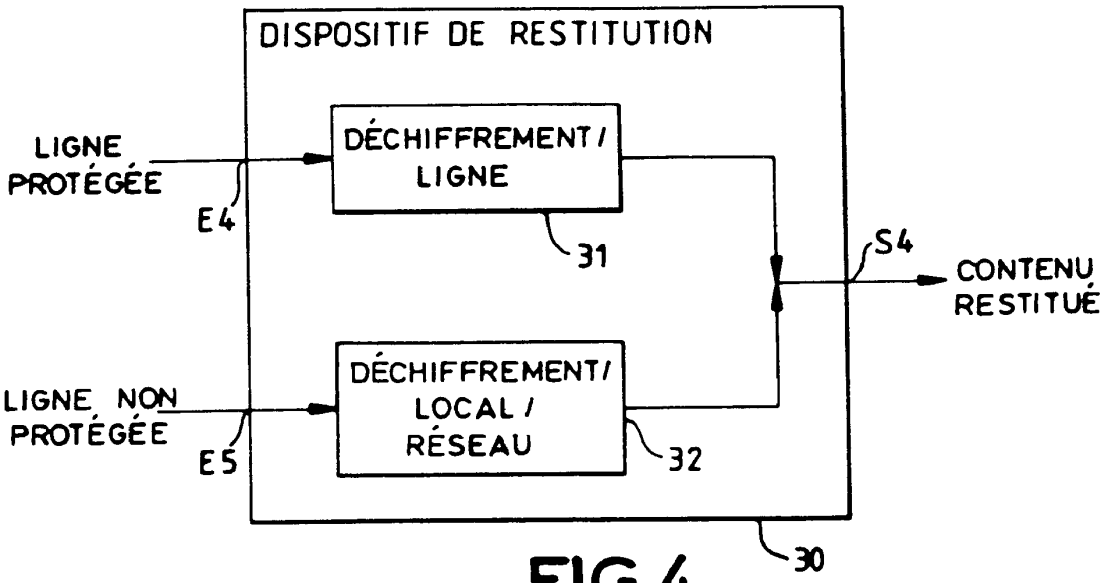

DISPOSITIF DE RESTITUTION
LIGNE PROTÉGÉE
E4
DÉCHIFFREMENT / LIGNE
31
S4
CONTENU RESTITUÉ
LIGNE NON PROTÉGÉE
E5
DÉCHIFFREMENT / LOCAL / RÉSEAU
32
30

FIG.4

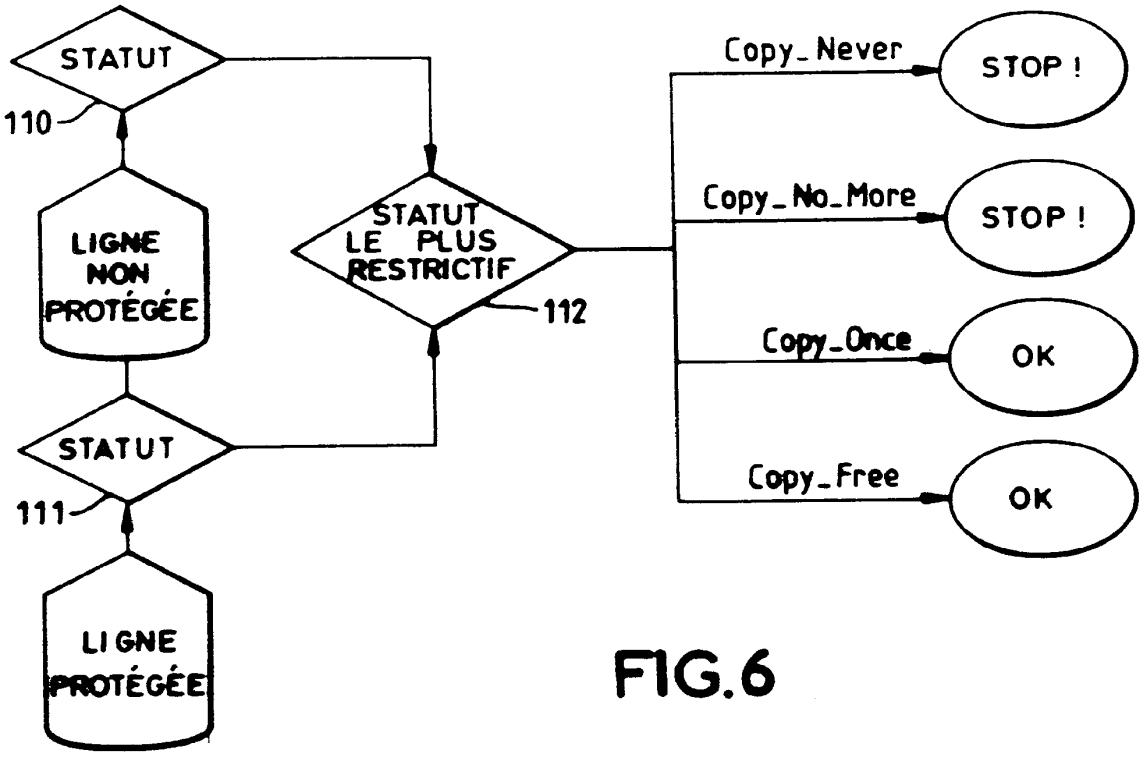

STATUT
110
LIGNE NON PROTÉGÉE
STATUT
111
LIGNE PROTÉGÉE
STATUT LE PLUS RESTRICTIF
112
Copy_Never
STOP !
Copy_No_More
STOP !
Copy_Once
OK
Copy_Free
OK

FIG.6

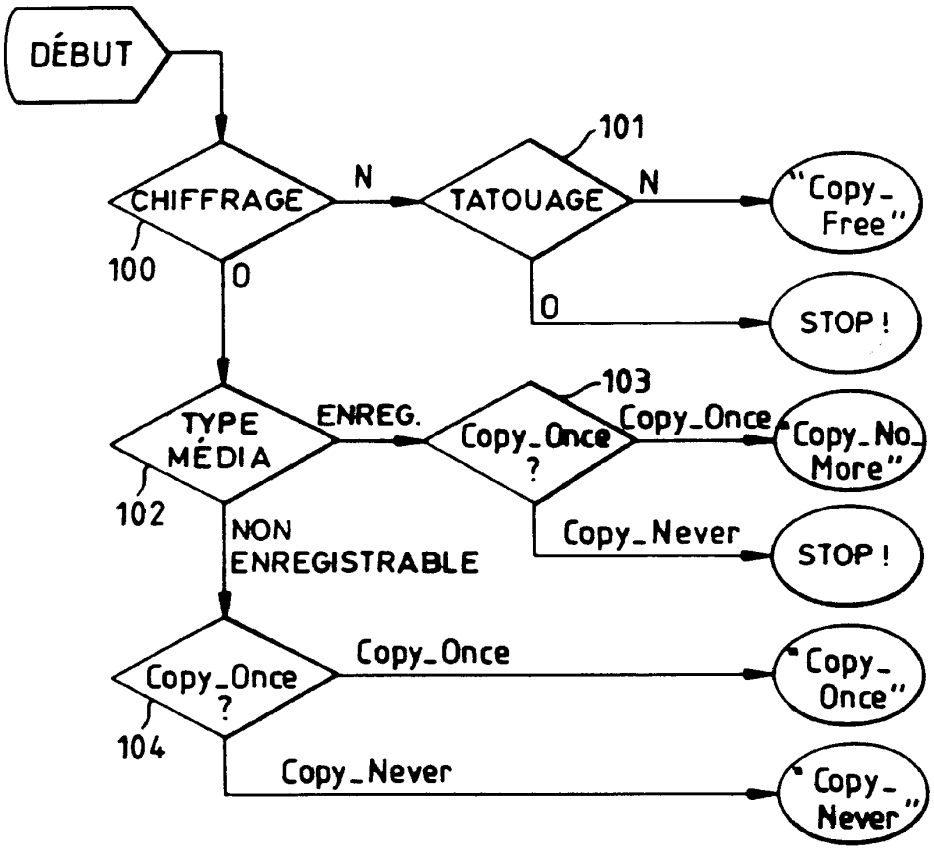

DÉBUT
CHIFFRAGE
100
N
0
101
TATOUAGE
N
0
"Copy_Free"
STOP !
TYPE MÉDIA
102
ENREG.
NON ENREGISTRABLE
103
Copy_Once ?
Copy_Once
"Copy_No_More"
Copy_Never
STOP !
Copy_Once ?
104
Copy_Once
"Copy_Once"
Copy_Never
"Copy_Never"

FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR 01/00572

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 382 296 A (PHILIPS NV) 16 August 1990 (1990-08-16) the whole document ---	1
A	EP 0 969 463 A (PIONEER ELECTRONIC CORP) 5 January 2000 (2000-01-05) the whole document ---	1-12,15, 17
A	HITACHI LTD ET AL: "5C Digital Transmission Content Protection White Paper - Revision 1.0" DTCP, 'Online! 14 July 1998 (1998-07-14), XP002134182 Retrieved from the Internet: <URL:http://www.dtcp.com/wp_spec.pdf> 'retrieved on 1999-10-15! cited in the application the whole document -----	1,12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 May 2001	29/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR 01/00572

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0969463 A	05-01-2000	JP 2000023089 A	21-01-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Int' ationale No
PCT/FR 01/00572

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G11B H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 382 296 A (PHILIPS NV) 16 août 1990 (1990-08-16) le document en entier ---	1
A	EP 0 969 463 A (PIONEER ELECTRONIC CORP) 5 janvier 2000 (2000-01-05) le document en entier ---	1-12,15, 17
A	HITACHI LTD ET AL: "5C Digital Transmission Content Protection White Paper - Revision 1.0" DTCP, 'en ligne! 14 juillet 1998 (1998-07-14), XP002134182 Extrait de l'Internet: <URL:http://www.dtcp.com/wp_spec.pdf> 'extrait le 1999-10-15! cité dans la demande le document en entier -----	1,12

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
21 mai 2001	29/05/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux mer. .s de familles de brevets

Demande Int^ ^nationale No
PCT/FR 01/00572

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0969463 A	05-01-2000	JP 2000023089 A	21-01-2000

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/77790 A1

(51) International Patent Classification[7]: G06F 1/00, G07F 17/16

(21) International Application Number: PCT/EP01/04088

(22) International Filing Date: 10 April 2001 (10.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00401007.0 11 April 2000 (11.04.2000) EP

(71) Applicant *(for all designated States except US)*: **THOMSON MULTIMEDIA** [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **DIEHL, Eric** [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **FISCHER, Pierre** [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Agent: **BONNANS, Arnaud**; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

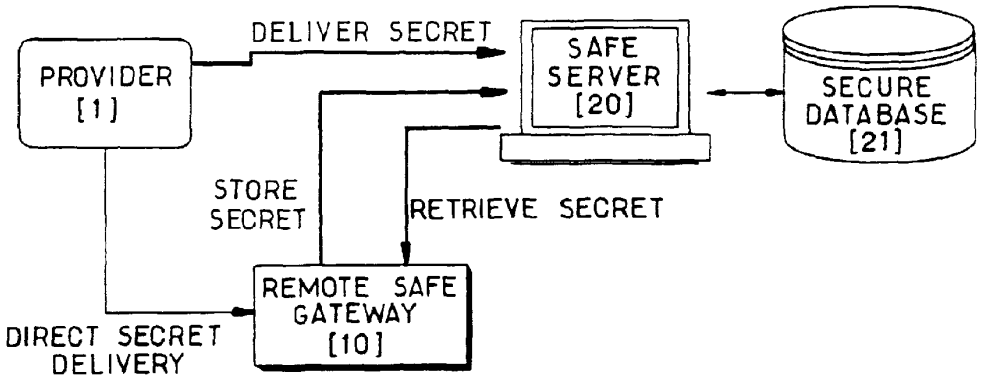
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT



(57) Abstract: A system for securely storing secret information comprises an apparatus (10; 1) containing the secret information, a device meant to use said secret information to decrypt a digital content and a remote server (20). The apparatus can send the secret information to the server (20) that has means for storing the secret information. A process with the following steps is proposed: initiating a remote communication between the apparatus (10; 1) and the remote server (20); sending the secret information from the apparatus (10; 1) to the server (20); storing the secret information on the server (20). A method for distribution of a digital content is also described.

WO 01/77790 A1

SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT

Field of the invention

The invention relates generally to secure storage of secret information and more particularly to a system and a process for securely storing secret information and to an apparatus and a server to be used in said system. The invention also relates to a method for distribution of a digital content.

Background art

With the advent of digital TV, and copy protection, the access to content will be protected by rights. These rights may have many forms like entitlements, or dedicated decryption keys. The notion of rights might be extended to any secret information. All these type of data have in common that they need to be stored in a safe place.

Today none of the consumer devices has such tamper proof place. The price would be prohibitive. Only smart cards offer sufficient security. Unfortunately the size of memory of smart cards, and thus their storage capability, is limited. Furthermore a smart card can break down, or be lost. So today, once the user mislays his secret data, he will have no simple way to retrieve them. If these data represent user's rights acquired on digital content (for example the right to view a film or to listen to music) it may be prejudicial to the user if he loses these rights he has paid for.

Summary of the invention

The present invention is therefore directed to the problem of finding a way of safely and securely storing secret data to be used by a single device or by a device in a network. Another problem to be solved by the invention is to find a way of retrieving these secret data if the device or the network has lost them.

The invention relates to a system for securely storing secret information to be used by a device wherein said secret information is stored in a remote server. The device may be part of a home network and preferably the secret information is used by said device to access to a digital content.

Therefore, the remote server acts as a bank which maintains in a safe place digital secrets.

The invention proposes an apparatus containing secret information to be used by a device to decrypt a digital content and having means for sending

said secret information to a remote server in order to store said information in said remote server, said server being remote from said device.

The invention also proposes a system for securely storing secret information comprising an apparatus containing said secret information, a device meant to use said secret information to decrypt a digital content and a server remote from said apparatus and from said device, wherein said apparatus comprises means for sending said secret information to said server and wherein said server comprises means for storing said secret information.

The apparatus may be part of said device, or may belong to the same home network as said device. In such cases, the apparatus is thereafter called the remote safe gateway. The apparatus may alternatively belong to a local network generating said secret information (*i.e.* belong to the secret provider).

According to another aspect of the invention, a server for securely storing secret information to be used by a device remote from said server to decrypt a digital content has means for receiving said secret information through a remote communication

A process is proposed for securely storing secret information to be used by a device to decrypt a digital content : this process comprises the steps of :

- initiating a remote communication between an apparatus containing said secret information and a server remote from said device ;
- sending said secret information from said apparatus to said server ;
- storing said secret information on said server.

The invention also relates to a method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server remote from said device for storing said secret information on said server ;
- providing means for said device to retrieve said secret information from said server and to decrypt the encrypted digital content with said secret information.

Brief description of the drawings

Fig. 1 illustrates the general architecture of a system according to the invention.

Fig. 2 illustrates the architecture of a device used in the system of Fig. 1.

Fig. 3 illustrates a process for storing secret information according to a first embodiment of the invention.

Fig. 4 illustrates a process for retrieving a secret information stored according to the process illustrated in Fig. 3.

Fig. 5 illustrates a second embodiment of the invention.

Fig. 6 illustrates a process for storing a secret information in the second embodiment of the invention.

Description of the preferred embodiments

In Fig. 1, we have illustrated a first embodiment of a system according to the invention. In this embodiment, the user has a Set Top Box device 10 (STB) with a return channel such as a PSTN (for "Public Switched Telephone Network") modem or a cable modem.

We assume that all the information to store securely can be carried to this STB. For instance, we can envisage that a complete home network can benefit from the remote safe facility. In this case, preferably, a unique device of the network will be able to store and retrieve secret information according to the invention. This unique dedicated STB is used as an apparatus called the remote safe gateway. Obviously it could be another type of device, for example a computer.

Through its return channel, each remote safe gateway interacts with a remote server 20 called the remote safe server. The remote server has direct access to its own secure database 21. The secure database will store safely and securely the secret information.

In a preferred embodiment of the system, the secure database will be duplicated at least once in different locations. This will avoid loss of data due to natural or malicious crashes. Nevertheless, only one occurrence of the secure database will be considered in the following in order to simplify the presentation of the invention.

The user receives his secrets from a secret provider 1 which is consider here as having generated the secret information. It may be for example a content provider which provides, with an encrypted content, a secret to decrypt this content.

The secret provider 1 provides the information directly to the remote safe gateway 10. The user may receive information from many secret providers.

The characteristics of the system are as follows :

- A user must be identified uniquely. It must not be possible to impersonate him.

- A user must be able to transfer the secret digital information stored in his home system to the safe server 20. No information must leak from this transfer. For that purpose, the remote safe gateway 10 is used to make this transfer.

- The user must be able to retrieve one, part, or all the information stored in his remote safe. No information must leak from this transaction. For that purpose, the remote safe gateway 10 is also used for this transaction.

- There must be no constraint on the format of the stored information.

We will now describe how the system is working.

A first stage of the process consists in the registration of the user. Prior to use the remote safe, the user must sign on the remote safe server's operator. For that purpose, he provides a set of personal information. The definition of these data depends on the operator and is out of the scope of this invention. In return the operator returns a set of secret user identity information (SI_{user}) used in the next stages. Among this set of information is the unique identifier (ID_{user}) that thoroughly defines a given user.

The channel used for this communication can be different from the return channel of the remote safe gateway. In any case the transfer of the secret user identity information (SI_{user}) needs to be secured. There are several possible ways: mailing of a smart card, encrypted information sent through the return channel, ... In the last case, the decryption key is transferred through a secure separate channel such as phone or post mail.

A second stage of the process consists in the storage of secret information in the safe. This requires several steps.

In a first step, the remote safe gateway authenticates the remote safe server using known authentication methods. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the storage operation fails.

In a third step, they define a common session key $K_{session}$. This means a remote communication is initiated between the remote safe server and the remote safe gateway.

Then, in a fourth step, the remote safe server creates a unique identifier, $InfID_{user\_i}$ for the information i to be stored. InfIDuser_i is unique for each information stored by the user. Its choice is fully under the control of the

remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule *f*, so that $f(InfID_{user\_i}, ID_{user})=true$.

In a fifth step, the remote safe gateway sends the information i to store to the remote safe server. The information i is encrypted using the session key Ksession before being sent. In an optional step, the remote safe gateway encrypts the information i using a secret key of the remote safe gateway before using the session key. Thus, with this optional step, the remote safe server will not have access to the plain text information.

Then, in the last step, the remote safe server decrypts the received information using the session key Ksession and stores it into its secure database.

The transfer may be secured against transmission errors, or message tampering. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

A third stage of the process consists in the retrieval of the secret information from the remote safe server. This operation requires the following steps.

In a first step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the retrieval operation fails.

In a second step, they define a common session key Ksession.

Then, in a third step, the remote safe gateway provides the remote safe server with the unique identifier of the information to retrieve InfIDuser_i.

In a fourth step, the remote safe server checks the validity of InfIDuser_i. It checks if the corresponding information exists in the database and if this is the case, the remote safe server sends back the requested information to the requesting remote safe gateway in a fifth step. The information is encrypted using the session key Ksession before being sent to the remote safe gateway.

Then, in a last step, the remote safe gateway decrypts the received message using the session key Ksession.

Preferably, the transfer is secured against transmission errors, or message tampering. In that case, the remote safe gateway checks the integrity of the decrypted message before using it.

According to one preferred aspect of the invention, all the operations, except the registration phase, should be transparent to the user. In other words, the retrieval of the stored secrets should be automatic and should not request any interaction from the user.

Fig. 2 illustrates a possible architecture for the remote safe gateway. In this figure, only the elements which are necessary for the understanding of the invention have been represented.

The remote safe gateway has a Central Processing Unit (CPU) 100. It is assumed that the CPU has its own volatile memory and non-volatile memory where its program is stored. In addition, the remote safe gateway has a non-volatile memory space 101 called the identifiers' memory. The CPU 100 can read and write the content of this space.

The remote safe gateway has also a secure processor 102. This secure processor is a tamper proof device that has at least a dedicated CPU 110, a non volatile memory 111 (ROM – Read Only Memory) to store program and persistent data, a volatile memory 112 (RAM – Random Access Memory), and a dedicated non-volatile memory area 113, called the secret cache memory. The secure processor 102 is, in a preferred embodiment, a smart card.

The CPU 100 never handles actual secrets. It handles only information identifiers InfIDuser_i. It maintains a list of the secret information through a list of their corresponding InfIDuser_i. This list is stored in the identifiers' memory. This space needs not to be tamper-proofed. Therefore it is not costly. The size of the identifiers' memory should be chosen to be large enough to store the expected amount of information identifiers.

The secure processor's CPU 110 handles the actual secrets. It stores them in its secret cache memory 113. Unfortunately this space is limited in size due to cost. Therefore it will employ memory-caching techniques that optimize the use of the space. It will store the most recently used secrets and some of the most frequently used secrets.

If the remote safe gateway needs a secret information which is not readily available in the secret cache memory 113, then the secure processor's CPU 110 requests it to the remote safe server.

In one embodiment of the invention, the remote safe gateway is part of a digital home network where other devices are connected. Some of these devices can also handle secrets. In that case they may reproduce the architecture of Fig. 2. Nevertheless, only the remote safe gateway is able to communicate with the remote safe server. The other devices exchange, through secure communication, with the remote safe gateway their secrets to store or to retrieve.

We will now enter into more details of this first embodiment.

Registration of the user.

When signing on, the user receives the secret user identity information as follows:

- A unique identifier IDuser.
- A pair of public (PUB_{user}) and private (PRI_{user}) keys; the remote safe server encrypts with a public key cryptosystem that we will call CS1. RSA (Rivest-Shamir-Adleman public key cryptosystem) could be such a system.
- A public key certificate $CERT_{user}$ signed by the remote safe server using its private signature key PRI_{safe_sign}. The remote safe server signs with a public key cryptosystem that we will call CS2. RSA could be such a system. CS2 can be identical to CS1.
- The public key of the remote safe server PUB_{safe_enc} using cryptosystem CS1.

These data must be transferred safely to the user. It is especially important that his private key, $PRI_{user,}$ is kept secret. He may for example receive these data in a smart card sent to him via mail.

Storage of the secret information.

The format of the message to store is preferably defined as follows:

```
Info_To_Store = {
     InfIDuser_i
     Length_clear_text
     Clear_Text
     Length_secret
     for I=0 to Length_secret-1
          Secret_data[i]
     Checksum
}
```

where :

- InfIDuser_i is a unique identifier of the information stored by the user. This identifier is unique to the user and delivered by the safe server ;
- Clear_Text is an ASCII text that describes the stored secret information. Its content is user defined. It could be envisaged that the secret provider delivers a default value for this secret ;
- Length_clear_text defines the length in bytes of Clear_Text ;
- Secret_data is the secret to store in the remote safe ;
- Length_secret defines the length in bytes of Secret_data ;
- Checksum is the sum of all previous bytes of the packet.

The process for storing a secret information is illustrated in Fig. 3 and explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe server defines a new value for the information identifier, InfIDuser_i. It sends it to the remote safe gateway.

The remote safe gateway builds the message Info_To_Store with its secret data and InfIDuser_i. It encrypts it with the Triple DES algorithm using the common session key Ksession. It sends the encrypted message to the remote safe server that decrypts it using the common key Ksession.

The remote safe server checks the validity of Checksum. If the received message is valid, the remote safe server sends it to the secure database. If the operation was successful, the remote safe server returns an acknowledgement to the remote safe gateway, else it returns a non-acknowledgement.

Retrieving the secret information.

The process for retrieving a secret information stored in the remote safe server is illustrated by Fig. 4 and will be explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe gateway sends the reference of the data to retrieve: InfIDuser_i.

On receipt of the information identifier InfIDuser_i, the remote safe server passes it to the secure database.

The secure database checks if the message exists, i.e., if there is an information, own by the user, that has the right identification. If it is the case, then it returns the requested information Info_To_Retrieve to the remote safe server. The remote safe server encrypts the received data using Triple DES with the session key Ksession and It sends the encrypted message to the remote safe gateway.

The remote safe gateway decrypts the received message using the session key Ksession. It checks the validity of Checksum and if it is valid, the remote safe gateway uses the retrieved secret information Info_To_Retrieve.

We will now describe a second embodiment of the invention which is illustrated in Fig. 5.

In this embodiment, the secret provider can provide the information directly to the remote safe gateway or by an indirect way using the remote safe server. The user may receive information from many secret providers.

The additional characteristics of the system are as follows:

- A third party, known as the secret provider, can deposit a secret to the remote safe server on behalf of a user. No information must leak from this transaction.

- It is not possible to impersonate a secret provider.

- Once a secret as been deposited by a secret provider, the secret provider has no possible access to it.

- A secret provider cannot retrieve any information stored on the account of a user.

- Only an authorized secret provider can deposit a secret onto the account of a user.

In this embodiment, the process for the secret provider has two stages :

The first stage consists in the registration of the secret provider. As for the remote safe gateway, the secret provider needs to sign on the remote safe server. He signs on as secret provider. In return, it receives a set of information known as secret provider identity information (SI_{prov}).

The second stage consists in the storage of a secret information on behalf of a user. This stage requires several steps.

In a first step, the secret provider, through an apparatus of a local network of its own, authenticates the remote safe server. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the secret provider. If the authentication fails, then the storage operation fails.

In a third step, the remote safe server and the secret provider's apparatus define a common session key $K_{session.}$

Then, in a fourth step, the secret provider provides the identity of the user that he is acting for: ID_{user}.

In a fifth step, the remote safe server creates a unique identifier, InfIDuser_i for the information to be stored. InfIDuser_i is unique for each information stored by the user identified by IDuser. Its choice is fully under the control of the remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule.

In a sixth step, the secret provider sends the information to store to the remote safe server. The sent information is encrypted using the session key $K_{session}$.

In a last step, the remote safe server decrypts the received information using the session key $K_{session}$ and stores it into its secure database. The transfer may be secured against transmission errors, or message tampering using known techniques. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

Once the operation was successfully ended, then the secret provider sends the information identifier InfIDuser_i to the corresponding remote safe gateway. The secret provider does not keep any copy of it. Therefore, it is impossible for the secret provider to access any more to the secret information to retrieve it or to modify it.

Details of this second embodiment are explained bellow:

Registration of the secret provider

When signing on, the secret provider receives the following secret provider identity information:

- A unique identifier ID_{prov}.
- A pair of public (PUB_{prov}) and private (PRI_{prov}) keys; the remote safe server encrypts with the public key cryptosystem CS1.
- A public key certificate $CERT_{prov}$ signed by the remote safe server using its private signature key $PRI_{safe\_sign\_2}$; the safe server signs with the public key cryptosystem CS2.
- The public key of the remote safe server PUB_{safe_enc}.

These information must be transferred safely to the secret provider. It is especially important that his private key is kept secret

Storage of an information on behalf of a user.

This process, which is illustrated in Fig. 6, is similar to the process described previously in view of Fig. 3. The main differences are:

- Prior to exchange the secret information, the secret provider has to identify the user to whom is it depositing. The identification uses the user's unique identifier IDuser.

- Once the secret provider successfully stored the information, it sends the reference of the information to the user, that is to its remote safe gateway.

The system if the invention may be applied to a new distribution model. For example, a content provider wants to distribute in a controlled manner a content. This content can be any digital content such as video, MP3 files, software, etc. For that purpose it distributes the content encrypted with an encryption key $K_{enc\_cont\_i}$. To read this encrypted content, the user must have access to the decryption key $K_{dec\_cont\_i}$. The decryption key may be equal to the encryption if we use a symmetric cryptosystem. The user contacts the content provider and buys the right to access the content. Acting as a secret provider, the content provider deposits the decryption key in the user's remote safe. In return the user receives the information identifier of the decryption key.

Another possible application of the system of the invention is a small footprint backup of a jukebox. The jukebox will be a future new type of consumer device. It will probably be successful. Nevertheless with the jukebox, a major risk is introduced: loss of all the contents stored in the jukebox. Currently it is envisaged to use hard disks as storage units. In the field of software, it is well known that regular backup of the hard disk is a safe practice. But it is not reasonable to expect the same feature in a consumer device.

The system of the invention will provide a backup facility based on the remote safe as a new service. For each legally delivered content, the content provider will provide an additional information called a digital purchase proof. The digital purchase proof is the result of a one way cryptographic function using as input parameter a unique identifier of the owned content, and the user identifier ID_{user}. Instead of backing up all his contents, the user stores in his remote safe all his digital purchase proofs. If he loses one content, the user returns to the content provider the corresponding digital proof. The content provider checks if the digital proof is consistent with the claimed content and the identity of the user. If it is the case, then the content provider sends back to the user a copy of the content.

In conclusion, the invention offers the following advantages:

- the possibility to handle in a safe and secure manner a large quantity of secret data without requesting an in-house large tamper-proof space;

- a simple new model of distribution of digital content that could fit for IP streaming, or even prerecorded contents;

- a small size backup of large library of digital contents.

CLAIMS

1. Apparatus containing secret information to be used by a device to decrypt a digital content,

characterised by means for sending said secret information to a remote server (20) in order to store said information in said remote server (20), said server (20) being remote from said device.

2. Apparatus according to claim 1, being part of said device.

3. Apparatus according to claim 1, belonging to the same home network as said device.

4. Apparatus according to claim 1, belonging to a local network (1) generating said secret information.

5. System for securely storing secret information comprising :

- an apparatus (10 ; 1) containing said secret information ;
- a device meant to use said secret information to decrypt a digital content ;
- a server (20) remote from said apparatus and from said device,

wherein said apparatus (10 ; 1) comprises means for sending said secret information to said server (20) and wherein said server (20) comprises means for storing said secret information.

6. System according to claim 5, wherein said apparatus (10) is part of said device.

7. System according to claim 5, wherein said apparatus (10) and said device are connected to a common home network.

8. System according to claim 5, wherein said apparatus (1) belongs to a local network generating said secret information.

9. Server (20) for securely storing secret information to be used by a device to decrypt a digital content, said device being remote from said server (20),

characterised by means for receiving said secret information through a remote communication.

10. Process for securely storing secret information to be used by a device to decrypt a digital content comprising the steps of :

- initiating a remote communication between an apparatus (10 ; 1) containing said secret information and a server (20) remote from said device ;
- sending said secret information from said apparatus (10 ; 1) to said server (20) ;
- storing said secret information on said server (20).

11. Method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server (20) remote from said device for storing said secret information on said server (20) ;
- providing means (10) for said device to retrieve said secret information from said server (20) and to decrypt the encrypted digital content with said secret information.

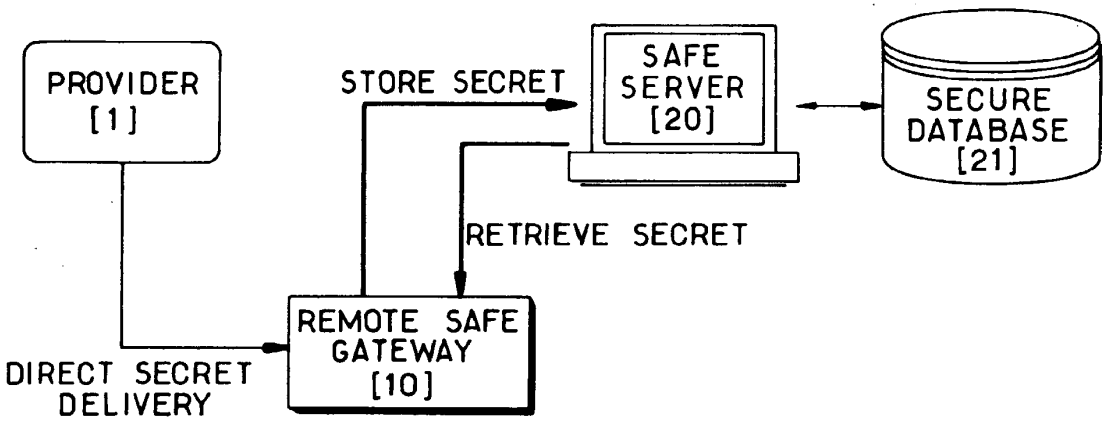

PROVIDER
[1]
STORE SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.1

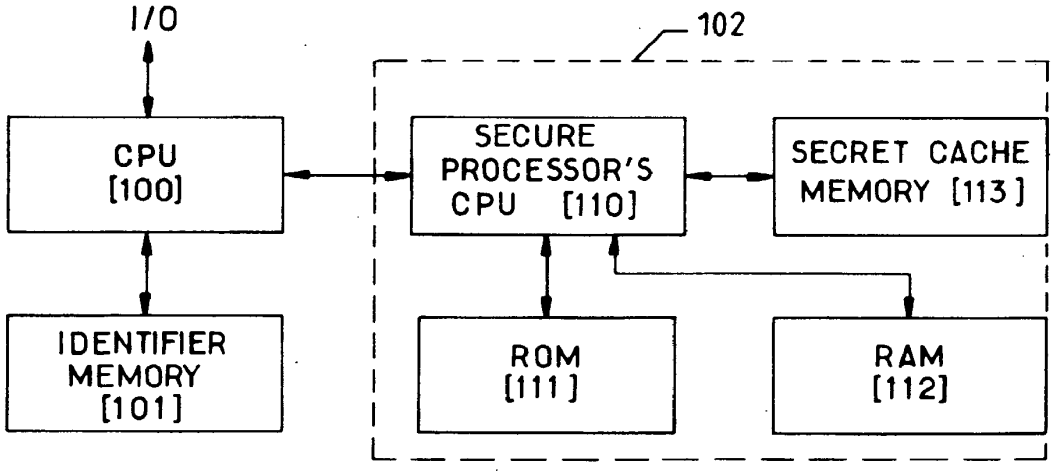

I/O
102
CPU
[100]
SECURE
PROCESSOR'S
CPU [110]
SECRET CACHE
MEMORY [113]
IDENTIFIER
MEMORY
[101]
ROM
[111]
RAM
[112]

FIG.2

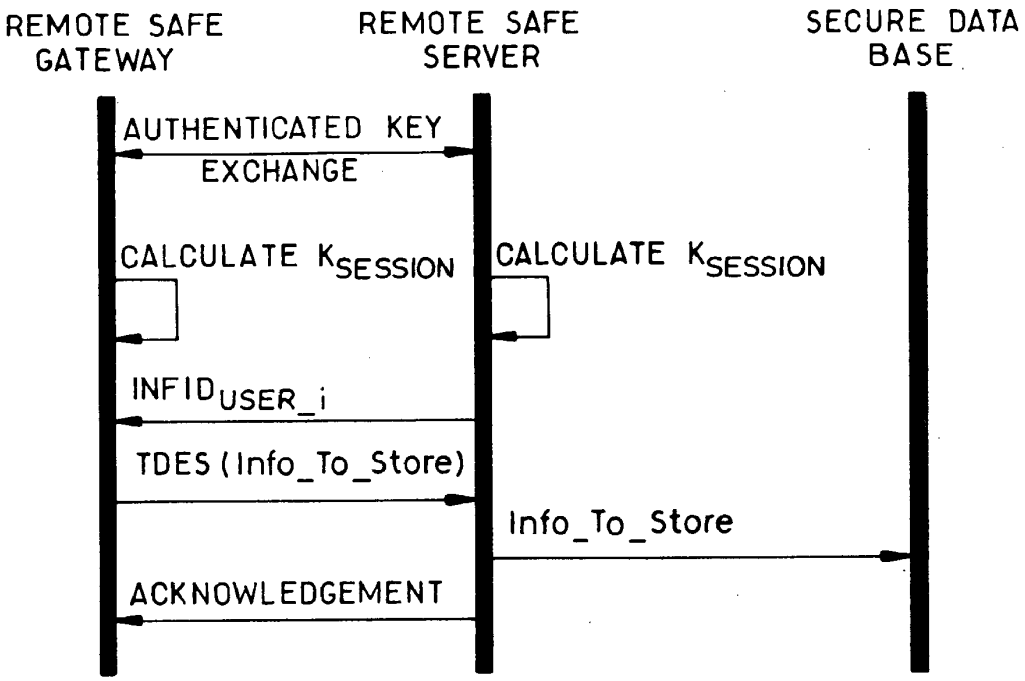

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
TDES (Info_To_Store)
Info_To_Store
ACKNOWLEDGEMENT

FIG.3

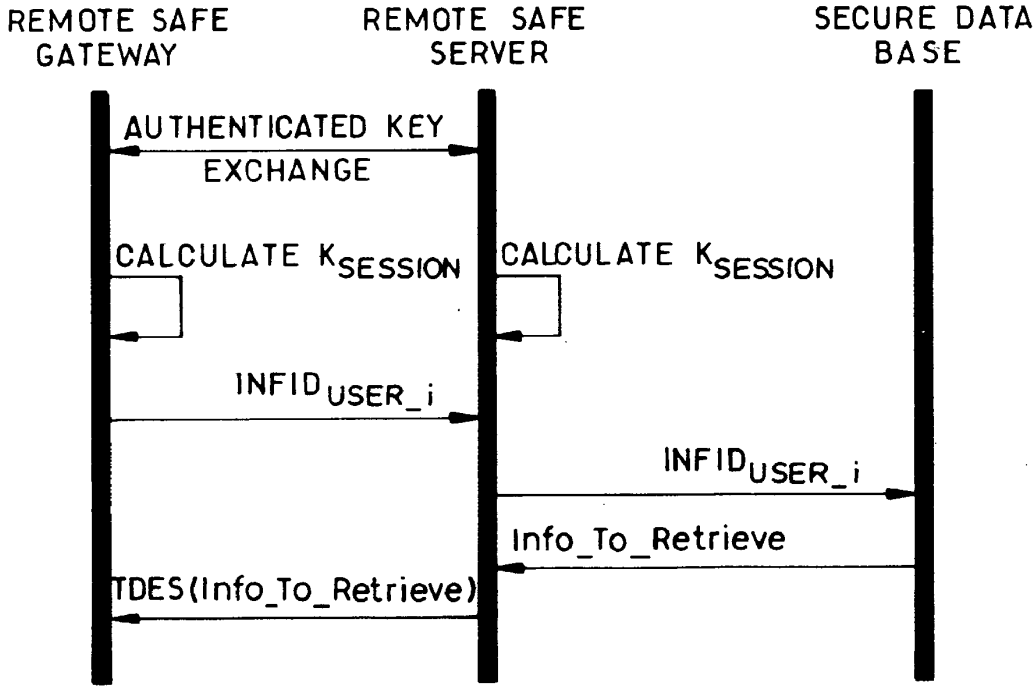

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
$INFID_{USER\_i}$
Info_To_Retrieve
TDES(Info_To_Retrieve)

FIG.4

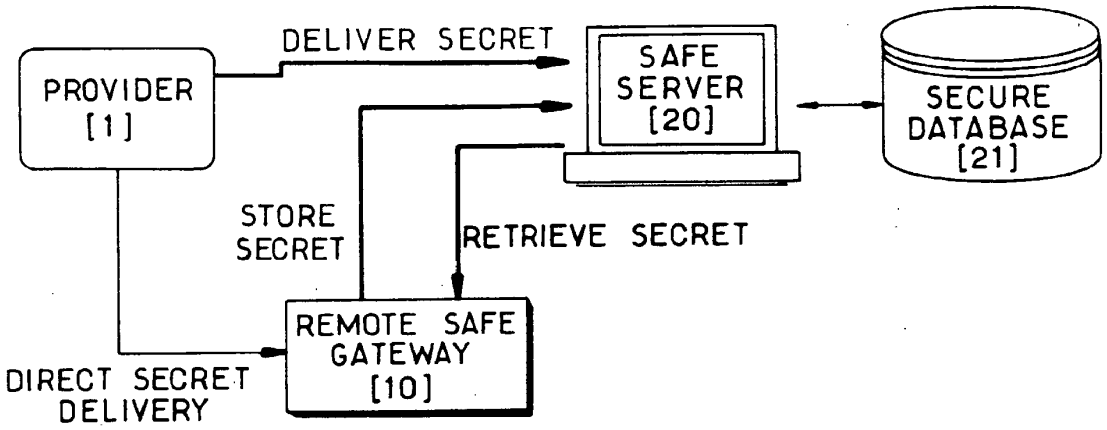

PROVIDER
[1]
DELIVER SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
STORE
SECRET
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.5

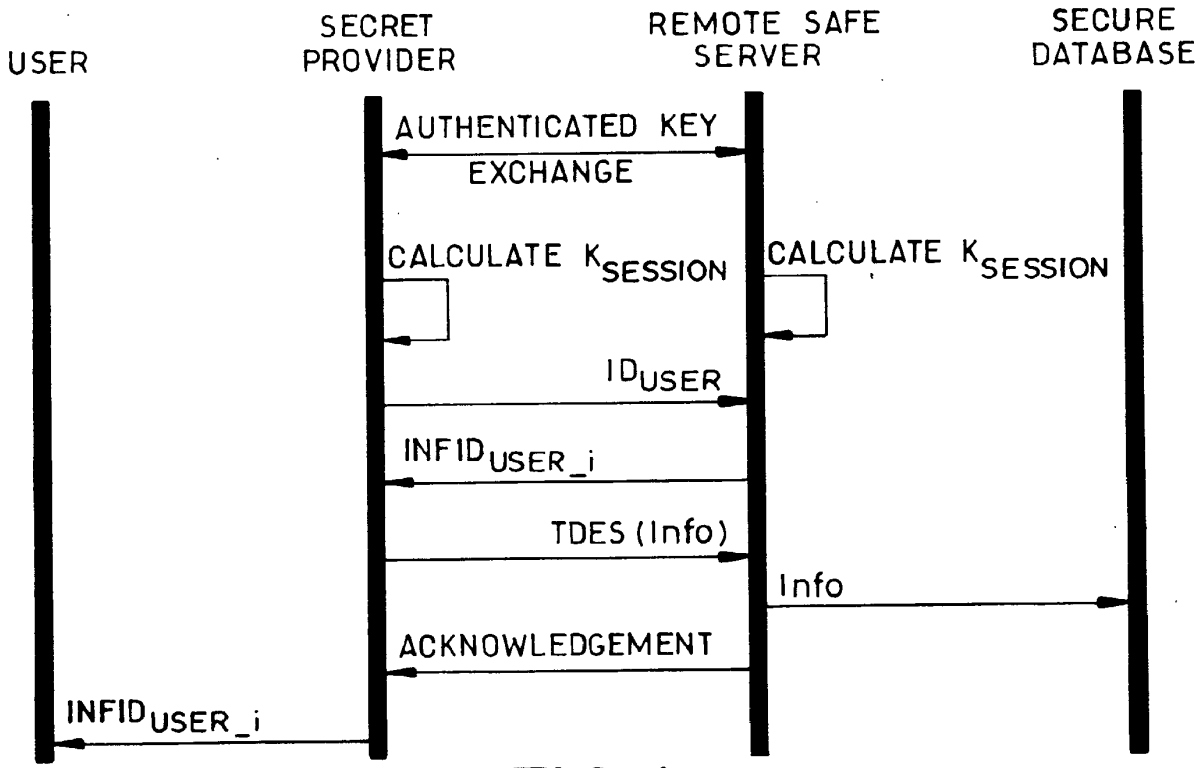

USER
SECRET
PROVIDER
REMOTE SAFE
SERVER
SECURE
DATABASE
AUTHENTICATED KEY
EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
ID_{USER}
$INFID_{USER\_i}$
TDES (Info)
Info
ACKNOWLEDGEMENT
$INFID_{USER\_i}$

FIG.6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/04088

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F17/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 337 357 A (CHOU WAYNE W ET AL) 9 August 1994 (1994-08-09) figure 1 column 3, line 26 -column 4, line 37	1-11
X	EP 0 843 449 A (SUNHAWK CORP INC) 20 May 1998 (1998-05-20) column 5, line 8 -column 8, line 19 figures 2-5	1-11
X	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) page 10, line 7 -page 11, line 29 figures 1,5,6,9	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 August 2001	14/08/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Papastefanou, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/04088

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5337357 A	09-08-1994	CA 2120816 A	18-12-1994
		EP 0636962 A	01-02-1995
EP 0843449 A	20-05-1998	US 5889860 A	30-03-1999
		CA 2220457 A	08-05-1998
		JP 10301904 A	13-11-1998
WO 9842098 A	24-09-1998	AU 6759198 A	12-10-1998
		EP 0968585 A	05-01-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2005 (02.06.2005)

PCT

(10) International Publication Number
WO 2005/050450 A1

(51) International Patent Classification[7]: G06F 11/30

(21) International Application Number:
PCT/US2004/038124

(22) International Filing Date:
15 November 2004 (15.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/715,035 17 November 2003 (17.11.2003) US
10/, 17 May 2004 (17.05.2004) US

(71) Applicant *(for all designated States except US)*: **MARGENT DEVELOPMENT, LLC** [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

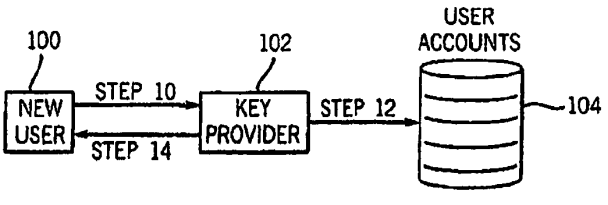
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DIGITAL CONTENT SECURITY SYSTEM



(57) Abstract: A Personal Digital Key Digital Content Security System (PDK-DCSS) is used to protect computers from unauthorized use and protect the digital content (110) stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are 1) a standard hard drive device (108), with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and 2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: 1) hard drive (108) access control for providing Drive-Level and Sector-Level protection and 2) operating system-level independent file protection for providing File-Level and Network-Level protection.

WO 2005/050450 A1

DIGITAL CONTENT SECURITY SYSTEM

REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. patent application Serial No. 10/xxx,xxx filed May 17, 2004, which is a continuation-in-part of U.S. patent application Serial No. 10/715,035 filed November 17, 2003, which is a continuation-in-part of U.S. patent application Serial No. 10/153,979 filed May 23, 2002, which is a continuation-in-part of U.S. patent application Serial No. 09/750,487 filed December 27, 2000 and Serial No. 10/016,857 filed December 14, 2001, all of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to digital content security systems and, more particularly, to a digital content security system and method that provides different levels of protection of a computer or other storage device and the digital content stored thereon.

BACKGROUND OF THE INVENTION

The market for downloading digital content online is rapidly climbing because distribution of such content is inexpensive, fast, and easy and the quality of the content itself is acceptable. The market, however, remains disorganized due to competing standards, competing companies, discontented artists and producers, and outright theft of digital content.

Digital rights management (DRM) companies seek to solve the foregoing problems by delivering the digital content from the real producers to the right customers and ensuring that everyone who should be paid in fact is paid. DRM seeks to get everyone paid by managing the multiple steps for distributing digital content (music, video, software) online: watermarking, encryption, transaction management, and rights management. Some DRM companies perform all these steps, while other DRM companies specialize in one or two steps of the process.

First, watermarking stamps each piece of digital content with a digital mark so it can be tracked wherever it goes. Digital watermarks are just like paper watermarks, except they cannot be seen or heard. Special software is required to read a digital watermark.

Second, encryption scrambles watermarked digital content and stores it inside a digital safe for shipment around the Internet. The safe protects the content during shipping by allowing only those with the right software key to the safe to decrypt and use the content.

Third, transaction management handles actual payments for the digital content using credit card techniques found elsewhere in e-commerce. An order is placed, a credit card number is taken, account status is checked, and the exchange is authorized.

Finally, rights management manages the information about the digital content itself: what it is, who gets it, how it is delivered, how many times it may be used, how long the rights last, who gets paid, how much they get paid, and how. This information travels with the digital content in something called a digital permit. The permits rests on top of the digital content as it travels the Internet and allows legal users to enjoy the digital content for as long as the rights last.

The primary objective of DRM companies is to deploy technologies that protect digital content as it is distributed online. Some of these proposed technologies and DRM in general are discussed in the article "Digital Rights Management May Solve the Napster 'Problem'," *Technology Investor*, October 2000, pp. 24-27. Although such technologies should reduce the amount of digital theft, they generally favor the content provider at the expense of the consumer or favor the consumer at the expense of the content provider. That is, the rights of either the content provider or the consumer are compromised. For example, some technologies severely limit the consumer's ability to make extra copies of digital content even when the digital content is solely for personal use. Other technologies facilitate the making of copies of digital content which can be used by different

consumers without the content provider being compensated by each consumer. The present inventor has discovered an improved DRM system and method that effectively balances and protects the rights of both the consumer and the content provider. In addition, the present inventor has discovered an associated digital content security system for protecting computers and other storage devices from unauthorized use and protecting the digital content stored on computers and other storage devices from being wrongfully accessed, copied, and/or distributed.

SUMMARY OF THE INVENTION

In accordance with the foregoing, there is disclosed a Personal Digital Key Digital Content Security System (PDK-DCSS) for protecting computers from unauthorized use and protecting the digital content stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are (1) a standard hard drive device, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and (2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: (1) hard drive access control for providing Drive-Level and Sector-Level protection and (2) operating system-level independent file protection for providing File-Level and Network-Level protection. A number of alternative embodiments are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a flow chart of a method of managing digital rights in accordance with the present invention;

FIGS. 2, 3, and 4 are block diagrams of portions of a DRM system for implementing the method in FIG. 1;

FIG. 5 is a conceptual model of core options for acquiring digital content that can be encoded to produce key-secured content and core options for playing back the key-secured content;

FIG. 6 is a block diagram for implementing a core acquisition option of downloaded content;

FIG. 7 is a block diagram for implementing a core acquisition option of store-bought content;

FIG. 8 is a block diagram for implementing a core acquisition option of broadcast content;

FIGS. 9a and 9b are block diagrams for implementing a core playback option of stand-alone devices;

FIG. 10 is a block diagram for implementing a core playback option of networked devices;

FIG. 11 is a block diagram of a standard computer hard drive incorporating an integrated PDK-RDC (receiver/decoder circuit) for the purpose of enabling multiple methods of securing digital content;

FIG. 12 is a block diagram for implementing Drive-Level protection and Sector-Level protection in connection with the computer hard drive;

FIG. 13 is a flow chart of the logic executed by the PDK-RDC for implementing Drive-Level protection and Sector-Level protection;

FIG. 14 is a block diagram for implementing File-Level protection in connection with the computer hard drive; and

FIG. 15 is a block diagram for implementing Network-Level protection by expanding File-Level protection to a network environment.

While the invention is susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and will be described in detail herein. However, it should be understood that the invention is not intended to be limited to the particular forms disclosed. Rather, the

invention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DESCRIPTION OF SPECIFIC EMBODIMENTS

Turning now to the drawings and referring initially to FIG. 1, there is depicted a method of managing digital rights in accordance with the present invention. First, a new user requests a physical electronic key or data unit from a key provider (step 10). The key provider may offer a web site on the Internet, a toll free telephone number, and/or retail outlet where the key may be acquired. In addition, the key provider may allow a key to be requested in writing, preferably using a form designed by the key provider. In one model the user may acquire as many keys as desired, while in another model each user is only entitled to a single key.

Second, in response to the user's request for a physical key, the key provider establishes a new secure account for that new user in a secure user account database (step 12). The new account may include the following data fields: account number, password, software encryption key, user label, number of users (linked to account), address, telephone number, e-mail address, and custom fields. The custom fields may, for example, include demographic information such as the user's age, gender, marital status, income level, interests, hobbies, etc. The physical key may include the following data fields: user label, account number, software decryption key, and a custom storage area. The user label and the account number serve as a first activation code (or key code) for the acquired physical key. All data fields on the physical key, except for the user label, are preferably encrypted. To allow the user to view his or her account in the future, the user is preferably assigned a login name and the above-noted password.

Third, the key provider ships the physical electronic key to the new user via a package courier such as the U.S. Postal Service, United Parcel Service, or Federal Express (step 14). In one pricing model the physical key is sent to the user at no charge, while in another pricing model the physical key must be purchased by the

user. If the physical key must be purchased by the user, either the user must provide credit/debit card information to the key provider in step 10 to pay with a credit/debit card, or the key provider includes an invoice with the shipped key in step 14.

FIG. 2 is a block diagram of a system for implementing steps 10, 12, and 14 of the method of managing digital rights. The system includes the new user 100, the key provider's web site 102, and the user account database 104.

Referring back to FIG. 1, fourth, the user transmits his or her activation code in the physical key to a digital content provider, who may have a cooperative relationship with the key provider, and requests to purchase digital content (music, video, or software) from that content provider (step 16). The content provider may offer a web site on the Internet containing a listing of digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.

Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As

used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.

Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital content either by providing credit/debit card information to the content provider in step 16 or by paying off of an invoice included with delivered digital content. If the digital content is delivered online, the user is preferably required to provide the credit/debit card information and have such information approved as a prerequisite to delivery of the digital content. If the user possesses more than one physical electronic key and would like the acquired digital content to function with each of the user's keys, all of the

activation codes are applied to the digital content. The content provider charges the user based on the number of keys with which the user would like the digital content to function. For example, the user may be charged the same amount for each activation code, or may be charged a larger amount for one activation code and lesser amounts (e.g., surcharges) for additional activation codes.

FIG. 3 is a block diagram of a system for implementing steps 16, 18, 20, 22, and 24 of the method of managing digital rights. The system includes the new user 100, the content provider 106, the key provider's web site 102, the digital content database 108, and the acquired digital content 110.

Returning to FIG. 1, ninth, the user enters the encrypted digital content into a playing device of a type suitable for playing the digital content (step 26). The device may, for example, be an MP3 player, a personal computer, a DVD player, a CD player, a cellular phone, or other portable device. In one embodiment, the device contains a wireless transceiver adapted to receive a radio frequency signal transmitted by a corresponding wireless transceiver in the user's physical electronic key. The wireless transceiver in the device is optionally tracked and "secured" for audit purposes by permanently including a unique identifier assigned by the device manufacturer in the transceiver.

Tenth, with the user's physical electronic key within a short range (e.g., few meters) of the playing device, the playing device reads (1) the first activation code carried in a secure radio frequency signal transmitted by the transceiver in the physical key to the transceiver in the device and (2) the second activation code marked on the encrypted digital content (step 28). The device contains decryption software or hardware for decrypting the encrypted digital content to the extent necessary to read any encrypted portion of the second activation code.

Eleventh, the playing device compares the first activation code and the second activation code and determines whether the first activation code is associated with the second activation code (step 30). Steps 29 and 30 may be performed, for example, when the user presses a "play" button on the playing device or when the

user first enters the encrypted digital content into the playing device. If the first activation code is associated with the second activation code, the device decrypts and plays the digital content. If the first activation code is not associated with the second activation code, the device does not play the digital content. If the second activation code is simply the same as the first activation code, then the foregoing comparison determines whether there is a match between the first activation code and the second activation code. In a preferred embodiment, the device continues to play the digital content only while the physical key is sufficiently close to the device to communicate the first activation code to the device and allow the device to compare the first activation code to the second activation code at least partially encrypted with the digital content even while the digital content is being played. If the physical key is moved out of range, the device is no longer enabled to decrypt and play the digital content. In an alternative embodiment, once the device is initially enabled to decrypt and play the digital content, the device remains enabled until either the "play" function is stopped, a play track/song ends, or the digital content is removed from the device, even if the physical key is moved out of range such that the key can no longer communicate the first activation code to the device.

FIG. 4 is a block diagram of a system for implementing steps 26, 28, and 30 of the method of managing digital rights. The system includes the encrypted digital content 110, the key-enabled playing devices 112, and the user's physical electronic key 114.

As stated above, the user's physical electronic key and the key-enabled playing device contain respective wireless transceivers to communicate the activation code in the key to the device. In a preferred embodiment, the transceivers are small, inexpensive *Bluetooth* radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are plugged into electronic devices, which can then communicate over short distances and through obstacles by means of radio waves. *Bluetooth* is a term used to describe the

protocol of a short range (e.g., about 10 meters) frequency-hopping radio link between devices containing the radio chips. These devices are then termed "*Bluetooth*-enabled." The secure radio link replaces a cable that would otherwise be used to connect the devices. Further details concerning *Bluetooth* wireless technology may be obtained from www.bluetooth.com.

Wireless technologies other than *Bluetooth* may be used to communicate the activation code from the user's physical electronic key to the playing device. One example of an alternative wireless technology is known by a trade term "Wi-Fi," which is short for wireless fidelity and is another name for IEEE 802.11 b. Products certified as Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA) are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

In other alternative embodiments, the communication between the user's physical electronic key and the playing device is not wireless. Rather, in one alternative embodiment, the user's physical electronic key communicates the activation code to the playing device via a transmission line such as a serial cable that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

The above-described DRM method and system for implementing the method are advantageous in that they afford the key holder with tremendous versatility in copying and using encrypted digital content for personal use. At the same time, the rights of the content provider are protected because only the key holder with a key-enabled device can use the encrypted digital content. The key holder can copy the encrypted digital content as many times as desired, but can only play the encrypted digital content on a key-enabled device that is enabled with the physical electronic key coded to decrypt the encrypted digital content. Thus, the digital content, even

when copied, remains personal to the key holder. Individuals other than the key holder cannot use the encrypted digital content, even if they copy it, because both the original and copies of the encrypted digital content are still encrypted and the individuals do not hold the physical electronic key coded to decrypt the digital content.

A core element of the present invention is the concept of a portable, physical electronic key that is personal to a particular user. The physical key represents a DRM solution that fully addresses the needs of both consumers and publishers of digital content. The physical key is permanently associated with a user's digital content library. At the time of content acquisition, the physical key becomes permanently associated with the newly acquired content. The user is now "linked" to that acquired content. A user (e.g., individual or family) may own as many physical keys as desired, but every piece of encrypted digital content purchased is tied to one specific key. The user may duplicate or transfer the acquired content to any media or device for playback as many times as desired, as long as the associated physical key is present. Thus, the present invention guarantees that the acquired content is played only by the user who has legitimately paid for it. The present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to FIG. 5, the present invention fully supports the use of "key-secured" digital content 125 with all core content acquisition options and all core playback options. The key-secured digital content 125 is encoded with a second activation code associated with a first activation code stored on the user's physical electronic key. The core acquisition options include downloaded content 120, store-bought content 122, and broadcast content 124. The core playback options include stand-alone devices 126 and networked devices 128. Each of these options are described in further detail below.

Referring to FIG. 6 generally, as already noted in FIGS. 1 through 4, a primary application of the present invention is its use in the downloading of digital

content from the Internet. A consumer shops a content distributor's website and selects a piece of content they wish to purchase (music, movies, software, E-books, etc.). The consumer then provides the web site with standard on-line purchase information including the selection's title and method of payment, as well as their physical electronic key information. Transparent to the consumer, the distributor's web site links to the key provider's web site and transmits the physical key information for validation. The key provider's web site then provides the distributor's web site with the information required to prepare the acquired content for secure shipment to the consumer (or notification that the physical key was invalid). The key provider's web site records the transaction for later billing. Finally, the distributor's web site retrieves a copy of the digital content from its library, permanently links it to the consumer's physical key (by using the key's information to encrypt it), and transmits the secured content to the consumer. The consumer is now free to duplicate the content as often as desired, and to play the content on any key-enabled playback device.

Referring to the specifics of FIG. 6, the process of implementing the core acquisition option of downloaded digital content 120 (see FIG. 5) proceeds as follows. At step 130, a receiver/decoder circuit 140 retrieves an account number from a consumer's physical key (transponder) 142 over a secure RF link. At step 131, the consumer enters such data as a password, purchase selection, and method of payment via the consumer's personal computer 144. The data is transmitted to a content distributor's web site 146 from the consumer's personal computer 144. At step 132, the content distributor's web site 146 transmits the account number and password to a key provider's web site 148. At step 133, the key provider's web site 148 authenticates all data against its database 150 and, if authentic, returns such information as the account number, user label, number of users, and software encryption key to the distributor's web site 146. If the data is not valid, the key provider's web site 148 sends a message to the distributor's web site 146 indicating the same. A counter, used for the key provider's billing purposes, is incremented. At

step 134, the distributor's web site 146 pulls the purchased content file from its database 152, encrypts it with the software encryption key it received in step 133, and builds a final key-secured content file that is then transmitted to the consumer's personal computer 144. Charges are assessed based on the number of users, etc. and billed to the consumer according to the method of payment. At step 135, invoices 154 are generated and sent to content distributors by the key provider's web site 148 on a regular cycle.

Optionally, to enable content providers to offer sample content (e.g., limiting playback to the device on which the content was originally downloaded, for a specified period of time) a special "enhanced" version of a receiver/decoder circuit 140 can be produced. These enhanced receiver/decoder circuits (primarily for PC's) would each include a unique identification number and additional functionality enabling them to "talk" to a key provider's web site 148 to acquire secured timing information. Sample content files may include the following information (in their encrypted header section):

- identification number of enhanced receiver/decoder circuit used for downloading and transmitted by the receiver/decoder circuit to the key provider's web site at the time of content purchase;
- hour stamp (i.e., the hour in which the content was downloaded; and
- life hours (i.e., number of hours content remains valid, such as perpetual, one hour, 24 hours, 48 hours, etc.).

The above information is used by an "enhanced" receiver/decoder circuit during playback to determine whether a content file has "expired" or is attempting to play on an unauthorized device (i.e., any device except the device on which the content was originally downloaded). This capability allows content distributor web sites to distribute limited-use samples with associated tiered-pricing models.

Referring to FIG. 7 generally, the present invention can be extended to store-bought content. To fully integrate store-bought content into the present invention, traditional store-bought content is modified in two ways. First, the content is

distributed in a copy protected format (e.g., using any valid copy protection technology). Second, the content contains a unique content serial code. The content serial code may be contained either directly in the digital content or as a physical label. Each content serial code is designated by a content distributor during manufacturing and stored in the key provider's database. This database is later used to validate that each content serial code is unique and used only a prescribed number of times. To a consumer, a content serial code on their newly purchased store-bought content represents a download of a key-secured version of that content for free or a prescribed price. This key-secured copy provides the consumer with exactly the same advantages and freedoms as any other key-secured content. From the consumer's standpoint, the download process occurs exactly as any other standard key-secured content download with the exception of how the payment is handled. The "payment" is the content serial code. By providing all of the advantages of the present invention to consumers of legacy-capable store-bought content (by way of "content serial code downloads"), the scheme provides the industry with the first complete DRM solution.

Referring to the specifics of FIG. 7, the process of implementing the core acquisition option of store-bought digital content 122 (see FIG. 5) proceeds as follows. At step 160, a receiver/decoder circuit 170 retrieves an account number from a consumer's physical key (transponder) 172 over a secure RF link, and the consumer's personal computer 174 reads a content serial code from the store-bought content 122. The store-bought content 122 contains the content serial code that uniquely identifies the content. The format of the content serial code may, for example, be PPPP.FFF.0123456789 where PPPP is a provider identification, FFF is a facility identification, and the numbers represent a sequence number. The store-bought content 122 incorporates a copy protection scheme such as Macrovision™, key2audio™, or SafeAudio™. Disc "copy flags" (specified in SDMI standards) may also be set to further inhibit duplication efforts.

At step 161, the consumer enters such data as a password and purchase selection via the consumer's personal computer 174. The previously-read content serial code specifies that the method of payment is to a "content serial code-credit" (i.e., there is typically no charge for this download because the content serial code confirms that the download in process is of content that the consumer has already legitimately purchased). The data is transmitted to a content distributor's web site 176 from the consumer's personal computer 174. At step 162, the distributor's web site 176 transmits the content serial code, account number, and password to a key provider's web site 178. At step 163, the key provider's web site 178 authenticates all data against its databases 180 and 182 and, if authentic, returns such information as the account number, user label, number of users, software encryption key, and paid-flag (indicating the content serial code has been validated) to the distributor's web site 176. The key provider's web site 178 now sets the paid-flag to disable any further downloads and records the account number field in the content serial code database 182 for auditing purposes. If the data is not valid, the key provider's web site 178 sends a message to the distributor's web site 176 indicating the same. A counter, used for the key provider's billing purposes, is incremented. Each entry in the content serial code database 182 may include the following data fields: CDC #, paid-flag, and account number. At step 164, the distributor's web site 176 pulls the content file from its database 184, encrypts it with the software encryption key it received in step 163, and builds a final key-secured file that is then transmitted to the consumer's personal computer 174. No charge is typically assessed because a valid content serial code serves as "payment" for the download. At step 165, invoices 186 are generated and sent to content distributors by the key provider's web site 178 on a regular cycle.

Referring to FIG. 8 generally, the present invention can be extended to broadcast content. To fully integrate broadcast content into the present invention, traditional broadcast content is only minimally modified. The modification is that the broadcast content is transmitted in a copy protected format (such as the DVD

standard known as Content Scramble System (CSS)). The remainder of the process is described below. A key-enabled recording device, incorporating a unique identifier, receives copy-protected broadcast content. If only playback of the broadcast content is desired, basic decoding (e.g., CSS) is performed and the broadcast content is sent on for playback. If the consumer wishes to record the broadcast content, however, the recording device performs additional steps prior to sending the broadcast content on for playback. The recording device connects to the key provider's web site to validate the recording device's internal identifier and the consumer's physical key. If both are valid, the recording device translates the broadcast content into a key-secured format by encoding it with the consumer's activation code, and then stores the key-secured content file, with its identifier permanently embedded within, for later use. The end result is key-secured broadcast content that provides the owner of the associated physical key all the freedoms and advantages of the present invention. Although the content was originally broadcast, it cannot be illegally copied or distributed. The present invention can be applied to pay per view offerings, as well as standard broadcast material.

Referring to the specifics of FIG. 8, the process of implementing the core acquisition option of broadcast digital content 124 (see FIG. 5) proceeds as follows. At step 180, a receiver/translator/recording device 190 receives digitally broadcast content in copy-protected format from a source 192 such as satellite, cable, Internet, or over-air. The broadcast content may be copy-protected using a copy-protection technology such as an enhanced CSS scheme. If a consumer wishes to only play (not record) the broadcast content, basic decoding (e.g., CSS decoding) is performed and the broadcast content is passed through to presentation device 194 for playback. The remaining steps below may be skipped.

If, however, the consumer wishes to record the broadcast content, the following additional steps are performed prior to sending the broadcast content on for playback. At step 181, the receiver/translator/recording device 190 retrieves an

account number from the consumer's physical key (transponder) 196 over a secure RF link. At step 182, the receiver/translator/recording device 190 transmits the account number and its recorder serial code to a key provider's web site 198. Each device 190 contains a recorder serial code that uniquely identifies the device. The format of the recorder serial code may, for example, be MMMM.FFF.0123456789 where MMMM is a manufacturer identification, FFF is a facility identification, and the numbers represent a sequence number. At step 183, the key provider's web site 198 authenticates the data against its databases 200 and 202 and returns an "approved" or "rejected" response. A counter, used for the key provider's billing purposes, is incremented. At step 184, if a "rejected" response is received, the broadcast content cannot be recorded. If an "approved" response is received, the receiver/translator/recording device 190 translates the decoded content into a key-secured format by encoding it with the consumer's activation code, and records the key-secured content, with the recorder serial code permanently embedded within, to a storage device (that can optionally be an external device). The broadcast content can now be copied to and played back on any key-enabled playback device. At step 185, invoices 199 are generated and sent to content distributors by the key provider's web site 198 on a regular cycle. While providing excellent additional security and protections, steps 182 and 183 are not mandatory for the present invention to function with broadcast content. It may be desirable, for cost purposes, to produce receiver/translator/recording devices 190 not capable of communicating with the key provider's web site 198.

Referring to FIGS. 9a and 9b generally, having acquired key-secured digital content and produced copies for playback on various devices such as a portable CD player, personal computer, home theater, etc., a consumer is now ready to use the digital content. Playback of key-secured content occurs as follows. A key-enabled playback device transparently reads information from a consumer's physical key and from the content file the consumer has requested to play. The pieces of information are then compared to validate that the physical key "matches" the content to be

played. If the elements match, the device begins playback of the content. If the elements do not match, the device will not play the content and, depending upon the device's capabilities, may display an "invalid content" message. From a consumer's point of view, when used with legitimately-acquired content, the process is entirely transparent, effortless, and non-intrusive. The consumer is free to use their content on any key-enabled playback device, with the only restriction being that the content can be played only when the associated physical key is present. As noted above, the present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to the specifics of FIGS. 9a and 9b, the process of implementing the core playback option of stand-alone devices 126 (see FIG. 5) proceeds as follows. At step 210, a consumer requests playback of a key-secured content file via a playback device 220. The playback device 220 may, for example, be the consumer's personal computer (FIG. 9a) or a stereo amplifier (FIG. 9b) with integrated compact disc reader/player. At step 211, a receiver/decoder circuit 222 searches for a physical key (transponder) 224. The circuit 222 may be a separate component from the playback device 220 as in FIG. 9a or integrated into the playback device 220 as in FIG. 9b. If the physical key is not found, the playback device 220 displays an "invalid content" message. If the physical key is found, the receiver/decoder circuit 222 retrieves all available information from the physical key 224 over a secure RF link. At step 212, the user labels in the physical key 224 and the key-secured content file are compared. If the user labels do not match, the playback device 220 displays an "invalid" message. If the user labels do match, the receiver/decoder circuit 222 retrieves the software decryption key from the physical key 224 over the secure RF link between the physical key 224 and the playback device 220 and begins decryption of the encrypted portion of key-secured file. When the account number is decrypted, it is matched against the account number retrieved from the physical key 224. If the account numbers do not match, the playback device 220 displays an "invalid content" message. If the account numbers

do match, the software decryption key is used by the playback device 220 to decrypt remaining data in the key-secured file for playback. The user label and the account number in the physical key serve as a first activation code, and the user label and the account number in the content file serve as a second activation code. These activation codes must match (or have some other predetermined association) in order for playback to proceed.

Referring to FIG. 10 generally, while stand-alone playback devices (e.g., CD players, PCs, DVD players, etc.) are currently the norm, the convergence of these devices and the Internet will lead to an environment where centralized digital distribution systems proliferate. Security of content in these environments is critical yet challenging to accomplish without imposing great restrictions. The present invention can provide security to a centralized digital distribution system and, in addition, offers many important enhancements that greatly increase the convenience and usability of such a system. These enhancements include integration of the physical key into a portable handheld computer which then doubles as the system remote. In addition to controlling all networked components, the remote is used for tasks such as purchasing content from the Internet, and tracking the movement of a user throughout a facility to provide automatic "content following" (i.e., where content playback follows the user from room to room). The centralized nature of the digital content distribution system means that only one storage device is required to maintain a consumer's entire digital content library (e.g., music, movies, software, E-books, etc.) and to feed that content to any networked playback device.

Referring to the specifics of FIG. 10, there is shown a centralized digital content distribution system for implementing the core playback option of networked devices 128 (see FIG. 5). The system is used in an establishment such as a residence or entertainment facility. The system includes a digital content server 310, a distribution hub 312, a plurality of remote clients 314, and a portable remote control 316. The digital content server 310 stores digital content acquired from a source 318 such as satellite, cable, Internet, or over-air. In addition, the digital

content server 310 may store digital content uploaded from a standard component 324. The plurality of remote clients 314 are located in different rooms of the establishment and linked to the digital content server 310 via the distribution hub 312 or switch. The remote clients 314 are linked to the distribution hub 312 by a backbone transmission network 315. The backbone transmission network 315 may be wireless or wired with fiber optic cables, coaxial cables, or twisted pair cables, may employ a networking protocol such as Ethernet, Wi-Fi, Arcnet, or ATM (Asynchronous Transfer Mode), and may employ a communications protocol such as TCP/IP. Each remote client 314 includes a network interface card (NIC) for interfacing with the backbone transmission network 315.

The remote control 316 is adapted to communicate with each of the remote clients 314 and select the digital content stored in the digital content server 310. The remote control 316 is essentially a personal digital assistant (i.e., hand-held computer) including a display and added remote control circuitry. The display may, for example, be a liquid crystal display (LCD). The added remote control circuitry includes "system remote" circuitry and "universal remote" circuitry.

The "system remote" circuitry in the remote control 316 is for establishing a first wireless transmission link 320 with each of the remote clients 314. The first wireless transmission link 320 may be a secure radio link (RF) as shown or an infrared link (IR). Upon establishing the first wireless transmission link 320 with one of the remote clients 314, the remote control 316 serves as a system remote capable of (1) displaying, scanning, and selecting the digital content available on the digital content server 310 and downloading the selected digital content from the digital content server 310 to the linked remote client 314 and (2) controlling the digital content server 310 to acquire or download digital content from a source 318 such as satellite, cable, Internet, or over-air. As used herein, the term "download" and similar variations thereof (e.g., downloaded, downloading, etc.) is intended to cover the transfer of content from one device to a receiving device whether the content is stored on the receiving device or merely "streamed" to the receiving

device for immediate playback. The remote control 316 preferably includes a display for displaying the digital content. The display may, for example, be a liquid crystal display (LCD). As a user holding the remote control 316 moves from room to room of the establishment, the remote control 316 successively establishes wireless transmission links 320 with the remote clients 314 in the respective rooms. In this way, the digital content available on the digital content server 310 follows the user's movement from room to room.

In a preferred embodiment, the first wireless transmission link 320 is a secure radio link established by matching transceivers in the remote control 316 and each remote client 314. The matching transceivers are preferably small, inexpensive Bluetooth™ radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are integrated into the respective remote control 316 and each remote client 314, which can then communicate over short distances and through obstacles by means of radio waves. Wireless technologies other than Bluetooth, such as Wi-Fi, may be used to communicate remote control signals between the remote control 316 and each remote client 314.

The "universal remote" circuitry in the remote control 316 is for establishing a second wireless transmission link 322 with standard components 324 connected to the remote clients 314. The second wireless transmission link 322 is preferably an infrared link (IR) as shown. Upon establishing the second wireless transmission link 322 with one of the standard components 324, the remote control 316 series as a universal remote capable of operating the standard component 324. The standard component 324 may, for example, be an audio receiver (stereo amplifier), an audiovisual receiver, a video monitor (television), etc. The standard components 324 may be physically separate from, but linked to, the respective remote clients 314 or may be physically integrated into the respective remote clients 314 like integrated device 324c.

The digital content stored on the digital content server 310 may be formatted as a compact disc (CD), digital video disc (DVD), MP3, electronic book, software, etc. When the remote control 316 is linked to one of the remote clients 314, a user may scan and select digital content to be downloaded from the digital content server 310 to the remote client 314 and converted by the remote client 314 to a standard playable format (e.g., analog format) that can be played on the associated standard component 324. The selected digital content is downloaded from the digital content server 310 to the remote client 314 as raw digital data packets. The remote client 314, in turn, converts the downloaded digital content to a standard component output(s) compatible with a standard component 324 connected to the remote client 314, and the standard component 324 plays the digital content. Ports may, for example, include S-Video, RCA jacks, serial ports, Universal Serial Bus, Ethernet, Wi-Fi, Firewire™, Bluetooth, RF, or other similar outputs. The standard component 324 incorporates, or is linked to, audio speakers for broadcasting any audio signals received from the remote client 314 and a video monitor for displaying any video signals received from the remote client 314.

All content is stored on the digital content server 310 digitally, and is key-secured if obtained via the download or broadcast acquisition options of FIGS. 6 and 8. If the digital content is key-secured, the plurality of remote clients 314 include decryption circuitry (i.e., receiver/decoder circuit) for unlocking the digital content. The digital content selected for download from the digital content server 310 to a remote client 314 preferably remains encrypted until converted to a standard component output(s) in the remote client 314. The remote client 314 acts as a converter between key-secured digital content from the digital content server 310 and the standard component output(s). To decrypt the selected digital content, the remote control 316 contains a physical key initially acquired from a key provider in accordance with the present invention. The digital content is initially acquired from a content provider 326 that marks the digital content with an activation code associated with the physical key. The decryption circuitry in the

remote client 314 receives an activation code from the remote control 316 via the wireless transmission link 320 and is enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content. If the activation code in the remote control 316 is not associated with the activation code in the digital content, the remote client 314 will not unlock and convert the digital content.

In an alternative embodiment, the remote clients 314 are eliminated and the standard components 324 are linked directly to standard component outputs of the distribution hub 312 by the backbone transmission network 315. In this case, the distribution hub 312 serves as a switch, and the digital content server 310 contains the decryption circuitry for unlocking the digital content. As the digital content is decrypted, it is converted to a playable format and fed to the distribution switch 312 for delivery to the appropriate standard component 324. The decryption circuitry in the digital content server 310 receives the activation code from the remote control 316 and is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content.

Instead of decrypting the digital content so that it can be played, the digital content may be downloaded (or "passed through") in its encrypted format to a storage device such as a media burner 324a or computer hard disk 324b for storage thereon. When a user ultimately desires to play the stored digital content on a media player, the media player must contain the decryption circuitry for unlocking the digital content. After unlocking the digital content, the media player converts the unlocked digital content to a playable format and plays the digital content. The decryption circuitry in the media player receives the activation code from the remote control 316 or physical key with the same activation code. The media player is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 or physical key is associated with the activation code in the digital content.

In addition to downloading selected digital content from the digital content server 310 to the remote clients 314, data (e.g., MP3, CD, DVD, software, etc.) from the standard components 324 can be uploaded to the digital content server 310 and stored digitally thereon. This allows for storage of legacy content on the digital content server 310.

Referring to FIG. 11 generally, a digital content security system and method protects computers from unauthorized use and protects the digital content stored on computers from being wrongfully accessed, copying, and/or distributed. The basic components of the Personal Digital Key Digital Content Security System (PDK-DCSS) are (1) a standard hard drive device 330, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) 332 integrated into the controller 334, and (2) a PDK-Key 336 associated with the PDK-RDC as described above. The standard computer hard drive 330 incorporates the integrated PDK-RDC 332 for the purpose of enabling multiple methods of securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the PDK-RDC 332 as being integrated with the hard drive's controller 334, all OS-level protections described below can be implemented using externally-based PDK-RDCs.

A PDK hard drive 330 is similar to any standard, currently available hard drive with the exception of the PDK-RDC 332 (which is integrated into the drive's controller circuit 334). A PDK-RDC 332 is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content. Additionally, this circuit 332 is able to secure the hard drive 330 itself. This is implemented by the circuit 332 enabling or disabling the hard drive's controller 334 depending on whether an associated PDK-Key 336 (one which is uniquely and permanently associated with the PDK hard drive 330) is present. Each PDK hard drive 330 would typically be delivered with its own PDK-Key 336.

Secure RF communications between a PDK-Key 336 and its associated hard drive 330 occurs in the same manner as described above. It should be noted that

software drivers can optionally be designed to allow for dynamic key assignment (assigning of keys after purchase to enable key swapping, or assigning of individual keys to multiple devices).

The PDK-Key and RDC technology is utilized to provide two categories of protection:

1) Hard drive access control - where an entire drive 330 is either completely accessible (unlocked) or inaccessible (locked), and/or individual data sectors or clusters of data sectors are optionally encrypted/decrypted, depending on whether the specific PDK-Key 336 associated (and shipped) with the drive 330 is within range. This category of protection can be accomplished transparently to the operating system (OS) responsible for managing the drive.

2) OS-level independent file protection - where the drive's RDC 332 functions independently of the drive 330 to protect individual files (typically copyrighted material) from wrongful copying. In this role, the RDC 332 works with any PDK-Key 336 (not just the one delivered with the drive 330) and any PDK-compliant file (they do not have to be stored on or associated with the hard drive 330). This category of protection requires an OS-level software driver be run under the OS responsible for managing the drive.

By utilizing these two categories of protection in various ways, four unique levels of content protection are enabled. Two of the levels (Drive-Level and Sector-Level) do not require external software support, while the remaining two (File-Level and Network-Level) require software drivers, as well as a stand-alone application for Network-Level implementations. Each of the four levels is defined below.

Referring to FIGS. 12 and 13 for Drive-Level protection, when implemented, a PDK hard drive 330 will only function when the associated PDK-Key 336 is within range. The drive's controller 334 is disabled whenever the PDK-Key 336 is not present. The contents of files stored on the drive 330 are not encrypted. The Drive-Level protection feature is designed to protect the hard drive's owner by locking access to the PDK hard drive 330 whenever the associated PDK-

Key 336 is not present (i.e. when the owner momentarily steps away from the computer, if the computer is stolen, etc.).

Referring to FIGS. 12 and 13 for Sector-Level protection, when enabled, every sector (or cluster of sectors) read or written is encrypted/decrypted by the RDC 332 using the drive's associated PDK-Key 336. Because the encryption is performed at Sector-Level as opposed to File-Level, the encoding can be accomplished without requiring any changes, involvement, or acknowledgement of the OS responsible for managing the drive. The Sector-Level protection feature is designed to further protect the hard drive's owner (beyond Drive-Level protection) by encrypting the contents of the files stored on the drive, without requiring any software modifications (OS, application, etc.). The security advantage is that if the drive access is in some way defeated, the contents of files on the drive are still protected. It should be noted that if users retrieve files from drive and purposely transfer them anywhere else (via email, memory sticks, etc.), the data will no longer be protected. Drive-Level protection and Sector-Level protection may be used individually or in combination. Also, as noted above, it should be understood that Sector-Level protection may be applied to individual data sectors or clusters of data sectors.

FIG. 13 illustrates the logic executed by the RDC 332 for implementing Drive-Level protection and Sector-Level protection. The logic ensures OS-level commands (save entire file, read entire file, etc.) are given adequate time to complete. This enables implementation of logic without requiring OS changes, involvement, or acknowledgement.

Referring to FIG. 14 for File-Level protection, implemented as an OS-level software driver utilizing the PDK-RDC 332 integrated in the PDK hard drive 330, File-Level protection provides standard PDK digital rights management services and functionality as described above. As needed, the driver instructs the RDC 332 to acquire PDK-Key information, validate the key-to-file match, and use the key's information to perform actual encryption/decryption of the file (as a whole, not at

the sector level). In the illustrated example, the file ABC 338 (which can reside on any storage device, in memory, etc.) is compared to any PDK-Key 336 within range of the PDK-RDC 332. If a match is found, the PDK-RDC 332 will decrypt the file 338 for use with whatever playback mechanism placed the request. Any PDK-Key 336 can be utilized, not just the key 336 associated with the PDK hard drive 330. When employed for File-Level protection (and Network-Level protection as described below), the PDK-RDC 332 functions independently of the hard drive 330 in which it resides. While PDK-compliant files it encrypts or decrypts may reside on the resident hard drive 330 and may be associated with the drive's PDK-Key 336, they do not have to be. The PDK-RDC 332 can work with other PDK-Keys and files residing on other mediums. When used in this manner, the PDK-RDC 332 can be thought of as just coincidently residing within the hard drive 330. For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

The primary use of File-Level protection is to secure and protect private or copyrighted material from wrongful copying and distribution. Because copies of any PDK-compliant files can only be accessed when the associated PDK-Key is present, File-Level protection enables copies (intended for use by the holder of the associated key) to be produced effortlessly and securely. In addition to the distribution of copyrighted content such as music and movies as described above, software developers can distribute their software products via the Internet with the same ease and security. Software distributed in this manner would allow the legal recipient to make unlimited copies (for backup purposes, use on a home computer, etc.), yet the copies would only function when the associated key is present, preventing unauthorized copies from being wrongfully distributed and used.

The File-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key

holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and pasted into another application (e.g., an email program) thereby defeating the protection. Therefore the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations.

Referring to FIG. 15 for Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application / database called a PDK Document Controller (DC) 340 ruing on a server 342. A DC 340 enables the creation of Groups 342 that list which PDK-Keys 344 are allowed access to files in specific directories. All files stored in directories controlled by the DC 340 are automatically encrypted using the DC administrator's PDK-Key and thereby become PDK-compliant files. This process places all files stored in the DC 340 in a uniformly encrypted format.

Each user request for a file residing in a directory listed in a DC Group 342 results in the following steps. An RDC located in the requester's workstation 346 acquires information from the user's PDK-Key 344 and relays that information to the DC 340. The DC then enables appropriate access as defined by the DC's Group database information. Specifically, the DC 340 performing a lookup of the requester's PDK-Key 344 in the appropriate Group's tables. If the DC 340 determines that the PDK-Key 344 is listed in a Group 342 that also lists the directory containing the file the user wishes to access, the DC 340 knows that a valid PDK-Key 344 was used in the file request and grants access. The requested file is first decrypted with the administrator's PDK-Key, re-encrypted with the requester's PDK-Key 344, and then downloaded to the user's workstation 346. The foregoing process mirrors the process employed when using PDK to download digital media files from the Internet.

The Network-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and paste into another application (e.g., an email program) thereby defeating the protection. Therefore, the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations. The system is well suited for establishing centralized databases of secure documents intended for distribution to entrusted recipients such as personnel in a law firm or medical facility.

While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention. A number of enhancements and variations can be implemented/utilized that effectively broaden the PDK technology's scope and utility. These enhancements and alternative embodiments are summarized below.

Integration of RDCs into Alternative Storage Devices. This embodiment involves integrating RDCs into alternative storage mechanisms beyond those of basic hard drives. These storage mechanisms include pure RAM/ROM-based storage commonly included/used in devices such as PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, and DVR players, as well as portable storage devices such as Memory Sticks, Secure Digital memory cards, or any similar such product, in which case the RDC is either directly installed on the device, or integrated into the device in which the memory cards/sticks are inserted.

When an RDC is utilized in this manner, File-Level and Network-Level security function in the same manner as that described above for PDK hard drives. Drive-Level and Sector-Level security function in the same *logical* manner as that described for hard drives, but the *physical* implementation varies so as to control the bus structure that provides the communications path between the storage mechanisms and their hosting devices. As with PDK hard drives, access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either "ready" or "busy," effectively enabling/disabling the device itself. To save batteries, RDCs used in this manner may only check for the presence of the associated PDK-Key on some periodic basis (versus every read or write sequence). And similar to PDK hard drives, Sector-Level security can be optionally utilized to encrypt/decrypt data traveling over the bus prior to writes and after reads to provide PDK's standard Sector-Level data encoding functionality.

As when utilized in PDK hard drives, the PDK's security features provide the same convenient, non-intrusive, wireless security mechanism for the above-defined devices. This security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely "disabled" to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled.

Dynamic PDK-Key Management. Utilizing dynamic PDK-Key management, PDK-Keys can be assigned to an RDC (whether integrated into a PDK hard drive or some other hosting device, or implemented independently) by a user (versus requiring such assignment at time of production). This capability is accomplished by including the required logic within the RDC's internal firmware (versus using an externally-based software driver to supply such capability).

Using this capability, a user can optionally assign any PDK-Key to act as the RDC's *master* key (the first key assigned to the device). Then by involving this

master key (to prove the original "owner's" validation of the process), the user can assign (or remove) *additional* keys to the PDK-device. The general benefits of this feature include:

- The ability for the individual possessing the *master* key to create backup keys (to be stored and later retrieved in the event the *master* is ever lost), and to allow other users (those possessing *additional* keys) to also access their PDK device(s).
- The option to ship PDK-RDCs (in any configuration, host devices, etc.) without any PDK-Keys. And to allow such devices containing these RDCs (such as PDK hard drives) to optionally function with all or part of the PDK-technology never enabled or utilized. For instance, a user may elect to not enable Drive-Level and Sector-Level security features, but still utilize the functionalities of File-Level and Network-Level security.
- Giving users the option to purchase and associate a PDK-Key at a later time, or importantly, assign a PDK-Key they *already* utilize for another PDK-based device. This allows a user to utilize a single PDK-Key to provide access to all their PDK-based devices.

This built-in (firmware-based) PDK-Key configuration/management capability greatly enhances PDK's overall flexibility and ease of setup/use.

Independent RDC configuration. While integrating an RDC into a hard drive offers numerous benefits, RDCs may exist separately from hard drive mechanisms. In this configuration (as previously defined) an RDC's physical circuitry may exist in the form of a PC Card, a PC expansion board that plugs into a standard PC expansion slot, a USB-based plug-in board, or any other similar design able to interface with a hosting device. Used in this manner, RDCs provide all previously defined functionalities with the exception of basic hard drive access-control.

Buffer Flush & Notification Software Driver. This enhancement involves using a simple software device driver to recognize when a PDK-Key is out of range

(by "watching" for signals from the RDC), and when such a condition is detected to flush (empty) the host system's "read" buffer (effectively clearing any data the system may have been cached in internal memory in order to speed data access), and display a simple message indicating the PDK-Key is in/out of range. This optional mechanism can be utilized with any RDC configuration and on any PDK-protected device.

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

CLAIMS:

1. A method of securing a storage device having a hard drive, comprising:

detecting a portable, physical key with a receiver/decoder circuit associated with the hard drive;

validating the detected portable, physical key with the receiver/decoder circuit; and

permitting access to the storage device or a portion thereof with the receiver/decoder circuit if the detected key is validated.

2. The method of claim 1, wherein the receiver/decoder circuit resides in the storage device.

3. The method of claim 1, wherein the detecting step includes detecting the key over a secure wireless link.

4. The method of claim 1, wherein the validating step includes determining whether or not the detected key is associated with the storage device.

5. The method of claim 4, wherein the receiver/decoder circuit enables the storage device if the detected key is validated and disables the storage device if the detected key is not validated in order to provide device-level protection.

6. The method of claim 5, wherein the storage device stores digital content that is not encrypted with the key.

7. The method of claim 4, wherein digital content read from or written to the storage device is decrypted or encrypted by the receiver/decoder circuit using the key associated with the storage device in order to provide sector-level protection.

8. The method of claim 4, wherein the key associated with the storage device is initially delivered with the storage device.

9. The method of claim 1, wherein the storage device is selected from a group consisting of PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, DVR players, memory sticks, and memory cards.

10. The method of claim 4, wherein the key associated with the storage device is assigned thereto by a user.

11. A system for securing a storage device of a computer, comprising:

a portable, physical key; and

a receiver/decoder circuit for detecting and validating the key and for permitting access to the storage device or a portion thereof if the detected key is valid, the receiver/decoder circuit being associated with the storage device;

12. The system of claim 11, wherein the receiver/decoder circuit resides in the computer.

13. The system of claim 11, wherein the receiver/decoder circuit detects the key over a secure wireless line.

14. The system of claim 11, wherein the receiver/decoder circuit validates the key by determining whether or not the detected key is associated with the storage device.

15. The system of claim 14, wherein the receiver/decoder circuit enables the storage device if the detected key is validated and disables the storage device if the detected key is not validated in order to provide device level protection.

16. The system of claim 15, wherein digital content stored on the computer is not encrypted with the key.

17. The system of claim 14, wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the storage device using the key associated with the storage device in order to provide sector-level protection.

18. The system of claim 14, wherein the key associated with the storage device is initially delivered with the storage device.

19. The system of claim 11, wherein the storage device is selected from a group consisting of PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, DVR players, memory sticks, and memory cards.

20. The system of claim 14, wherein the key associated with the storage device is assigned thereto by a user.

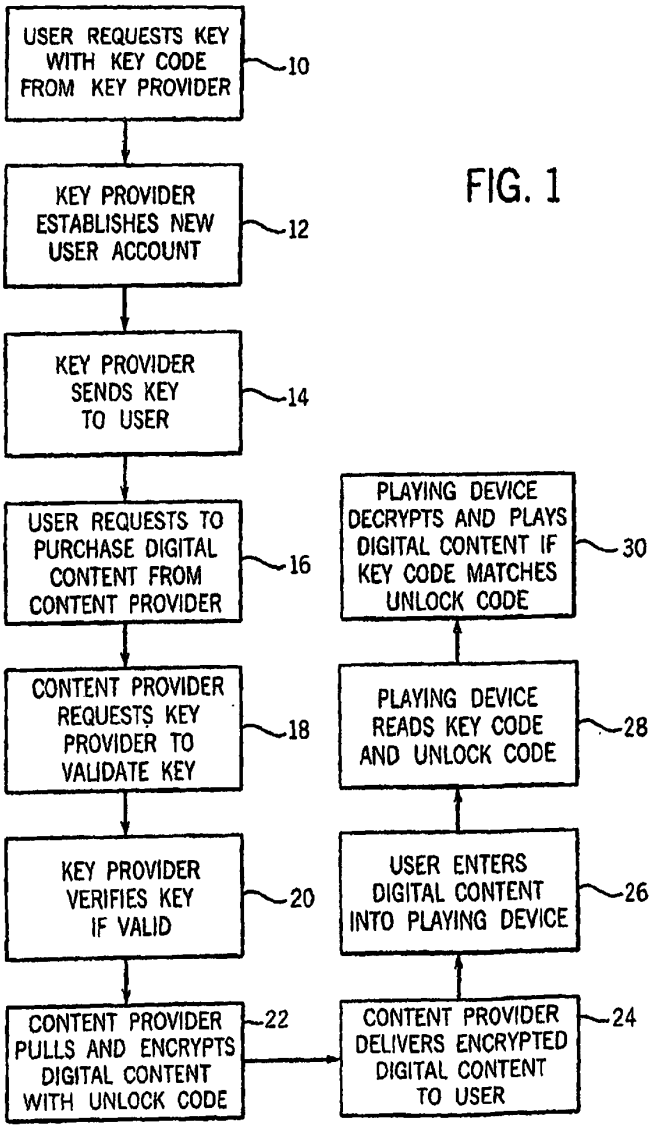

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT PROVIDER PULLS AND ENCRYPTS DIGITAL CONTENT WITH UNLOCK CODE
22
CONTENT PROVIDER DELIVERS ENCRYPTED DIGITAL CONTENT TO USER
24
USER ENTERS DIGITAL CONTENT INTO PLAYING DEVICE
26
PLAYING DEVICE READS KEY CODE AND UNLOCK CODE
28
PLAYING DEVICE DECRYPTS AND PLAYS DIGITAL CONTENT IF KEY CODE MATCHES UNLOCK CODE
30

FIG. 1

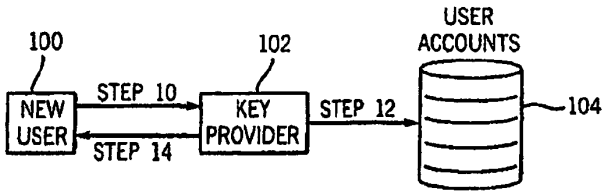


FIG. 2

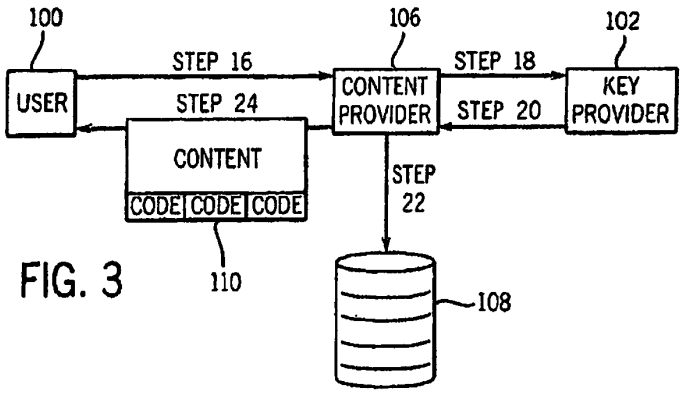


FIG. 3

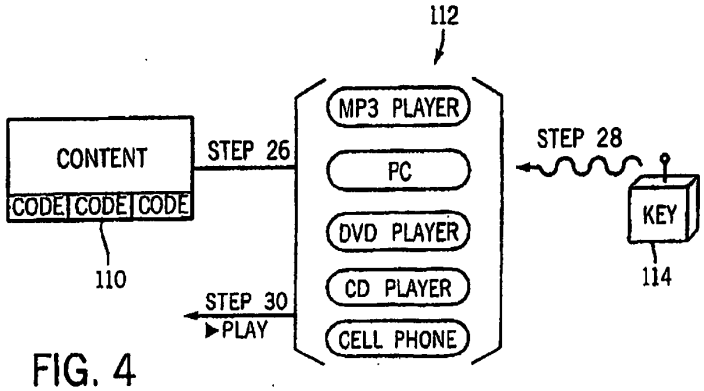


FIG. 4

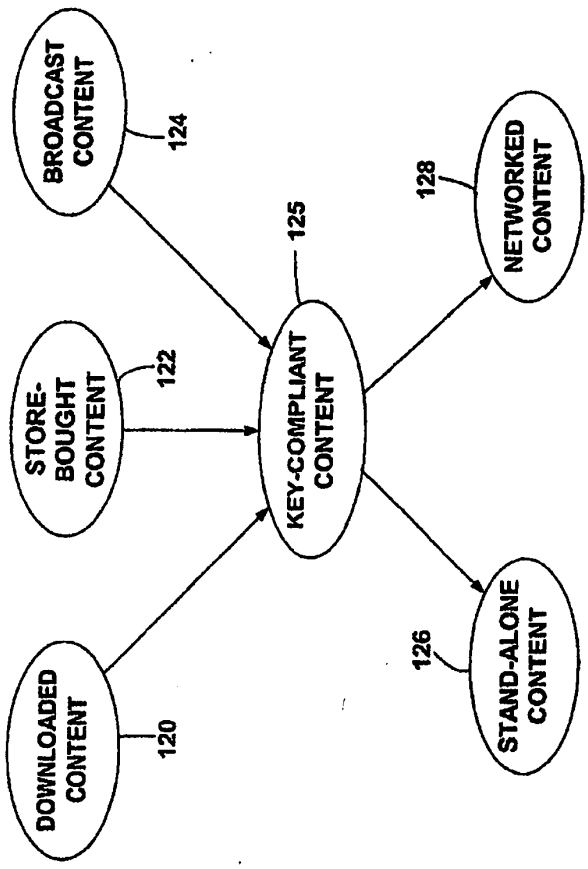

BROADCAST CONTENT
124
STORE-BOUGHT CONTENT
122
DOWNLOADED CONTENT
120
KEY-COMPLIANT CONTENT
125
NETWORKED CONTENT
128
STAND-ALONE CONTENT
126

FIG. 5

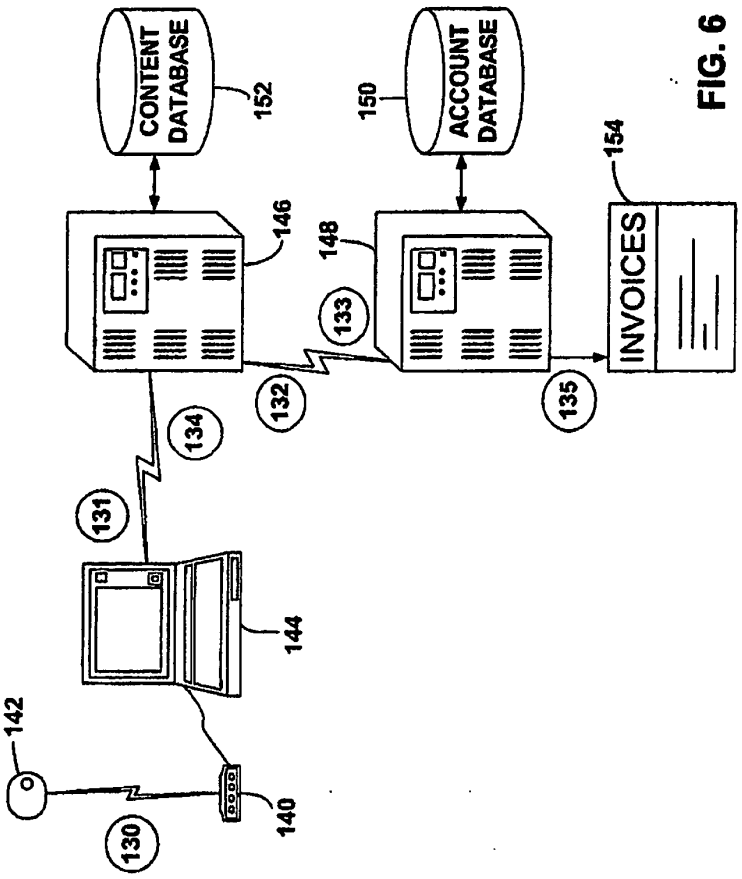

CONTENT DATABASE
152
ACCOUNT DATABASE
150
154
INVOICES
146
148
133
132
134
135
131
144
142
140
130

FIG. 6

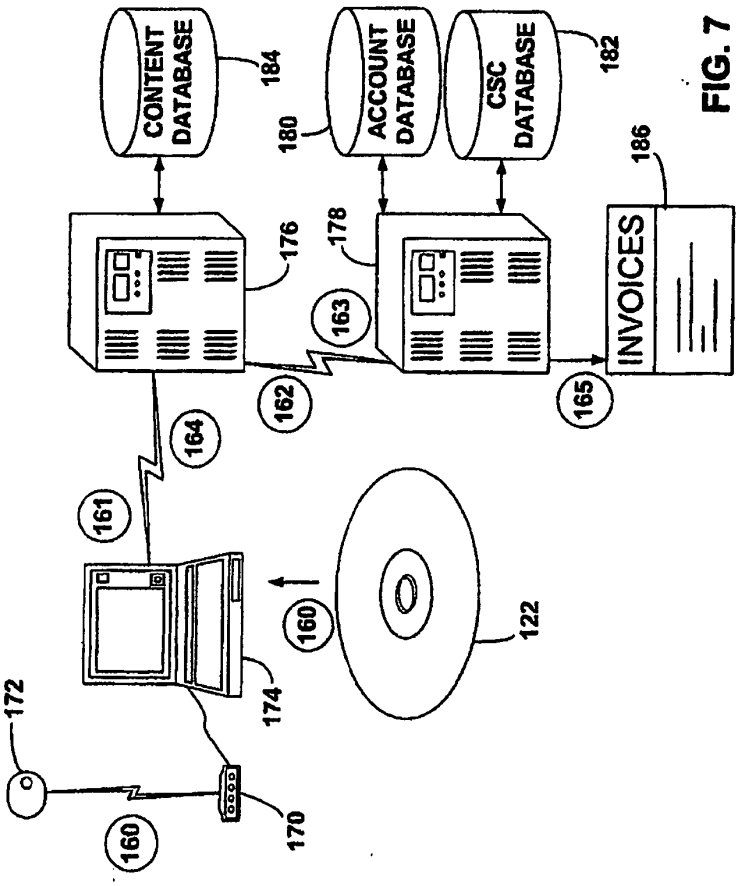

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
186
INVOICES
176
178
163
162
164
165
161
160
122
174
172
170
160

FIG. 7

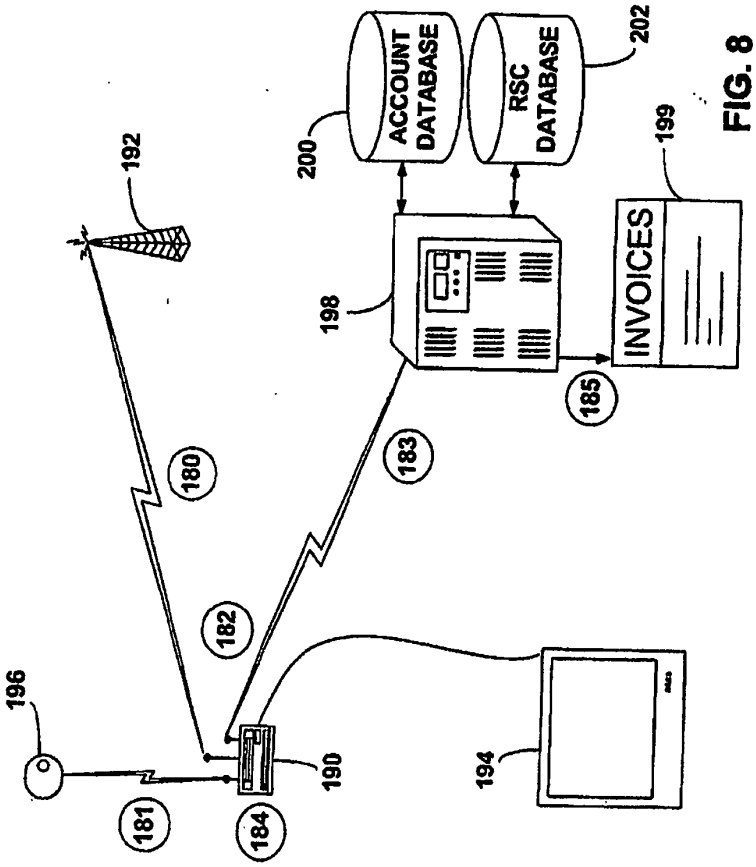

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
192
198
185
180
183
182
196
190
194
181
184

FIG. 8

FIG. 9a

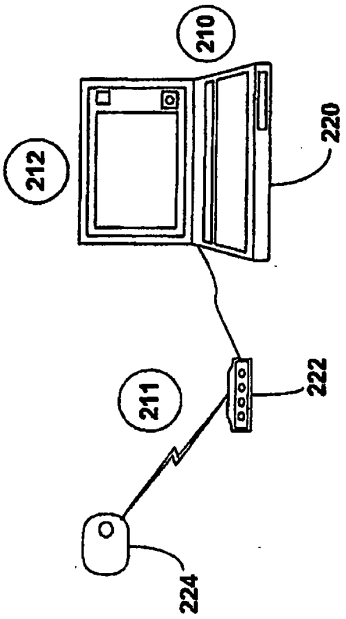
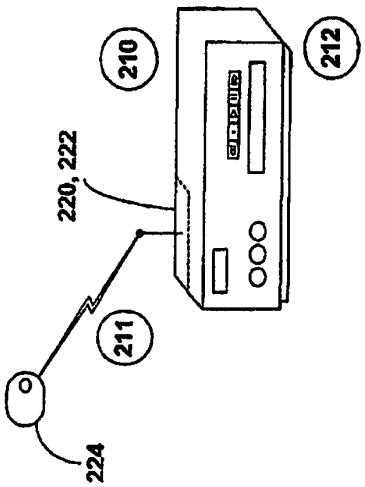


FIG. 9b



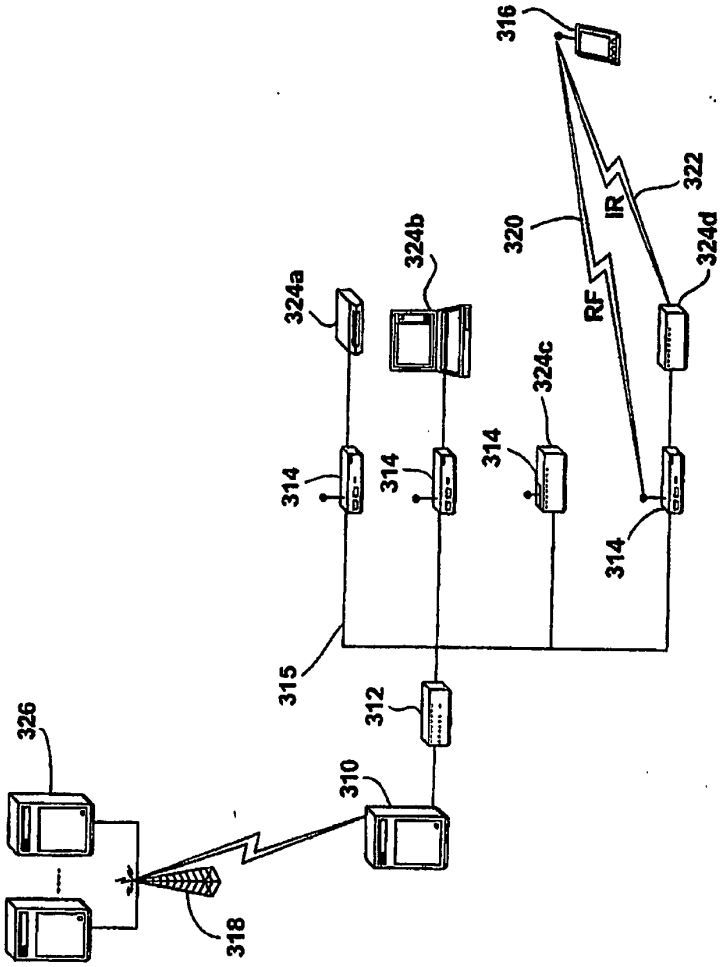

316
322
IR
320
RF
324d
324b
324a
324c
314
314
314
314
315
312
310
326
318

FIG. 10

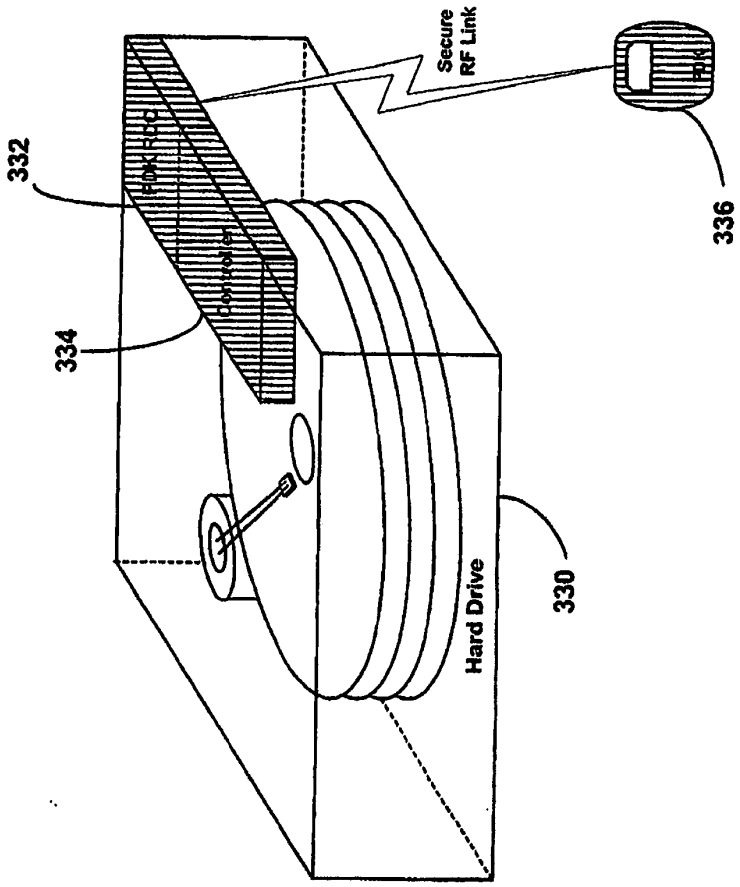


FIG. 11

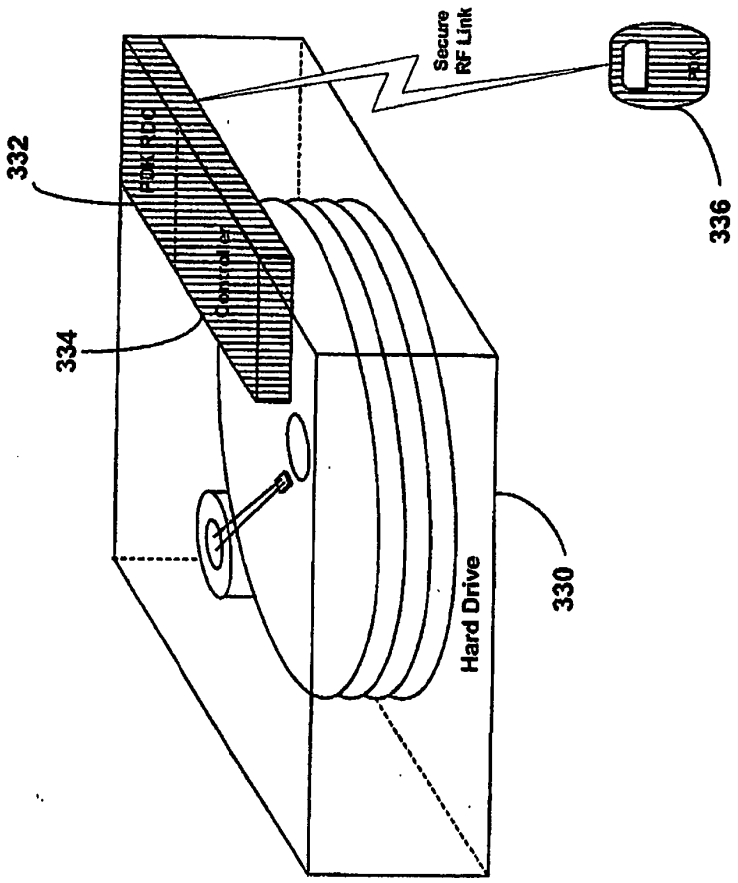


FIG. 12

11/13

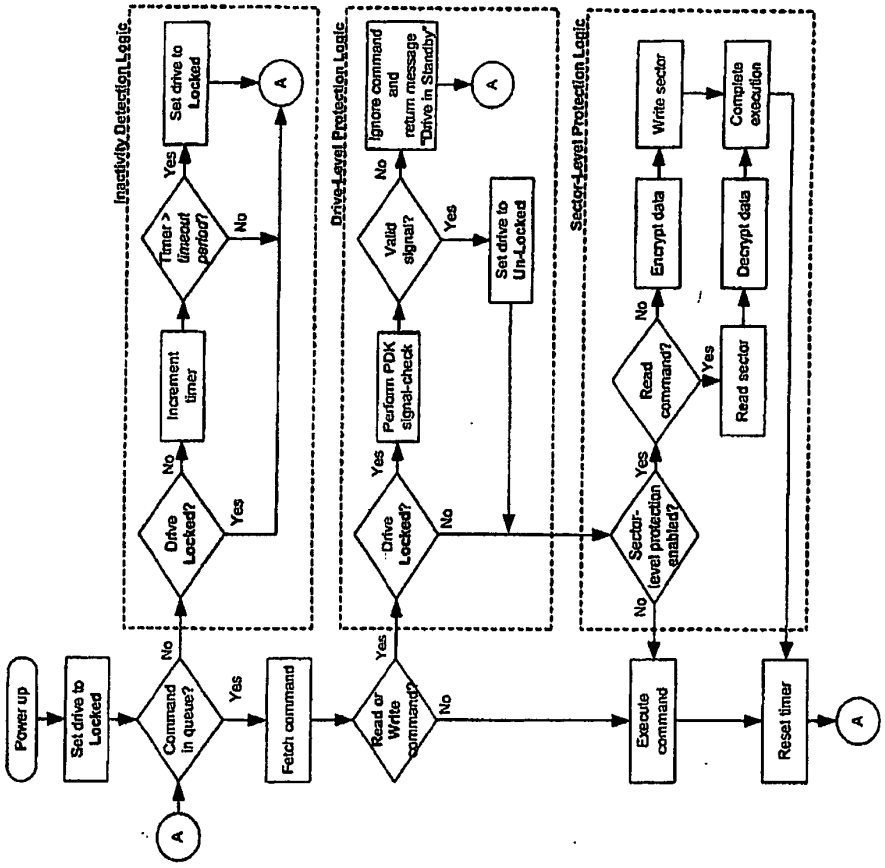

Power up
Set drive to Locked
Command in queue?
No
Yes
A
Fetch command
Read or Write command?
Yes
No
Inactivity Detection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
A
Drive-Level Protection Logic
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
A
Set drive to Un-Locked
Sector-Level Protection Logic
Sector-level protection enabled?
Yes
No
Read command?
No
Yes
Encrypt data
Write sector
Read sector
Decrypt data
Complete execution
Execute command
Reset timer
A

FIG. 13

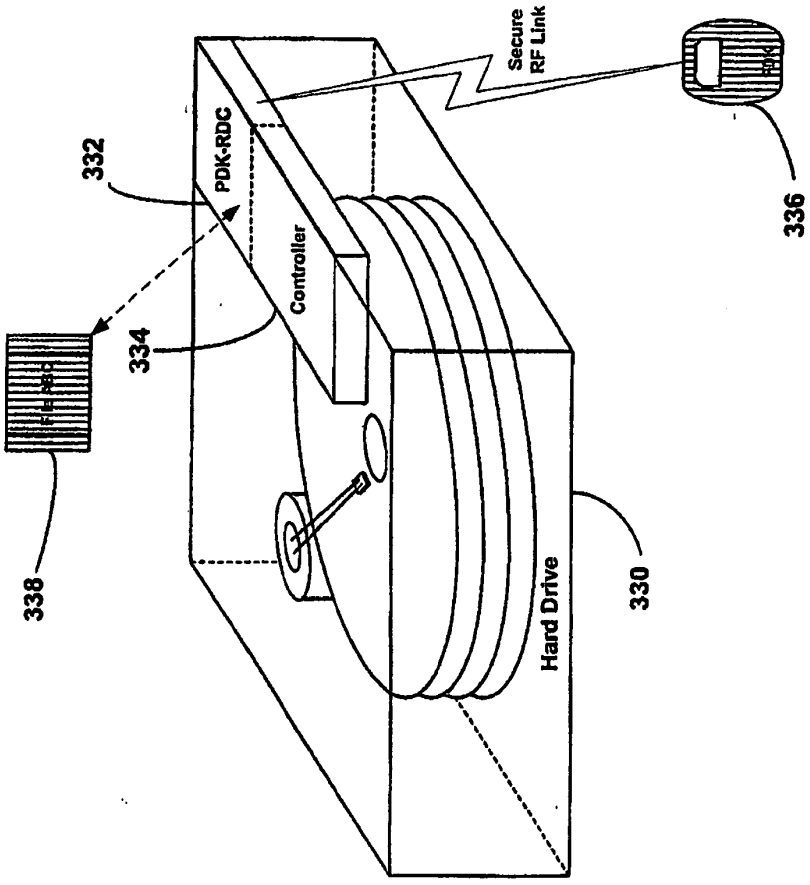

Secure
RF Link
PDK
336
332
PDK-RDC
Controller
334
338
Hard Drive
330

FIG. 14

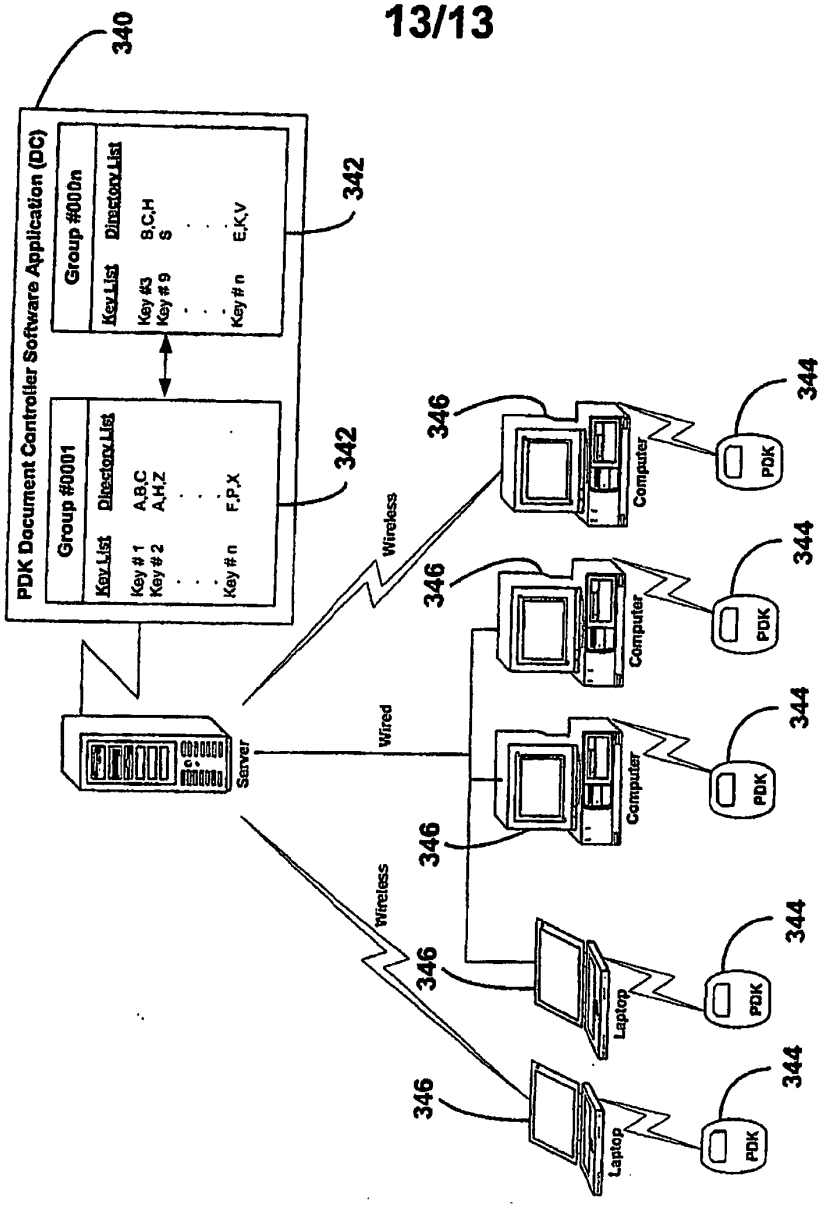

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key # 1
Key # 2
Key # n
A,B,C
A,H,Z
F,P,X
342
Group #000n
Key List
Directory List
Key #3
Key # 9
Key # n
B,C,H
S
E,K,V
342
Server
Wired
Wireless
Wireless
346
Computer
344
PDK
346
Computer
344
PDK
346
Computer
344
PDK
346
Laptop
344
PDK
346
Laptop
344
PDK

FIG. 15

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086802 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/007535

(22) International Filing Date: 8 March 2005 (08.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/551,320 8 March 2004 (08.03.2004) US

(71) Applicant *(for all designated States except US)*: **MARGENT DEVELOPMENT, LLC** [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; P.O. Box 2938, Minneapolis, MN 55402 (US).

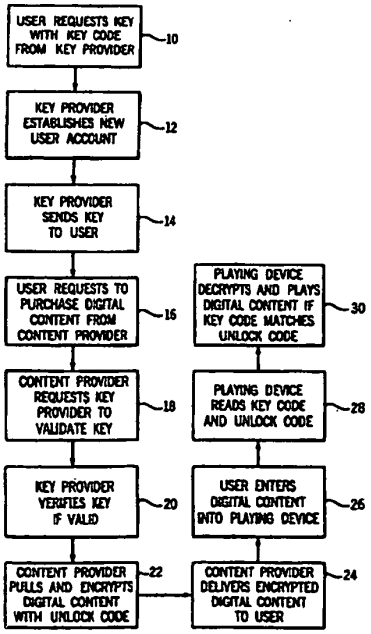
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)

(57) Abstract: One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.



WO 2005/086802 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)

FIELD OF THE INVENTION

The present invention relates generally to embodiments of a linked account system using personal digital key (PDK-LAS).

BACKGROUND OF THE INVENTION

The market for downloading digital content online is rapidly climbing because distribution of such content is inexpensive, fast, and easy and the quality of the content itself is acceptable. The market, however, remains disorganized due to competing standards, competing companies, discontented artists and producers, and outright theft of digital content.

Digital rights management (DRM) companies seek to solve the foregoing problems by delivering the digital content from the real producers to the right customers and ensuring that everyone who should be paid in fact is paid. DRM seeks to get everyone paid by managing the multiple steps for distributing digital content (music, video, software) online: watermarking, encryption, transaction management, and rights management. Some DRM companies perform all these steps, while other DRM companies specialize in one or two steps of the process.

First, watermarking stamps each piece of digital content with a digital mark so it can be tracked wherever it goes. Digital watermarks are just like paper watermarks, except they cannot be seen or heard. Special software is required to read a digital watermark.

Second, encryption scrambles watermarked digital content and stores it inside a digital safe for shipment around the Internet. The safe protects the content during shipping by allowing only those with the right software key to the safe to decrypt and use the content.

Third, transaction management handles actual payments for the digital content using credit card techniques found elsewhere in e-commerce. An order

is placed, a credit card number is taken, account status is checked, and the exchange is authorized.

Finally, rights management manages the information about the digital content itself: what it is, who gets it, how it is delivered, how many times it may be used, how long the rights last, who gets paid, how much they get paid, and how. This information travels with the digital content in something called a digital permit. The permits rests on top of the digital content as it travels the Internet and allows legal users to enjoy the digital content for as long as the rights last.

The primary objective of DRM companies is to deploy technologies that protect digital content as it is distributed online. Some of these proposed technologies and DRM in general are discussed in the article "Digital Rights Management May Solve the Napster 'Problem'," *Technology Investor*, October 2000, pp. 24-27. Although such technologies should reduce the amount of digital theft, they generally favor the content provider at the expense of the consumer or favor the consumer at the expense of the content provider. That is, the rights of either the content provider or the consumer are compromised. For example, some technologies severely limit the consumer's ability to make extra copies of digital content even when the digital content is solely for personal use. Other technologies facilitate the making of copies of digital content which can be used by different consumers without the content provider being compensated by each consumer. The present inventor has discovered an improved DRM system and method that effectively balances and protects the rights of both the consumer and the content provider. In addition, the present inventor has discovered an associated digital content security system for protecting computers and other storage devices from unauthorized use and protecting the digital content stored on computers and other storage devices from being wrongfully accessed, copied, and/or distributed.

With the advent of the Internet, and online shopping, banking and so forth, the Internet has enabled the incidence of credit card, bank account

information, and similar data being stolen has risen dramatically. The cost to providers of transactions performed with these stolen items is enormous and results in higher transaction fees and product pricing to consumers, as it is the providers who are typically responsible for charges applied to stolen account information.

Additionally, the inconvenience and tangential problems that victims, consumers, suffer as a result of such crimes are often traumatic, but are minimally troublemsome. The insufficient technologies and procedures currently utilized to secure account-based transaction processing do little to prevent these crimes. The problem is most notable in the case of the largest growing segment for such transactions, the on-line environment.

SUMMARY OF THE INVENTION

One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a flow chart of a method of managing digital rights in accordance with the present invention;

FIGS. 2, 3, and 4 are block diagrams of portions of a DRM system for implementing the method in FIG. 1;

FIG. 5 is a conceptual model of core options for acquiring digital content that can be encoded to produce key-secured content and core options for playing back the key-secured content;

FIG. 6 is a block diagram for implementing a core acquisition option of downloaded content;

FIG. 7 is a block diagram for implementing a core acquisition option of store-bought content;

FIG. 8 is a block diagram for implementing a core acquisition option of broadcast content;

FIGS. 9a and 9b are block diagrams for implementing a core playback option of stand-alone devices;

FIG. 10 is a block diagram for implementing a core playback option of networked devices;

FIG. 11 is a block diagram of a standard computer hard drive incorporating an integrated PDK-RDC (receiver/decoder circuit) for the purpose of enabling multiple methods of securing digital content;

FIG. 12 is a block diagram for implementing Drive-Level protection and Sector-Level protection in connection with the computer hard drive;

FIG. 13 is a flow chart of the logic executed by the PDK-RDC for implementing Drive-Level protection and Sector-Level protection;

FIG. 14 is a block diagram for implementing File-Level protection in connection with the computer hard drive; and

FIG. 15 is a block diagram for implementing Network-Level protection by expanding File-Level protection to a network environment.

FIG. 16 is a schematic view of a PDK key system embodiment of the invention.

FIG. 17 is a schematic view of a PDK key system embodiment of the invention.

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

DESCRIPTION OF SPECIFIC EMBODIMENTS

Definitions

As used herein, "PDK Key or Key" refers to a PDK-compliant wireless key providing access to PDK-protected objects. The acronym "PDK" refers to "personal digital key."

A "PDK-hard drive" refers to a physical or "electronic" hard drive containing an integrated RDC.

A "PDK-protected product/object" refers to a hard drive or accounts or content protected via PDK technology .

An "assigned key" is a PDK key assigned to one or more protected objects.

An "RDC" refers to a Reader/Decoder circuit installed in a user's computer, or built into computer hard drive, or point-of-sale (POS) credit card swipe unit which communicates with PDK keys and decodes PDK data.

A "POS RCD" refers to a reader/decoder circuit integrated in a standard point-of-sale (POS) credit-card swipe unit.

A "manufacturer" as used herein refers to a manufacturer of PDK-keys.

A "provider" as used herein refers to an entity issuing a PDK-linked account, PDK hard drives and so forth.

A "customer" or "user" refers to an individual possessing or utilizing a PDK key.

A "master" or "master key" refers to a PDK key initially assigned to a PDK protected object, and which is required to be present for configuration transactions.

Description

One system embodiment of the invention, illustrated at 1000 in FIG. 16 includes a personal digital key, PDK, 1010, a point-of-sale reader decoder circuit, POS RDC, 1012, a PDK reader decoder circuit, 1014 that is connected to a provider 1016 having a database 1018. For some

embodiments, the PDK reader decoder circuit and POS RDC 1014 are in a single unit 1020, which for some embodiments, is a standard credit card swipe unit integrated with RDC. For some embodiments, a standard credit card 1022 is readable in the reader 1020. The provider 1016 may be a credit card processor, bank or other similar entity. The account database 1018 maintains the account number, PDK key number and other identifiers of the user.

In another embodiment, illustrated at 2000 in FIG. 17, the PDK 1010 interfaces with a computer 2002 through a secure RF link 2004. The computer 2002 is a standard personal computer, with integrated RDC, PDK-hard drive or RDC adaptor card. The computer 2002 communicates with the provider 1016 through a standard Internet connection 2006. The provider 1016 communicates with the database 1018 in a manner as described in the embodiment described above.

Once in possession of a PDK key, a user optionally registers the key with the key manufacturer or a central key database. No usage data, credit or bank account numbers, hard drive IDs, etc. is maintained in the manufacturer's database, only user verification information. This information includes a customer account number, indicating for some embodiments, a customer's record within the manufacturer's database, customer name, address and phone, key number, and status of key, in-use, stolen, lost and so forth. This information is used primarily for verification purposes during lost key replacement procedures.

The data fields stored in PDK keys include a user label which includes user text label in an unprotected field. The data fields also include an account number, which is a user's manufacturer account number, which is in a protected field. The data fields also include a key number which is a unique key identification and is a protected field.

The PDK key communicates with one of three basic implementations of a PDK-RDC which include POS RDC, a standard credit card swipe type device with an integrated RDC. A second implementation is an RDC

adaptor, which is an add-on PC board RDC, interfacing via USB, firewall, PC card, expansion slot and so forth. A third implementation is a PDK hard drive which is a standard hard drive with an integrated RDC.

POS RDC devices are used in stores at checkout lanes, purchase counters, hand-held swipes, and so forth. RDC adaptors or PDK hard drives are intended for PC based use.

Physical cards such as credit/debit card accounts, bank accounts, membership accounts, or similar types of accounts, intended for use with the PDK LAS technology are conventional cards. No changes are required to such cards in order to ready them for use with the PDK LAS technology. From a consumer standpoint, this feature, along with an ability for a PDK-key to be purchased and assigned to an object at any point, enables easy acceptance of the technology.

Additionally, the PDK-LAS technology offers great flexibility in how PDK-keys are distributed, assigned, and used. For example, providers may optionally allow dynamic key assignment, assigning keys at a later date, assigning multiple keys to the same account and so forth, and users may elect to use one PDK key for all their PDK based security needs, i.e. one PDK key can be assigned to multiple accounts, PDK hard drives, and other PDK based products.

Specific examples illustrating uses of the PDK linked account embodiments are described as follows. These examples are presented to show particular applications of the PDK linked accounts and are not intended to limit embodiments of the invention.

In a first example, a user wishes to assign a key to a new PDK linked account. The user logs onto a provider's site over the Internet via the user's personal computer, in one embodiment. The user inputs whatever validation the provider typically requires. Sufficient data is requested by the provider during this transaction to authenticate the user. An RDC reads the user's PDK key data and transmits the data to the provider. The provider confirms the user's request to link the PDK key to the account. Once confirmed, the

PDK key data is permanently stored in the provider's database as a master PDK key and can only be changed by directly contacting the provider.

In one other embodiment, users phone providers directly and verbally relay all required information, including master PDK key data, printed on a card included with the PDK key at purchase. For users with Internet access but no RDC, this information is hand entered on the provider's website.

In a second example, a user wishes to assign additional keys to a PDK linked account. The user logs onto a provider site and inputs whatever validation the provider typically requires. The user ensures that the assigned master PDK key is within the vicinity of RDC. The RDC reads the master and additional PDK key data and transmits the data to the provider. The provider confirms a user's request to link additional PDK keys to the account number, or change PDK keys or remove PDK keys. Once confirmed, the updated PDK key data is stored in the provider's database along with master PDK key data.

In an alternate embodiment, to facilitate users without an RCD equipped personal computer and Internet access, users may phone providers directly and verbally relay all required information, including both master and additional PDK key data, printed on cards (or similar) included with PDK keys at purchase. For users with Internet access but no RDC, this information may be hand entered on the provider's website.

In a third example, the user wishes to utilize a PDK linked account to purchase a product at a store. The user ensures that an assigned PDK key is within the vicinity of POS RDC at a checkout counter. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using currently accepted procedures, to the provider for verification. If more than one PDK key is read at the counter, either data from all of the PDK keys may be transmitted to the provider or User Labels may be displayed on POS RDC to enable the user or clerk to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to

information stored in the record. If a match is confirmed, the sales transaction is completed normally. If not confirmed, the transaction cannot be completed.

A fourth example is one where a user desires to utilize a PDK linked account to purchase a product on –line or the user wishes to access account information on line. The user must ensure that an assigned PDK key is within the vicinity of RDC. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using conventional techniques, to the provider for verification. If more than one PDK key is read at RDC, either data from all PDK keys is transmitted to the provider or User Labels are displayed on a computer screen to enable the user to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to information stored in the record. If a match is confirmed, the transaction/session is completed normally. If not confirmed, the transaction/session cannot be completed.

A fifth example is one where the user loses a PDK key. After an initial master PDK key setup, users are encouraged to immediately assign an additional PDK key, which serves as a day-to-day key, and store the master PDK key in a safe location. If the day-to-day key is lost, the master is usable to assign the new day-to-day key. As a last resort, for users losing all PDK keys, the key manufacturer may be contacted and, after authentication is performed, instructed to ship a replacement PDK key.

Turning now to the drawings and referring initially to FIG. 1, there is depicted a method of managing digital rights in accordance with the present invention. First, a new user requests a physical electronic key or data unit from a key provider (step 10). The key provider may offer a web site on the Internet, a toll free telephone number, and/or retail outlet where the key may be acquired. In addition, the key provider may allow a key to be requested in writing, preferably using a form designed by the key provider. In one model the user may acquire

as many keys as desired, while in another model each user is only entitled to a single key.

Second, in response to the user's request for a physical key, the key provider establishes a new secure account for that new user in a secure user account database (step 12). The new account may include the following data fields: account number, password, software encryption key, user label, number of users (linked to account), address, telephone number, e-mail address, and custom fields. The custom fields may, for example, include demographic information such as the user's age, gender, marital status, income level, interests, hobbies, etc. The physical key may include the following data fields: user label, account number, software decryption key, and a custom storage area. The user label and the account number serve as a first activation code (or key code) for the acquired physical key. All data fields on the physical key, except for the user label, are preferably encrypted. To allow the user to view his or her account in the future, the user is preferably assigned a login name and the above-noted password.

Third, the key provider ships the physical electronic key to the new user via a package courier such as the U.S. Postal Service, United Parcel Service, or Federal Express (step 14). In one pricing model the physical key is sent to the user at no charge, while in another pricing model the physical key must be purchased by the

user. If the physical key must be purchased by the user, either the user must provide credit/debit card information to the key provider in step 10 to pay with a credit/debit card, or the key provider includes an invoice with the shipped key in step 14.

FIG. 2 is a block diagram of a system for implementing steps 10, 12, and 14 of the method of managing digital rights. The system includes the new user 100, the key provider's web site 102, and the user account database 104.

Referring back to FIG. 1, fourth, the user transmits his or her activation code in the physical key to a digital content provider, who may have a cooperative relationship with the key provider, and requests to purchase digital

content (music, video, or software) from that content provider (step 16). The content provider may offer a web site on the Internet containing a listing of digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.

Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.

Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second

activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital content either by providing credit/debit card information to the content provider in step 16 or by paying off of an invoice included with delivered digital content. If the digital content is delivered online, the user is preferably required to provide the credit/debit card information and have such information approved as a prerequisite to delivery of the digital content. If the user possesses more than one physical electronic key and would like the acquired digital content to function with each of the user's keys, all of the activation codes are applied to the digital content. The content provider charges the user based on the number of keys with which the user would like the digital content to function. For example, the user may be charged the same amount for each activation code, or may be charged a larger amount for one activation code and lesser amounts (e.g., surcharges) for additional activation codes.

FIG. 3 is a block diagram of a system for implementing steps 16, 18, 20, 22, and 24 of the method of managing digital rights. The system includes the new user 100, the content provider 106, the key provider's web site 102, the digital content database 108, and the acquired digital content 110.

Returning to FIG. 1, ninth, the user enters the encrypted digital content into a playing device of a type suitable for playing the digital content (step 26). The device may, for example, be an MP3 player, a personal computer, a DVD player, a CD player, a cellular phone, or other portable device. In one embodiment, the device contains a wireless transceiver adapted to receive a radio frequency signal transmitted by a corresponding wireless transceiver in the user's physical electronic key. The wireless transceiver in the device is optionally tracked and "secured" for audit purposes by permanently including a unique identifier assigned by the device manufacturer in the transceiver.

Tenth, with the user's physical electronic key within a short range (e.g., few meters) of the playing device, the playing device reads (1) the first activation code carried in a secure radio frequency signal transmitted by the transceiver in the physical key to the transceiver in the device and (2) the second activation code marked on the encrypted digital content (step 28). The device contains decryption software or hardware for decrypting the encrypted digital content to the extent necessary to read any encrypted portion of the second activation code.

Eleventh, the playing device compares the first activation code and the second activation code and determines whether the first activation code is associated with the second activation code (step 30). Steps 29 and 30 may be performed, for example, when the user presses a "play" button on the playing device or when the user first enters the encrypted digital content into the playing device. If the first activation code is associated with the second activation code, the device decrypts and plays the digital content. If the first activation code is not associated with the second activation code, the device does not play the digital content. If the second activation code is simply the same as the first activation code, then the foregoing comparison determines whether there is a match between the first activation code and the second activation code. In a preferred embodiment, the device continues to play the digital content only while the physical key is sufficiently close to the device to communicate the first activation code to the device and allow the device to compare the first activation

code to the second activation code at least partially encrypted with the digital content even while the digital content is being played. If the physical key is moved out of range, the device is no longer enabled to decrypt and play the digital content. In an alternative embodiment, once the device is initially enabled to decrypt and play the digital content, the device remains enabled until either the "play" function is stopped, a play track/song ends, or the digital content is removed from the device, even if the physical key is moved out of range such that the key can no longer communicate the first activation code to the device.

FIG. 4 is a block diagram of a system for implementing steps 26, 28, and 30 of the method of managing digital rights. The system includes the encrypted digital content 110, the key-enabled playing devices 112, and the user's physical electronic key 114.

As stated above, the user's physical electronic key and the key-enabled playing device contain respective wireless transceivers to communicate the activation code in the key to the device. In a preferred embodiment, the transceivers are small, inexpensive *Bluetooth* radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are plugged into electronic devices, which can then communicate over short distances and through obstacles by means of radio waves. *Bluetooth* is a term used to describe the protocol of a short range (e.g., about 10 meters) frequency-hopping radio link between devices containing the radio chips. These devices are then termed "*Bluetooth*-enabled." The secure radio link replaces a cable that would otherwise be used to connect the devices. Further details concerning *Bluetooth* wireless technology may be obtained from www.bluetooth.com.

Wireless technologies other than *Bluetooth* may be used to communicate the activation code from the user's physical electronic key to the playing device. One example of an alternative wireless technology is known by a trade term "Wi-Fi," which is short for wireless fidelity and is another name for IEEE 802.11

b. Products certified as Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA) are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

In other alternative embodiments, the communication between the user's physical electronic key and the playing device is not wireless. Rather, in one alternative embodiment, the user's physical electronic key communicates the activation code to the playing device via a transmission line such as a serial cable that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

The above-described DRM method and system for implementing the method are advantageous in that they afford the key holder with tremendous versatility in copying and using encrypted digital content for personal use. At the same time, the rights of the content provider are protected because only the key holder with a key-enabled device can use the encrypted digital content. The key holder can copy the encrypted digital content as many times as desired, but can only play the encrypted digital content on a key-enabled device that is enabled with the physical electronic key coded to decrypt the encrypted digital content. Thus, the digital content, even when copied, remains personal to the key holder. Individuals other than the key holder cannot use the encrypted digital content, even if they copy it, because both the original and copies of the encrypted digital content are still encrypted and the individuals do not hold the physical electronic key coded to decrypt the digital content.

A core element of the present invention is the concept of a portable, physical electronic key that is personal to a particular user. The physical key represents a DRM solution that fully addresses the needs of both consumers and publishers of digital content. The physical key is permanently associated with a user's digital content library. At the time of content acquisition, the physical key becomes permanently associated with the newly acquired content. The user is

now "linked" to that acquired content. A user (e.g., individual or family) may own as many physical keys as desired, but every piece of encrypted digital content purchased is tied to one specific key. The user may duplicate or transfer the acquired content to any media or device for playback as many times as desired, as long as the associated physical key is present. Thus, the present invention guarantees that the acquired content is played only by the user who has legitimately paid for it. The present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to FIG. 5, the present invention fully supports the use of "key-secured" digital content 125 with all core content acquisition options and all core playback options. The key-secured digital content 125 is encoded with a second activation code associated with a first activation code stored on the user's physical electronic key. The core acquisition options include downloaded content 120, store-bought content 122, and broadcast content 124. The core playback options include stand-alone devices 126 and networked devices 128. Each of these options are described in further detail below.

Referring to FIG. 6 generally, as already noted in FIGS. 1 through 4, a primary application of the present invention is its use in the downloading of digital content from the Internet. A consumer shops a content distributor's website and selects a piece of content they wish to purchase (music, movies, software, E-books, etc.). The consumer then provides the web site with standard on-line purchase information including the selection's title and method of payment, as well as their physical electronic key information. Transparent to the consumer, the distributor's web site links to the key provider's web site and transmits the physical key information for validation. The key provider's web site then provides the distributor's web site with the information required to prepare the acquired content for secure shipment to the consumer (or notification that the physical key was invalid). The key provider's web site records the transaction for later billing. Finally, the distributor's web site retrieves a copy of the digital content from its library, permanently links it to the consumer's

physical key (by using the key's information to encrypt it), and transmits the secured content to the consumer. The consumer is now free to duplicate the content as often as desired, and to play the content on any key-enabled playback device.

Referring to the specifics of FIG. 6, the process of implementing the core acquisition option of downloaded digital content 120 (see FIG. 5) proceeds as follows. At step 130, a receiver/decoder circuit 140 retrieves an account number from a consumer's physical key (transponder) 142 over a secure RF link. At step 131, the consumer enters such data as a password, purchase selection, and method of payment via the consumer's personal computer 144. The data is transmitted to a content distributor's web site 146 from the consumer's personal computer 144. At step 132, the content distributor's web site 146 transmits the account number and password to a key provider's web site 148. At step 133, the key provider's web site 148 authenticates all data against its database 150 and, if authentic, returns such information as the account number, user label, number of users, and software encryption key to the distributor's web site 146. If the data is not valid, the key provider's web site 148 sends a message to the distributor's web site 146 indicating the same. A counter, used for the key provider's billing purposes, is incremented. At step 134, the distributor's web site 146 pulls the purchased content file from its database 152, encrypts it with the software encryption key it received in step 133, and builds a final key-secured content file that is then transmitted to the consumer's personal computer 144. Charges are assessed based on the number of users, etc. and billed to the consumer according to the method of payment. At step 135, invoices 154 are generated and sent to content distributors by the key provider's web site 148 on a regular cycle.

Optionally, to enable content providers to offer sample content (e.g., limiting playback to the device on which the content was originally downloaded, for a specified period of time) a special "enhanced" version of a receiver/decoder circuit 140 can be produced. These enhanced receiver/decoder circuits (primarily for PC's) would each include a unique identification number and additional functionality enabling them to "talk" to a key provider's web site 148

to acquire secured timing information. Sample content files may include the following information (in their encrypted header section):

- identification number of enhanced receiver/decoder circuit used for downloading and transmitted by the receiver/decoder circuit to the key provider's web site at the time of content purchase;
- hour stamp (i.e., the hour in which the content was downloaded; and
- life hours (i.e., number of hours content remains valid, such as perpetual, one hour, 24 hours, 48 hours, etc.).

The above information is used by an "enhanced" receiver/decoder circuit during playback to determine whether a content file has "expired" or is attempting to play on an unauthorized device (i.e., any device except the device on which the content
was originally downloaded). This capability allows content distributor web sites to distribute limited-use samples with associated tiered-pricing models.

Referring to FIG. 7 generally, the present invention can be extended to store-bought content. To fully integrate store-bought content into the present invention, traditional store-bought content is modified in two ways. First, the content is distributed in a copy protected format (e.g., using any valid copy protection technology). Second, the content contains a unique content serial code. The content serial code may be contained either directly in the digital content or as a physical label. Each content serial code is designated by a content distributor during manufacturing and stored in the key provider's database. This database is later used to validate that each content serial code is unique and used only a prescribed number of times. To a consumer, a content serial code on their newly purchased store-bought content represents a download of a key-secured version of that content for free or a prescribed price. This key-secured copy provides the consumer with exactly the same advantages and freedoms as any other key-secured content. From the consumer's standpoint, the download process occurs exactly as any other standard key-secured content download with the exception of how the payment is handled. The "payment" is the content serial code. By providing all of the advantages of the present

invention to consumers of legacy-capable store-bought content (by way of "content serial code downloads"), the scheme provides the industry with the first complete DRM solution.

Referring to the specifics of FIG. 7, the process of implementing the core acquisition option of store-bought digital content 122 (see FIG. 5) proceeds as follows. At step 160, a receiver/decoder circuit 170 retrieves an account number from a consumer's physical key (transponder) 172 over a secure RF link, and the consumer's personal computer 174 reads a content serial code from the store-bought content 122. The store-bought content 122 contains the content serial code that uniquely identifies the content. The format of the content serial code may, for example, be PPPP.FFF.0123456789 where PPPP is a provider identification, FFF is a facility identification, and the numbers represent a sequence number. The store-bought content 122 incorporates a copy protection scheme such as Macrovision™, key2audio™, or SafeAudio™. Disc "copy flags" (specified in SDMI standards) may also be set to further inhibit duplication efforts.

At step 161, the consumer enters such data as a password and purchase selection via the consumer's personal computer 174. The previously-read content serial code specifies that the method of payment is to a "content serial code-credit" (i.e., there is typically no charge for this download because the content serial code confirms that the download in process is of content that the consumer has already legitimately purchased). The data is transmitted to a content distributor's web site 176 from the consumer's personal computer 174. At step 162, the distributor's web site 176 transmits the content serial code, account number, and password to a key provider's web site 178. At step 163, the key provider's web site 178 authenticates all data against its databases 180 and 182 and, if authentic, returns such information as the account number, user label, number of users, software encryption key, and paid-flag (indicating the content serial code has been validated) to the distributor's web site 176. The key provider's web site 178 now sets the paid-flag to disable any further downloads and records the account number field in the content serial code database 182 for

auditing purposes. If the data is not valid, the key provider's web site 178 sends a message to the distributor's web site 176 indicating the same. A counter, used for the key provider's billing purposes, is incremented. Each entry in the content serial code database 182 may include the following data fields: CDC #, paid-flag, and account number. At step 164, the distributor's web site 176 pulls the content file from its database 184, encrypts it with the software encryption key it received in step 163, and builds a final key-secured file that is then transmitted to the consumer's personal computer 174. No charge is typically assessed because a valid content serial code serves as "payment" for the download. At step 165, invoices 186 are generated and sent to content distributors by the key provider's web site 178 on a regular cycle.

Referring to FIG. 8 generally, the present invention can be extended to broadcast content. To fully integrate broadcast content into the present invention, traditional broadcast content is only minimally modified. The modification is that the broadcast content is transmitted in a copy protected format (such as the DVD standard known as Content Scramble System (CSS)). The remainder of the process is described below. A key-enabled recording device, incorporating a unique identifier, receives copy-protected broadcast content. If only playback of the broadcast content is desired, basic decoding (e.g., CSS) is performed and the broadcast content is sent on for playback. If the consumer wishes to record the broadcast content, however, the recording device performs additional steps prior to sending the broadcast content on for playback. The recording device connects to the key provider's web site to validate the recording device's internal identifier and the consumer's physical key. If both are valid, the recording device translates the broadcast content into a key-secured format by encoding it with the consumer's activation code, and then stores the key-secured content file, with its identifier permanently embedded within, for later use. The end result is key-secured broadcast content that provides the owner of the associated physical key all the freedoms and advantages of the present invention. Although the content was originally broadcast, it cannot be

illegally copied or distributed. The present invention can be applied to pay per view offerings, as well as standard broadcast material.

Referring to the specifics of FIG. 8, the process of implementing the core acquisition option of broadcast digital content 124 (see FIG. 5) proceeds as follows. At step 180, a receiver/translator/recording device 190 receives digitally broadcast content in copy-protected format from a source 192 such as satellite, cable, Internet, or over-air. The broadcast content may be copy-protected using a copy-protection technology such as an enhanced CSS scheme. If a consumer wishes to only play (not record) the broadcast content, basic decoding (e.g., CSS decoding) is performed and the broadcast content is passed through to presentation device 194 for playback. The remaining steps below may be skipped.

If, however, the consumer wishes to record the broadcast content, the following additional steps are performed prior to sending the broadcast content on for playback. At step 181, the receiver/translator/recording device 190 retrieves an account number from the consumer's physical key (transponder) 196 over a secure RF link. At step 182, the receiver/translator/recording device 190 transmits the account number and its recorder serial code to a key provider's web site 198. Each device 190 contains a recorder serial code that uniquely identifies the device. The format of the recorder serial code may, for example, be MMMM.FFF.0123456789 where MMMM is a manufacturer identification, FFF is a facility identification, and the numbers represent a sequence number. At step 183, the key provider's web site 198 authenticates the data against its databases 200 and 202 and returns an "approved" or "rejected" response. A counter, used for the key provider's billing purposes, is incremented. At step 184, if a "rejected" response is received, the broadcast content cannot be recorded. If an "approved" response is received, the receiver/translator/recording device 190 translates the decoded content into a key-secured format by encoding it with the consumer's activation code, and records the key-secured content, with the recorder serial code permanently embedded within, to a storage device (that can optionally be an external device).

The broadcast content can now be copied to and played back on any key-enabled playback device. At step 185, invoices 199 are generated and sent to content distributors by the key provider's web site 198 on a regular cycle. While providing excellent additional security and protections, steps 182 and 183 are not mandatory for the present invention to function with broadcast content. It may be desirable, for cost purposes, to produce receiver/translator/recording devices 190 not capable of communicating with the key provider's web site 198.

Referring to FIGS. 9a and 9b generally, having acquired key-secured digital content and produced copies for playback on various devices such as a portable CD player, personal computer, home theater, etc., a consumer is now ready to use the digital content. Playback of key-secured content occurs as follows. A key-enabled playback device transparently reads information from a consumer's physical key and from the content file the consumer has requested to play. The pieces of information are then compared to validate that the physical key "matches" the content to be played. If the elements match, the device begins playback of the content. If the elements do not match, the device will not play the content and, depending upon the device's capabilities, may display an "invalid content" message. From a consumer's point of view, when used with legitimately-acquired content, the process is entirely transparent, effortless, and non-intrusive. The consumer is free to use their content on any key-enabled playback device, with the only restriction being that the content can be played only when the associated physical key is present. As noted above, the present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to the specifics of FIGS. 9a and 9b, the process of implementing the core playback option of stand-alone devices 126 (see FIG. 5) proceeds as follows. At step 210, a consumer requests playback of a key-secured content file via a playback device 220. The playback device 220 may, for example, be the consumer's personal computer (FIG. 9a) or a stereo amplifier (FIG. 9b) with integrated compact disc reader/player. At step 211, a

receiver/decoder circuit 222 searches for a physical key (transponder) 224. The circuit 222 may be a separate component from the playback device 220 as in FIG. 9a or integrated into the playback device 220 as in FIG. 9b. If the physical key is not found, the playback device 220 displays an "invalid content" message. If the physical key is found, the receiver/decoder circuit 222 retrieves all available information from the physical key 224 over a secure RF link. At step 212, the user labels in the physical key 224 and the key-secured content file are compared. If the user labels do not match, the playback device 220 displays an "invalid" message. If the user labels do match, the receiver/decoder circuit 222 retrieves the software decryption key from the physical key 224 over the secure RF link between the physical key 224 and the playback device 220 and begins decryption of the encrypted portion of key-secured file. When the account number is decrypted, it is matched against the account number retrieved from the physical key 224. If the account numbers do not match, the playback device 220 displays an "invalid content" message. If the account numbers do match, the software decryption key is used by the playback device 220 to decrypt remaining data in the key-secured file for playback. The user label and the account number in the physical key serve as a first activation code, and the user label and the account number in the content file serve as a second activation code. These activation codes must match (or have some other predetermined association) in order for playback to proceed.

Referring to FIG. 10 generally, while stand-alone playback devices (e.g., CD players, PCs, DVD players, etc.) are currently the norm, the convergence of these devices and the Internet will lead to an environment where centralized digital distribution systems proliferate. Security of content in these environments is critical yet challenging to accomplish without imposing great restrictions. The present invention can provide security to a centralized digital distribution system and, in addition, offers many important enhancements that greatly increase the convenience and usability of such a system. These enhancements include integration of the physical key into a portable handheld computer which then doubles as the system remote. In addition to controlling all

networked components, the remote is used for tasks such as purchasing content from the Internet, and tracking the movement of a user throughout a facility to provide automatic "content following" (i.e., where content playback follows the user from room to room). The centralized nature of the digital content distribution system means that only one storage device is required to maintain a consumer's entire digital content library (e.g., music, movies, software, E-books, etc.) and to feed that content to any networked playback device.

Referring to the specifics of FIG. 10, there is shown a centralized digital content distribution system for implementing the core playback option of networked devices 128 (see FIG. 5). The system is used in an establishment such as a residence or entertainment facility. The system includes a digital content server 310, a distribution hub 312, a plurality of remote clients 314, and a portable remote control 316. The digital content server 310 stores digital content acquired from a source 318 such as satellite, cable, Internet, or over-air. In addition, the digital content server 310 may store digital content uploaded from a standard component 324. The plurality of remote clients 314 are located in different rooms of the establishment and linked to the digital content server 310 via the distribution hub 312 or switch. The remote clients 314 are linked to the distribution hub 312 by a backbone transmission network 315. The backbone transmission network 315 may be wireless or wired with fiber optic cables, coaxial cables, or twisted pair cables, may employ a networking protocol such as Ethernet, Wi-Fi, Arcnet, or ATM (Asynchronous Transfer Mode), and may employ a communications protocol such as TCP/IP. Each remote client 314 includes a network interface card (NIC) for interfacing with the backbone transmission network 315.

The remote control 316 is adapted to communicate with each of the remote clients 314 and select the digital content stored in the digital content server 310. The remote control 316 is essentially a personal digital assistant (i.e., hand-held computer) including a display and added remote control circuitry. The display may, for example, be a liquid crystal display (LCD). The

added remote control circuitry includes "system remote" circuitry and "universal remote" circuitry.

The "system remote" circuitry in the remote control 316 is for establishing a first wireless transmission link 320 with each of the remote clients 314. The first wireless transmission link 320 may be a secure radio link (RF) as shown or an infrared link (IR). Upon establishing the first wireless transmission link 320 with one of the remote clients 314, the remote control 316 serves as a system remote capable of (1) displaying, scanning, and selecting the digital content available on the digital content server 310 and downloading the selected digital content from the digital content server 310 to the linked remote client 314 and (2) controlling the digital content server 310 to acquire or download digital content from a source 318 such as satellite, cable, Internet, or over-air. As used herein, the term "download" and similar variations thereof (e.g., downloaded, downloading, etc.) is intended to cover the transfer of content from one device to a receiving device whether the content is stored on the receiving device or merely "streamed" to the receiving device for immediate playback. The remote control 316 preferably includes a display for displaying the digital content. The display may, for example, be a liquid crystal display (LCD). As a user holding the remote control 316 moves from room to room of the establishment, the remote control 316 successively establishes wireless transmission links 320 with the remote clients 314 in the respective rooms. In this way, the digital content available on the digital content server 310 follows the user's movement from room to room.

In a preferred embodiment, the first wireless transmission link 320 is a secure radio link established by matching transceivers in the remote control 316 and each remote client 314. The matching transceivers are preferably small, inexpensive Bluetooth™ radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are integrated into the respective remote control 316 and each remote client 314, which can then communicate over short distances and through obstacles by means of radio

waves. Wireless technologies other than Bluetooth, such as Wi-Fi, may be used to communicate remote control signals between the remote control 316 and each remote client 314.

The "universal remote" circuitry in the remote control 316 is for establishing a second wireless transmission link 322 with standard components 324 connected to the remote clients 314. The second wireless transmission link 322 is preferably an infrared link (IR) as shown. Upon establishing the second wireless transmission link 322 with one of the standard components 324, the remote control 316 series as a universal remote capable of operating the standard component 324. The standard component 324 may, for example, be an audio receiver (stereo amplifier), an audiovisual receiver, a video monitor (television), etc. The standard components 324 may be physically separate from, but linked to, the respective remote clients 314 or may be physically integrated into the respective remote clients 314 like integrated device 324c.

The digital content stored on the digital content server 310 may be formatted as a compact disc (CD), digital video disc (DVD), MP3, electronic book, software, etc. When the remote control 316 is linked to one of the remote clients 314, a user may scan and select digital content to be downloaded from the digital content server 310 to the remote client 314 and converted by the remote client 314 to a standard playable format (e.g., analog format) that can be played on the associated standard component 324. The selected digital content is downloaded from the digital content server 310 to the remote client 314 as raw digital data packets. The remote client 314, in turn, converts the downloaded digital content to a standard component output(s) compatible with a standard component 324 connected to the remote client 314, and the standard component 324 plays the digital content. Ports may, for example, include S-Video, RCA jacks, serial ports, Universal Serial Bus, Ethernet, Wi-Fi, Firewire™, Bluetooth, RF, or other similar outputs. The standard component 324 incorporates, or is linked to, audio speakers for broadcasting any audio signals received from the remote client 314 and a video monitor for displaying any video signals received from the remote client 314.

All content is stored on the digital content server 310 digitally, and is key-secured if obtained via the download or broadcast acquisition options of FIGS. 6 and 8. If the digital content is key-secured, the plurality of remote clients 314 include decryption circuitry (i.e., receiver/decoder circuit) for unlocking the digital content. The digital content selected for download from the digital content server 310 to a remote client 314 preferably remains encrypted until converted to a standard component output(s) in the remote client 314. The remote client 314 acts as a converter between key-secured digital content from the digital content server 310 and the standard component output(s). To decrypt the selected digital content, the remote control 316 contains a physical key initially acquired from a key provider in accordance with the present invention. The digital content is initially acquired from a content provider 326 that marks the digital content with an activation code associated with the physical key. The decryption circuitry in the remote client 314 receives an activation code from the remote control 316 via the wireless transmission link 320 and is enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content. If the activation code in the remote control 316 is not associated with the activation code in the digital content, the remote client 314 will not unlock and convert the digital content.

In an alternative embodiment, the remote clients 314 are eliminated and the standard components 324 are linked directly to standard component outputs of the distribution hub 312 by the backbone transmission network 315. In this case, the distribution hub 312 serves as a switch, and the digital content server 310 contains the decryption circuitry for unlocking the digital content. As the digital content is decrypted, it is converted to a playable format and fed to the distribution switch 312 for delivery to the appropriate standard component 324. The decryption circuitry in the digital content server 310 receives the activation code from the remote control 316 and is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content.

Instead of decrypting the digital content so that it can be played, the digital content may be downloaded (or "passed through") in its encrypted format to a storage device such as a media burner 324a or computer hard disk 324b for storage thereon. When a user ultimately desires to play the stored digital content on a media player, the media player must contain the decryption circuitry for unlocking the digital content. After unlocking the digital content, the media player converts the unlocked digital content to a playable format and plays the digital content. The decryption circuitry in the media player receives the activation code from the remote control 316 or physical key with the same activation code. The media player is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 or physical key is associated with the activation code in the digital content.

In addition to downloading selected digital content from the digital content server 310 to the remote clients 314, data (e.g., MP3, CD, DVD, software, etc.) from the standard components 324 can be uploaded to the digital content server 310 and stored digitally thereon. This allows for storage of legacy content on the digital content server 310.

Referring to FIG. 11 generally, a digital content security system and method protects computers from unauthorized use and protects the digital content stored on computers from being wrongfully accessed, copying, and/or distributed. The basic components of the Personal Digital Key Digital Content Security System (PDK-DCSS) are (1) a standard hard drive device 330, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) 332 integrated into the controller 334, and (2) a PDK-Key 336 associated with the PDK-RDC as described above. The standard computer hard drive 330 incorporates the integrated PDK-RDC 332 for the purpose of enabling multiple methods of securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the PDK-RDC 332 as being integrated with the hard drive's controller 334, all OS-level protections described below can be implemented using externally-based PDK-RDCs.

A PDK hard drive 330 is similar to any standard, currently available hard drive with the exception of the PDK-RDC 332 (which is integrated into the drive's controller circuit 334). A PDK-RDC 332 is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content. Additionally, this circuit 332 is able to secure the hard drive 330 itself. This is implemented by the circuit 332 enabling or disabling the hard drive's controller 334 depending on whether an associated PDK-Key 336 (one which is uniquely and permanently associated with the PDK hard drive 330) is present. Each PDK hard drive 330 would typically be delivered with its own PDK-Key 336.

Secure RF communications between a PDK-Key 336 and its associated hard drive 330 occurs in the same manner as described above. It should be noted that software drivers can optionally be designed to allow for dynamic key assignment (assigning of keys after purchase to enable key swapping, or assigning of individual keys to multiple devices).

The PDK-Key and RDC technology is utilized to provide two categories of protection:

1) Hard drive access control - where an entire drive 330 is either completely accessible (unlocked) or inaccessible (locked), and/or individual data sectors or clusters of data sectors are optionally encrypted/decrypted, depending on whether the specific PDK-Key 336 associated (and shipped) with the drive 330 is within range. This category of protection can be accomplished transparently to the operating system (OS) responsible for managing the drive.

2) OS-level independent file protection - where the drive's RDC 332 functions independently of the drive 330 to protect individual files (typically copyrighted material) from wrongful copying. In this role, the RDC 332 works with any PDK-Key 336 (not just the one delivered with the drive 330) and any PDK-compliant file (they do not have to be stored on or associated with the hard drive 330). This category of protection requires an OS-level software driver be run under the OS responsible for managing the drive.

By utilizing these two categories of protection in various ways, four unique levels of content protection are enabled. Two of the levels (Drive-Level and Sector-Level) do not require external software support, while the remaining two (File-Level and Network-Level) require software drivers, as well as a stand-alone application for Network-Level implementations. Each of the four levels is defined below.

Referring to FIGS. 12 and 13 for Drive-Level protection, when implemented, a PDK hard drive 330 will only function when the associated PDK-Key 336 is within range. The drive's controller 334 is disabled whenever the PDK-Key 336 is not present. The contents of files stored on the drive 330 are not encrypted. The Drive-Level protection feature is designed to protect the hard drive's owner by locking access to the PDK hard drive 330 whenever the associated PDK-Key 336 is not present (i.e. when the owner momentarily steps away from the computer, if the computer is stolen, etc.).

Referring to FIGS. 12 and 13 for Sector-Level protection, when enabled, every sector (or cluster of sectors) read or written is encrypted/decrypted by the RDC 332 using the drive's associated PDK-Key 336. Because the encryption is performed at Sector-Level as opposed to File-Level, the encoding can be accomplished without requiring any changes, involvement, or acknowledgement of the OS responsible for managing the drive. The Sector-Level protection feature is designed to further protect the hard drive's owner (beyond Drive-Level protection) by encrypting the contents of the files stored on the drive, without requiring any software modifications (OS, application, etc.). The security advantage is that if the drive access is in some way defeated, the contents of files on the drive are still protected. It should be noted that if users retrieve files from drive and purposely transfer them anywhere else (via email, memory sticks, etc.), the data will no longer be protected. Drive-Level protection and Sector-Level protection may be used individually or in combination. Also, as noted above, it should be understood that Sector-Level protection may be applied to individual data sectors or clusters of data sectors.

FIG. 13 illustrates the logic executed by the RDC 332 for implementing Drive-Level protection and Sector-Level protection. The logic ensures OS-level commands (save entire file, read entire file, etc.) are given adequate time to complete. This enables implementation of logic without requiring OS changes, involvement, or acknowledgement.

Referring to FIG. 14 for File-Level protection, implemented as an OS-level software driver utilizing the PDK-RDC 332 integrated in the PDK hard drive 330, File-Level protection provides standard PDK digital rights management services and functionality as described above. As needed, the driver instructs the RDC 332 to acquire PDK-Key information, validate the key-to-file match, and use the key's information to perform actual encryption/decryption of the file (as a whole, not at the sector level). In the illustrated example, the file ABC 338 (which can reside on any storage device, in memory, etc.) is compared to any PDK-Key 336 within range of the PDK-RDC 332. If a match is found, the PDK-RDC 332 will decrypt the file 338 for use with whatever playback mechanism placed the request. Any PDK-Key 336 can be utilized, not just the key 336 associated with the PDK hard drive 330. When employed for File-Level protection (and Network-Level protection as described below), the PDK-RDC 332 functions independently of the hard drive 330 in which it resides. While PDK-compliant files it encrypts or decrypts may reside on the resident hard drive 330 and may be associated with the drive's PDK-Key 336, they do not have to be. The PDK-RDC 332 can work with other PDK-Keys and files residing on other mediums. When used in this manner, the PDK-RDC 332 can be thought of as just coincidently residing within the hard drive 330. For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

The primary use of File-Level protection is to secure and protect private or copyrighted material from wrongful copying and distribution. Because copies of any PDK-compliant files can only be accessed when the associated PDK-Key is present, File-Level protection enables copies (intended for use by the holder of

the associated key) to be produced effortlessly and securely. In addition to the distribution of copyrighted content such as music and movies as described above, software developers can distribute their software products via the Internet with the same ease and security. Software distributed in this manner would allow the legal recipient to make unlimited copies (for backup purposes, use on a home computer, etc.), yet the copies would only function when the associated key is present, preventing unauthorized copies from being wrongfully distributed and used.

The File-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and pasted into another application (e.g., an email program) thereby defeating the protection. Therefore the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations.

Referring to FIG. 15 for Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application / database called a PDK Document Controller (DC) 340 ruing on a server 342. A DC 340 enables the creation of Groups 342 that list which PDK-Keys 344 are allowed access to files in specific directories. All files stored in directories controlled by the DC 340 are automatically encrypted using the DC administrator's PDK-Key and thereby become PDK-compliant files. This process places all files stored in the DC 340 in a uniformly encrypted format.

Each user request for a file residing in a directory listed in a DC Group 342 results in the following steps. An RDC located in the requester's workstation 346 acquires information from the user's PDK-Key 344 and relays that information to the DC 340. The DC then enables appropriate access as

defined by the DC's Group database information. Specifically, the DC 340 performing a lookup of the requester's PDK-Key 344 in the appropriate Group's tables. If the DC 340 determines that the PDK-Key 344 is listed in a Group 342 that also lists the directory containing the file the user wishes to access, the DC 340 knows that a valid PDK-Key 344 was used in the file request and grants access. The requested file is first decrypted with the administrator's PDK-Key, re-encrypted with the requester's PDK-Key 344, and then downloaded to the user's workstation 346. The foregoing process mirrors the process employed when using PDK to download digital media files from the Internet.

The Network-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and paste into another application (e.g., an email program) thereby defeating the protection. Therefore, the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations. The system is well suited for establishing centralized databases of secure documents intended for distribution to entrusted recipients such as personnel in a law firm or medical facility.

While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention. A number of enhancements and variations can be implemented/utilized that effectively broaden the PDK technology's scope and utility. These enhancements and alternative embodiments are summarized below.

Integration of RDCs into Alternative Storage Devices. This embodiment involves integrating RDCs into alternative storage mechanisms

beyond those of basic hard drives. These storage mechanisms include pure RAM/ROM-based storage commonly included/used in devices such as PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, and DVR players, as well as portable storage devices such as Memory Sticks, Secure Digital memory cards, or any similar such product, in which case the RDC is either directly installed on the device, or integrated into the device in which the memory cards/sticks are inserted.

When an RDC is utilized in this manner, File-Level and Network-Level security function in the same manner as that described above for PDK hard drives. Drive-Level and Sector-Level security function in the same *logical* manner as that described for hard drives, but the *physical* implementation varies so as to control the bus structure that provides the communications path between the storage mechanisms and their hosting devices. As with PDK hard drives, access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either "ready" or "busy," effectively enabling/disabling the device itself. To save batteries, RDCs used in this manner may only check for the presence of the associated PDK-Key on some periodic basis (versus every read or write sequence). And similar to PDK hard drives, Sector-Level security can be optionally utilized to encrypt/decrypt data traveling over the bus prior to writes and after reads to provide PDK's standard Sector-
Level data encoding functionality.

As when utilized in PDK hard drives, the PDK's security features provide the same convenient, non-intrusive, wireless security mechanism for the above-defined devices. This security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely "disabled" to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled.

Dynamic PDK-Key Management. Utilizing dynamic PDK-Key management, PDK-Keys can be assigned to an RDC (whether integrated into a

PDK hard drive or some other hosting device, or implemented independently) by a user (versus requiring such assignment at time of production). This capability is accomplished by including the required logic within the RDC's internal firmware (versus using an externally-based software driver to supply such capability).

Using this capability, a user can optionally assign any PDK-Key to act as the RDC's *master* key (the first key assigned to the device). Then by involving this *master* key (to prove the original "owner's" validation of the process), the user can assign (or remove) *additional* keys to the PDK-device. The general benefits of this feature include:

- The ability for the individual possessing the *master* key to create backup keys (to be stored and later retrieved in the event the *master* is ever lost), and to allow other users (those possessing *additional* keys) to also access their PDK device(s).
- The option to ship PDK-RDCs (in any configuration, host devices, etc.) without any PDK-Keys. And to allow such devices containing these RDCs (such as PDK hard drives) to optionally function with all or part of the PDK-technology never enabled or utilized. For instance, a user may elect to not enable Drive-Level and Sector-Level security features, but still utilize the functionalities of File-Level and Network-Level security.
- Giving users the option to purchase and associate a PDK-Key at a later time, or importantly, assign a PDK-Key they *already* utilize for another PDK-based device. This allows a user to utilize a single PDK-Key to provide access to all their PDK-based devices.

This built-in (firmware-based) PDK-Key configuration/management capability greatly enhances PDK's overall flexibility and ease of setup/use.

Independent RDC configuration. While integrating an RDC into a hard drive offers numerous benefits, RDCs may exist separately from hard drive mechanisms. In this configuration (as previously defined) an RDC's physical circuitry may exist in the form of a PC Card, a PC expansion board that plugs into a standard PC expansion slot, a USB-based plug-in board, or any other

similar design able to interface with a hosting device. Used in this manner, RDCs provide all previously defined functionalities with the exception of basic hard drive access-control.

Buffer Flush & Notification Software Driver. This enhancement involves using a simple software device driver to recognize when a PDK-Key is out of range (by "watching" for signals from the RDC), and when such a condition is detected to flush (empty) the host system's "read" buffer (effectively clearing any data the system may have been cached in internal memory in order to speed data access), and display a simple message indicating the PDK-Key is in/out of range. This optional mechanism can be utilized with any RDC configuration and on any PDK-protected device.

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

CLAIMS:

1. A system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.
2. The system of claim 1, further comprising a reader/decoder circuit wherein the personal digital key is a tangible object, capable of wireless communication with the reader/decoder circuit.
3. The system of claim 2 further comprising a computer with a computer hard drive, wherein the reader/decoder circuit is located in the computer hard drive.
4. The system of claim 2 further comprising a swipe unit, wherein the reader/decoder circuit is located in the swipe unit.
5. The system of claim 1, further comprising a second personal digital key wherein the second digital key also authenticates a user attempting to access the computer readable medium.
6. The system of claim 1 wherein the personal digital key is a tangible article.
7. The system of claim 3, wherein the reader/decoder circuit is integrated with the computer.
8. The system of claim 3, wherein the computer comprises a personal digital key hard drive.
9. The system of claim 3, wherein the computer further comprises a reader/decoder circuit card.
10. The system of claim 3 wherein data from the personal digital key transfers and receives data through a secure RF port on the computer.
11. The system of claim 3 wherein the computer transmits and receives data from a provider through an Internet connection.
12. The system of claim 3, further comprising a database wherein the database includes an account identifier and a personal digital key identifier.

13. The system of claim 3 wherein data transmitted by the personal digital key to the computer is authenticated by personal digital key data stored in the database.

14. The system of claim 4 wherein the swipe unit transfers and receives data from a provider through an Internet connection.

15. The system of claim 4 wherein wherein data transmitted by the personal digital key to the reader is authenticated by personal digital key data stored in the database.

16. A method for securing computer readable media from unauthorized access, comprising:

Providing a tangible, personal digital key to a user, wherein the personal digital key is stores information unique to the user; and,

Authenticating the user if the information relayed from the personal digital key matches identification data separately provided.

17. The method of claim 16, wherein the identification data is data from a credit card.

18. The method of claim 16 wherein the personal digital key transmits the unique information through a wireless link.

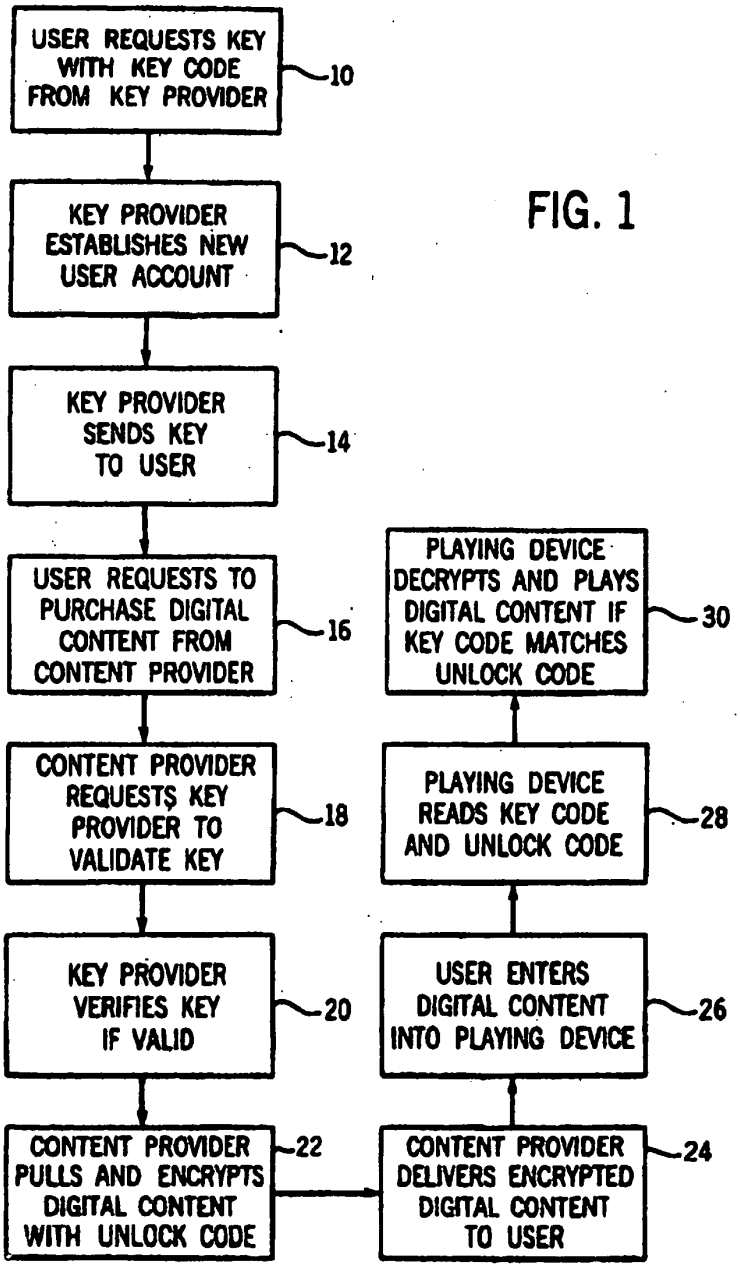

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT PROVIDER PULLS AND ENCRYPTS DIGITAL CONTENT WITH UNLOCK CODE
22
CONTENT PROVIDER DELIVERS ENCRYPTED DIGITAL CONTENT TO USER
24
USER ENTERS DIGITAL CONTENT INTO PLAYING DEVICE
26
PLAYING DEVICE READS KEY CODE AND UNLOCK CODE
28
PLAYING DEVICE DECRYPTS AND PLAYS DIGITAL CONTENT IF KEY CODE MATCHES UNLOCK CODE
30

FIG. 1

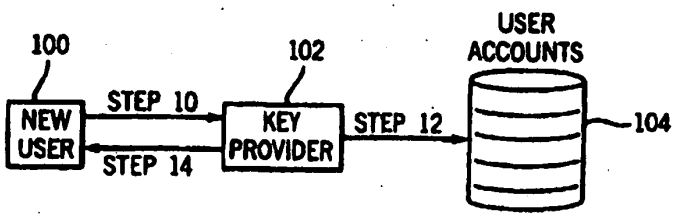


FIG. 2

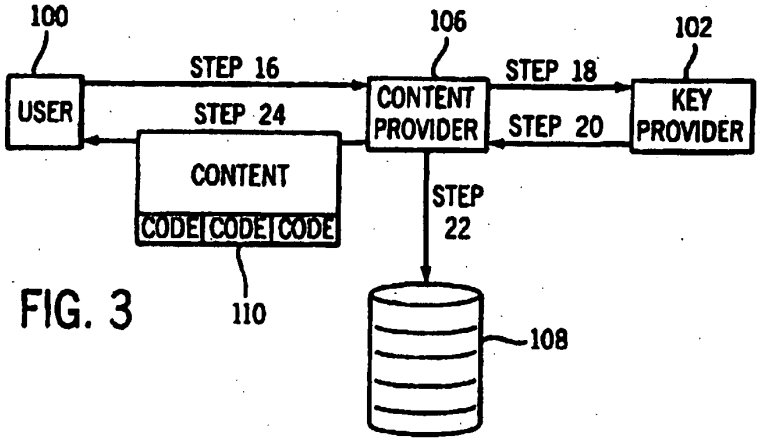


FIG. 3

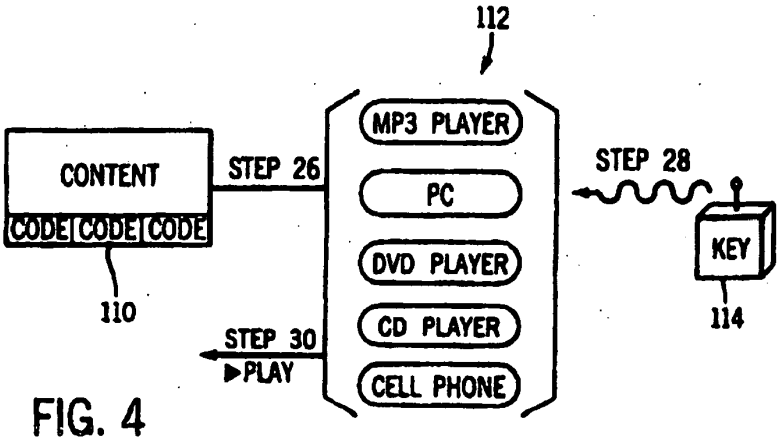


FIG. 4

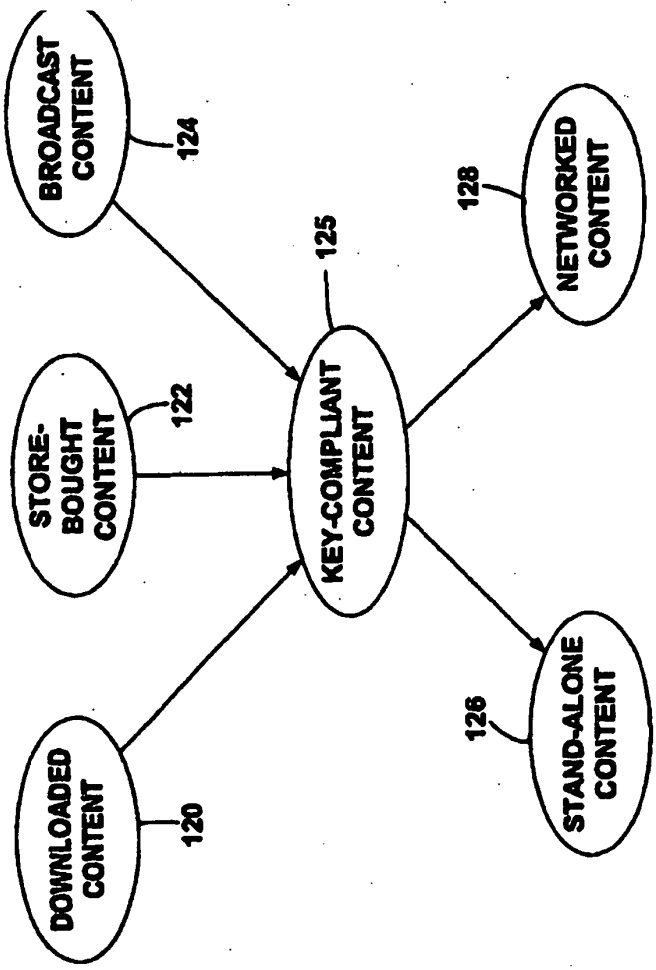

BROADCAST CONTENT
124
STORE-BOUGHT CONTENT
122
DOWNLOADED CONTENT
120
KEY-COMPLIANT CONTENT
125
NETWORKED CONTENT
128
STAND-ALONE CONTENT
126

FIG. 5

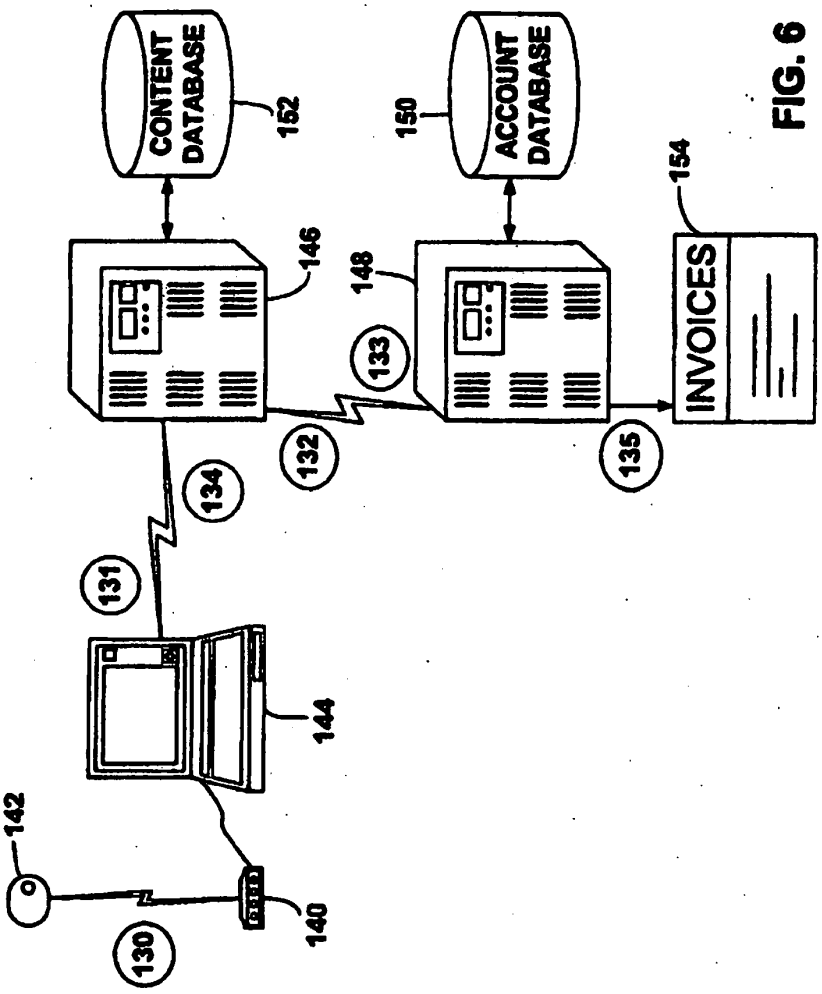

CONTENT DATABASE
152
ACCOUNT DATABASE
150
154
INVOICES
146
148
133
132
134
135
131
144
142
140
130

FIG. 6

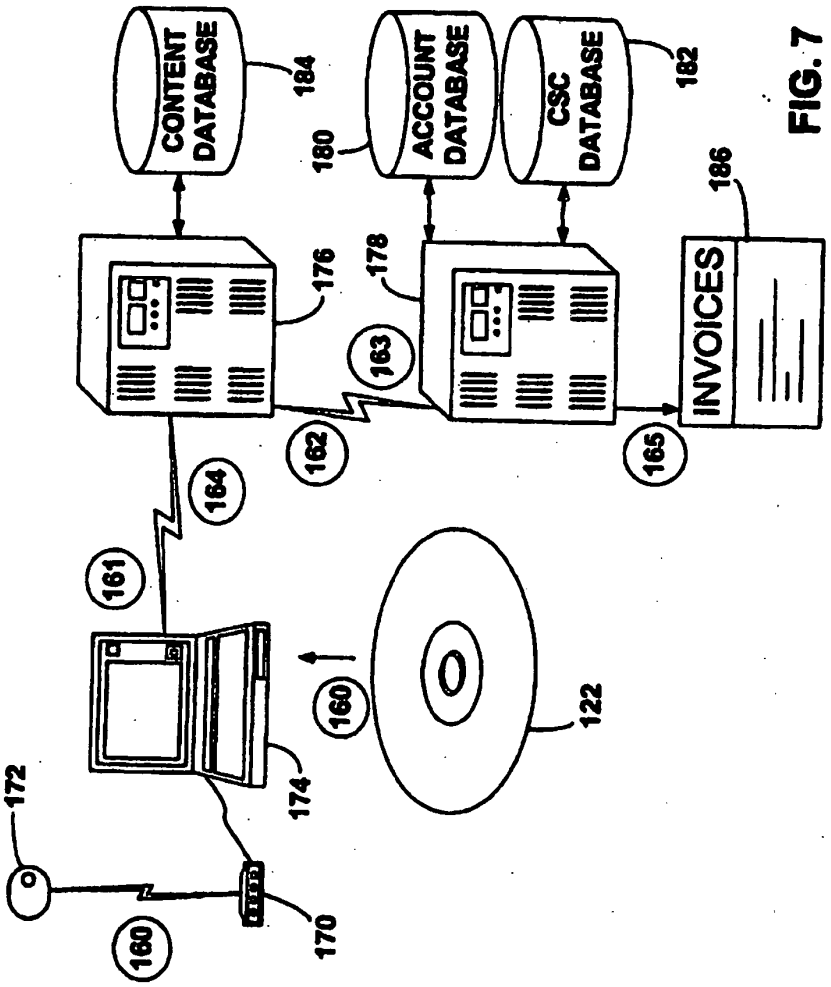

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
186
INVOICES
176
178
163
162
165
164
161
160
122
174
172
160
170

FIG. 7

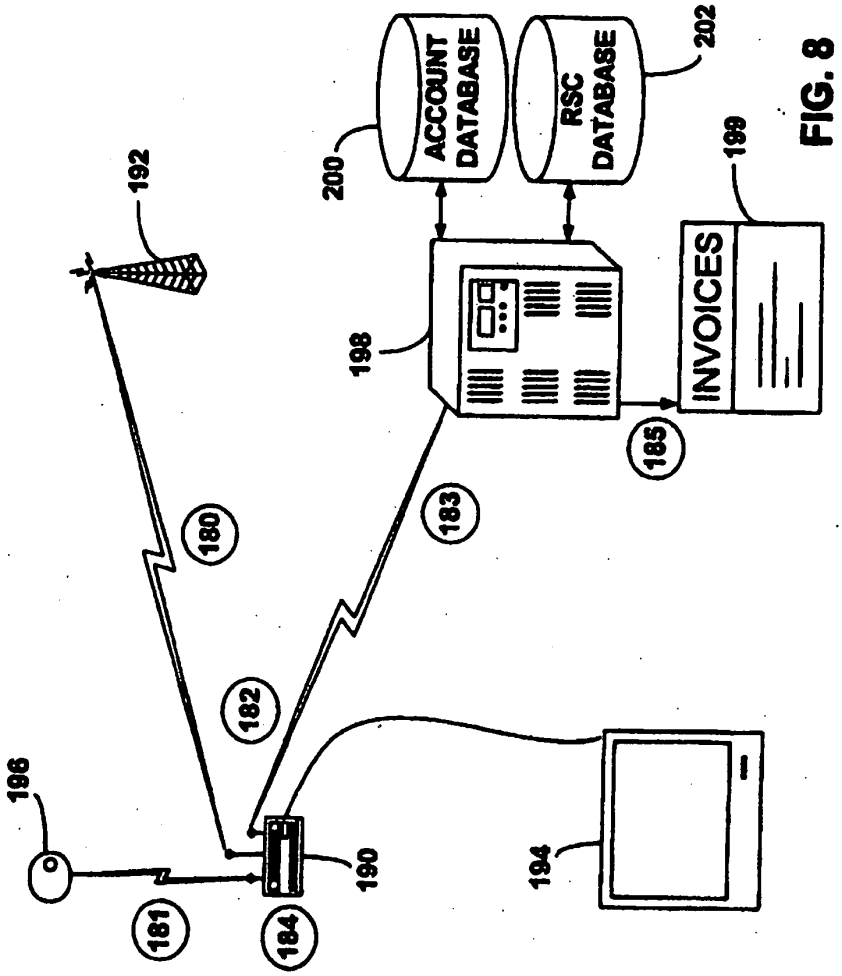

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
198
192
180
183
182
185
196
190
194
181
184

FIG. 8

FIG. 9a

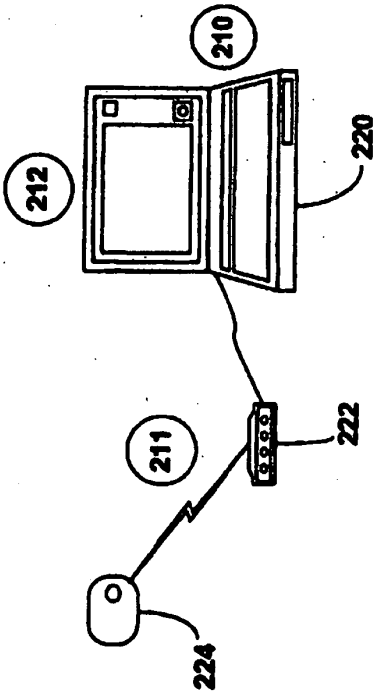
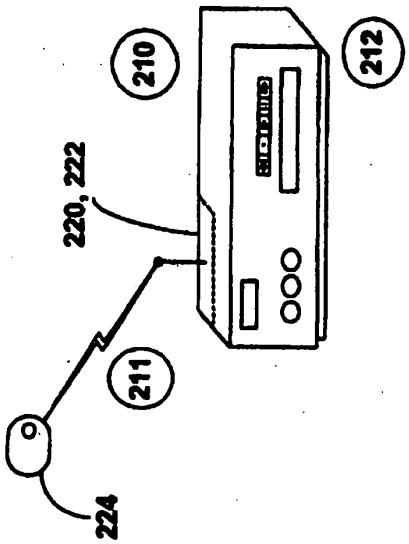


FIG. 9b



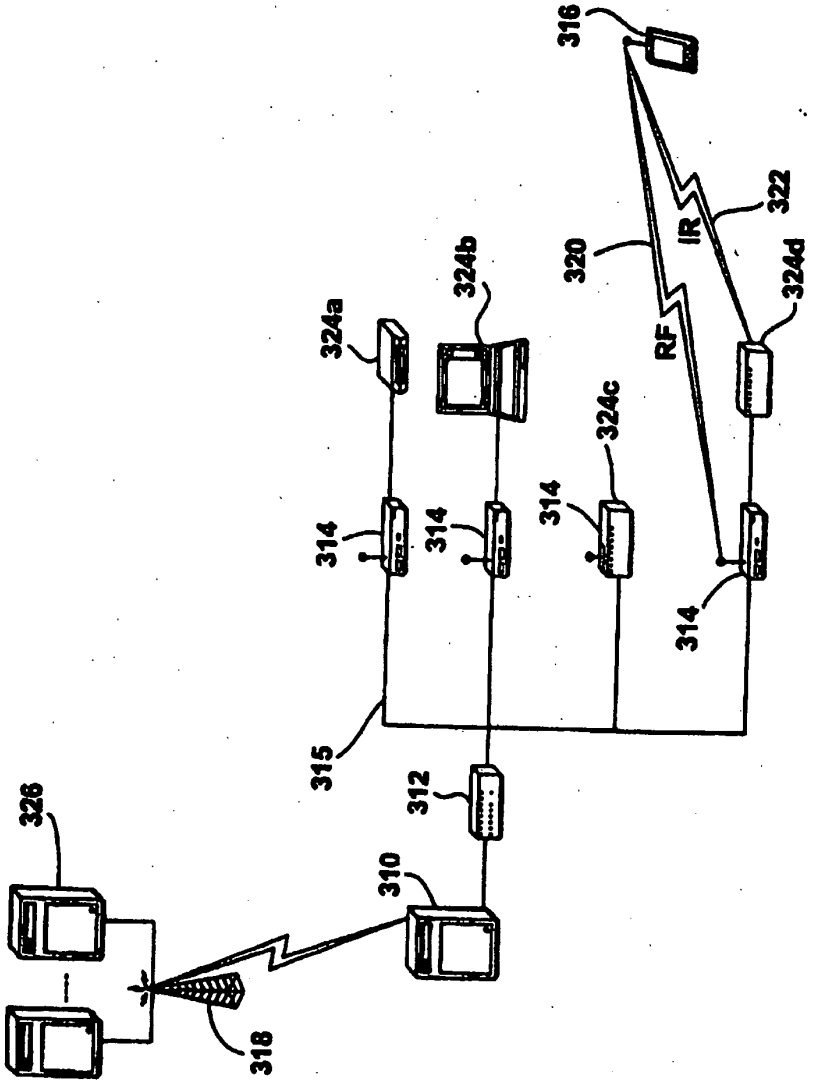

316
320
IR
322
RF
324d
324a
324b
324c
314
314
314
314
315
312
310
326
318

FIG. 10

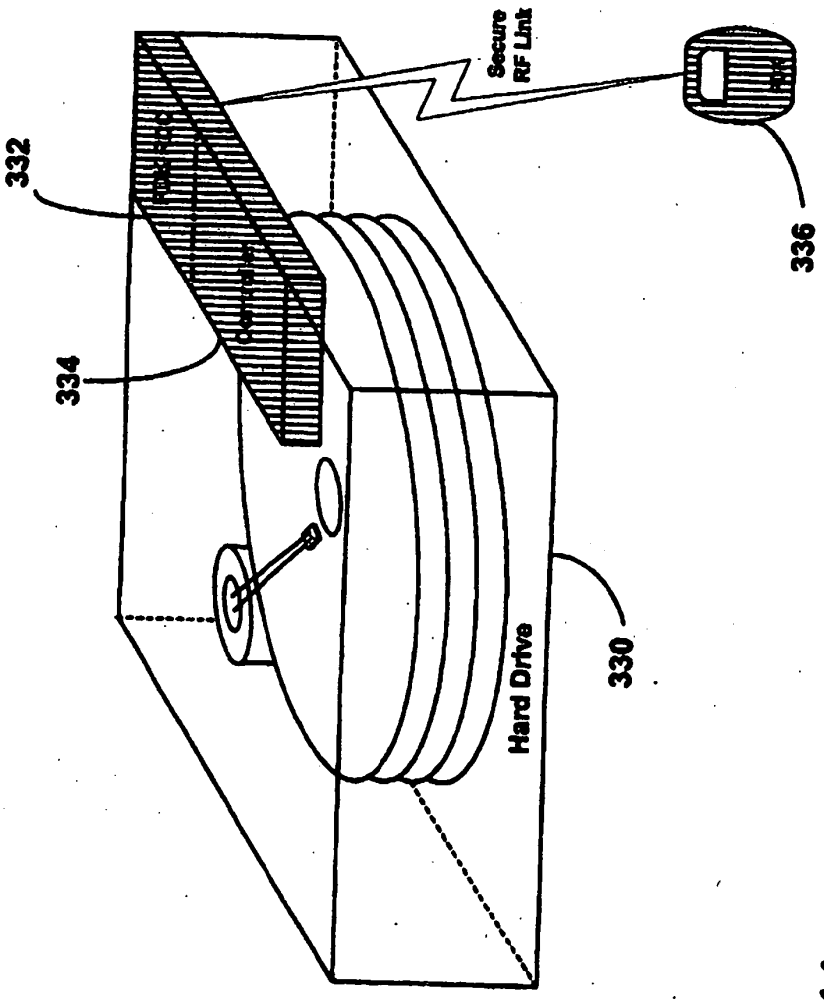


FIG. 11

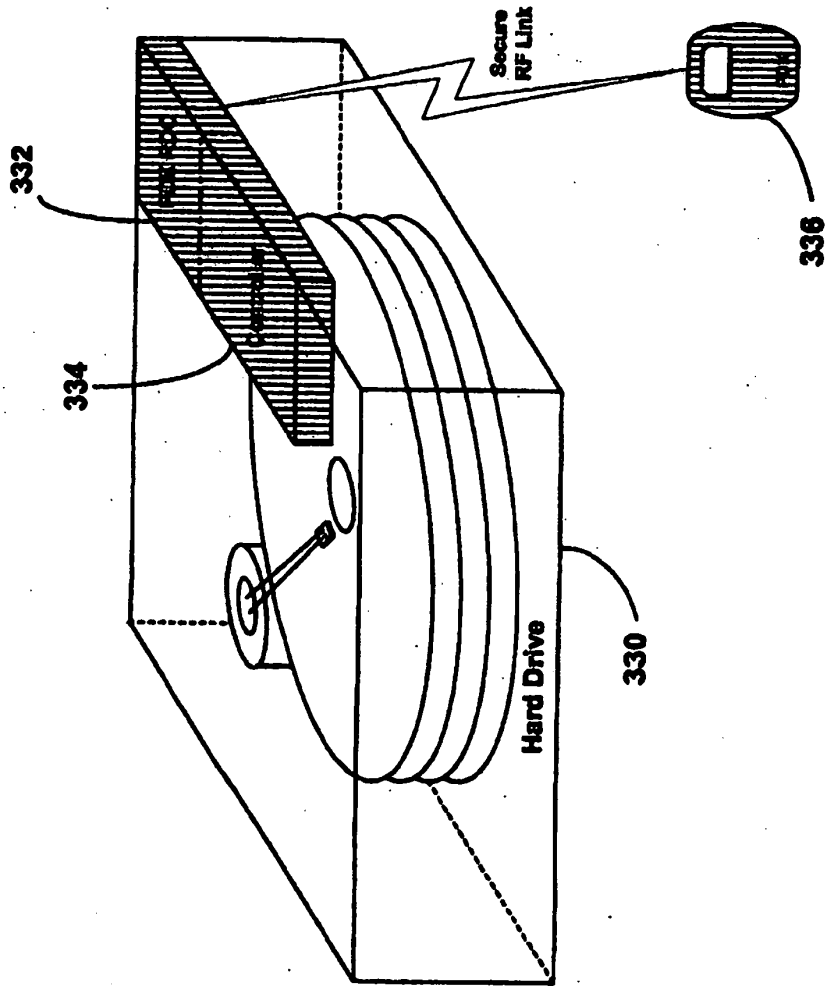


FIG. 12

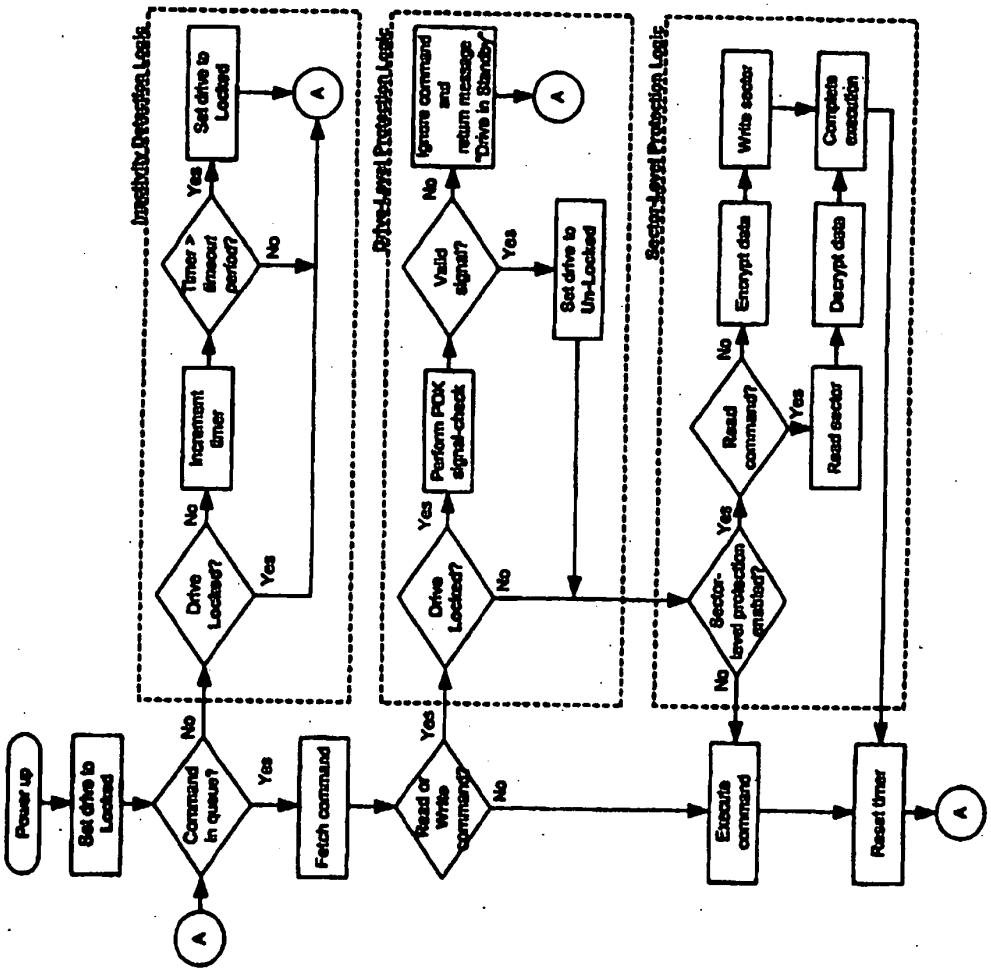

Power up
Set drive to Locked
Command in queue?
No
Yes
Fetch command
Read or Write command?
Yes
No
Inactivity Protection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
Drive-Level Protection Logic
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
Set drive to Un-Locked
Sector-Level Protection Logic
Sector-level protection enabled?
Yes
No
Read command?
No
Yes
Encrypt data
Write sector
Read sector
Decrypt data
Complete execution
Execute command
Reset timer
A

FIG. 13

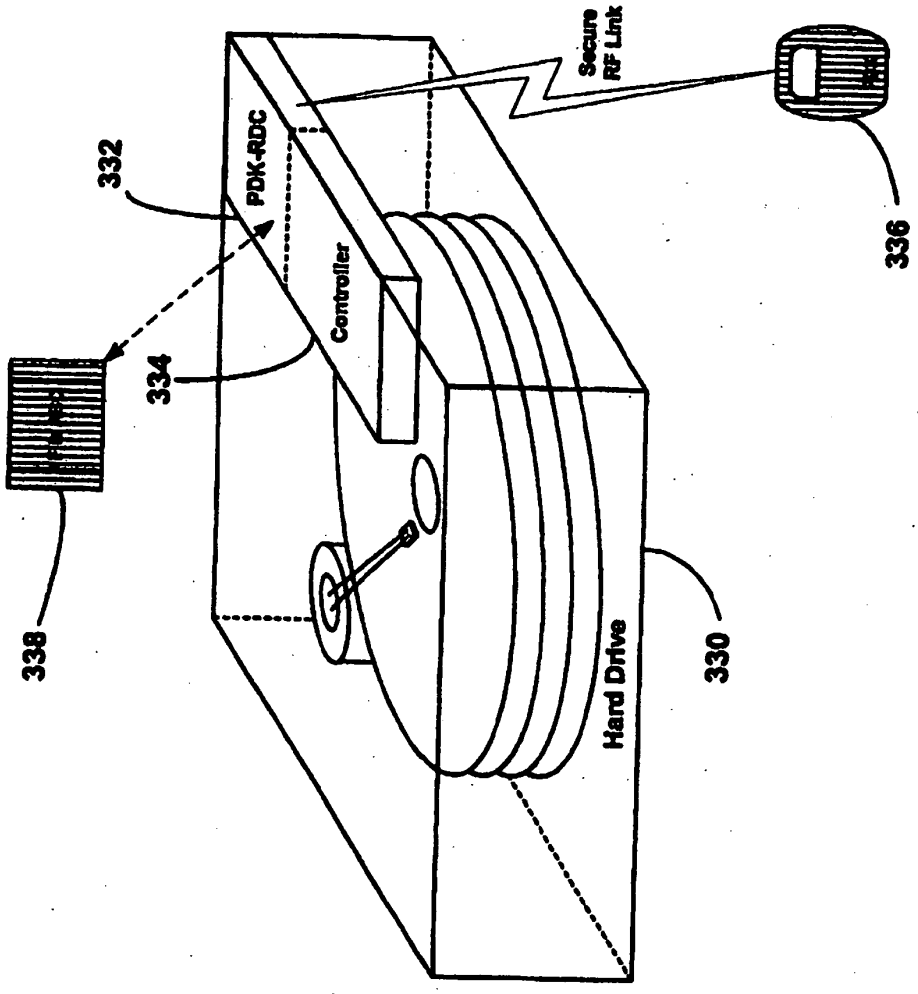

Secure
RF Link
PDK-RDC
332
Controller
334
336
338
330
Hard Drive

FIG. 14

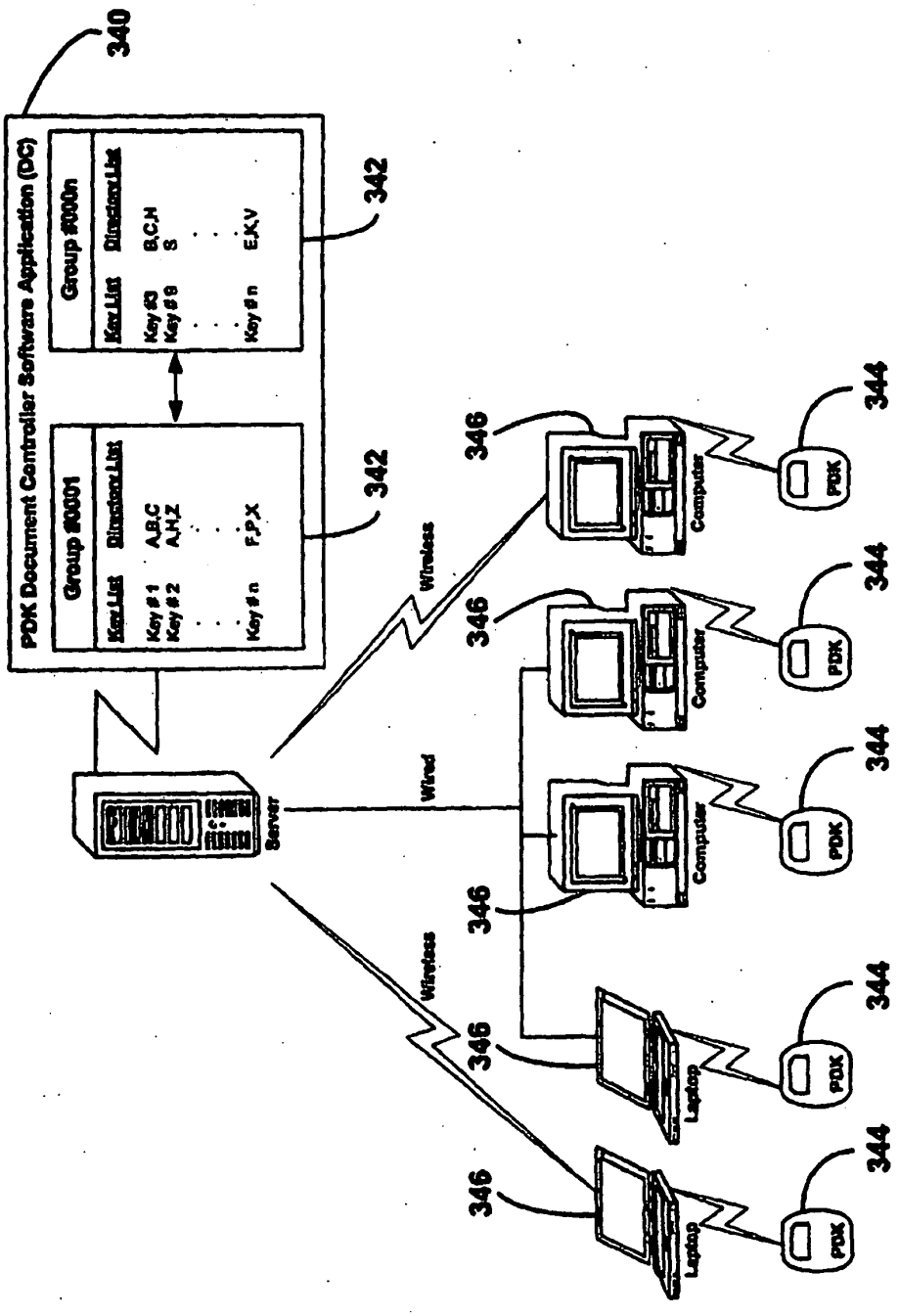

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key #1
Key #2
Key #n
A,B,C
A,H,Z
F,P,X
Group #000n
Key #3
Key #8
Key #n
B,C,H
S
E,K,V
342
342
Server
Wired
Wireless
Wireless
Computer
Computer
Computer
Laptop
Laptop
PDK
PDK
PDK
PDK
PDK
346
346
346
346
346
344
344
344
344
344

FIG. 15

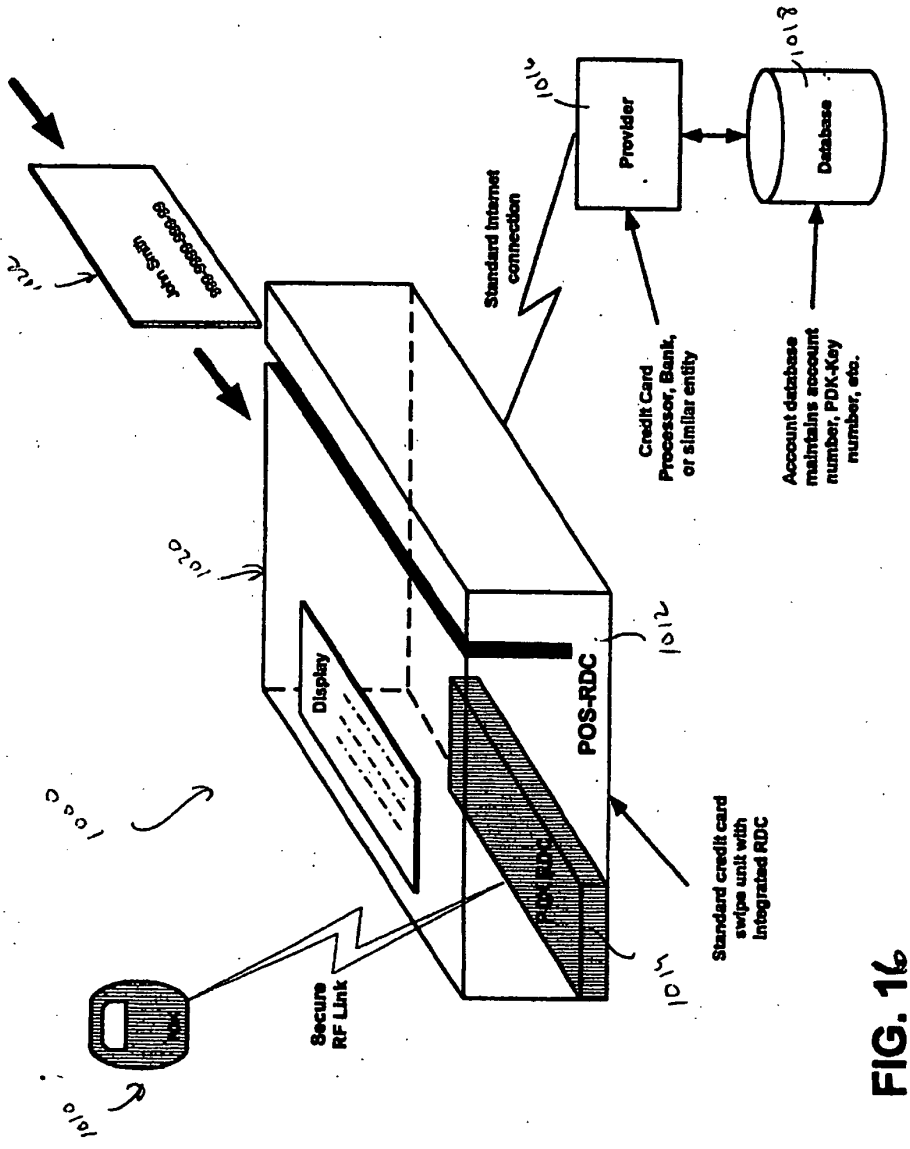

Provider
Database
Standard Internet connection
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
Display
POS-RDC
Standard credit card swipe unit with integrated RDC
Secure RF Link

FIG. 16

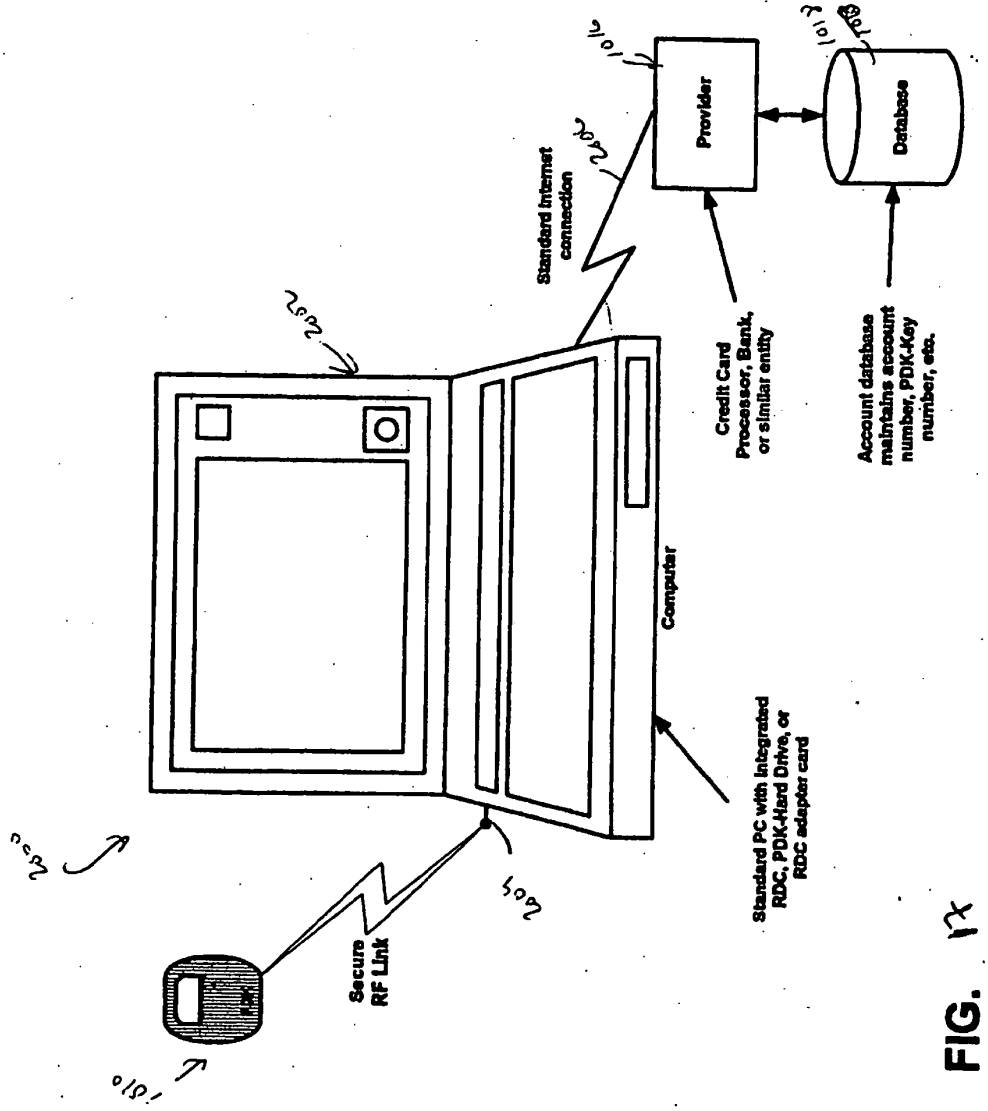

Provider
Database
Standard Internet connection
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
Computer
Standard PC with integrated RDC, PDK-Hard Drive, or RDC adapter card
Secure RF Link

FIG. 17

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086802 A3

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number:
PCT/US2005/007535

(22) International Filing Date: 8 March 2005 (08.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/551,320 8 March 2004 (08.03.2004) US

(71) Applicant *(for all designated States except US)*: **MARGENT DEVELOPMENT, LLC** [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; P.O. Box 2938, Minneapolis, MN 55402 (US).

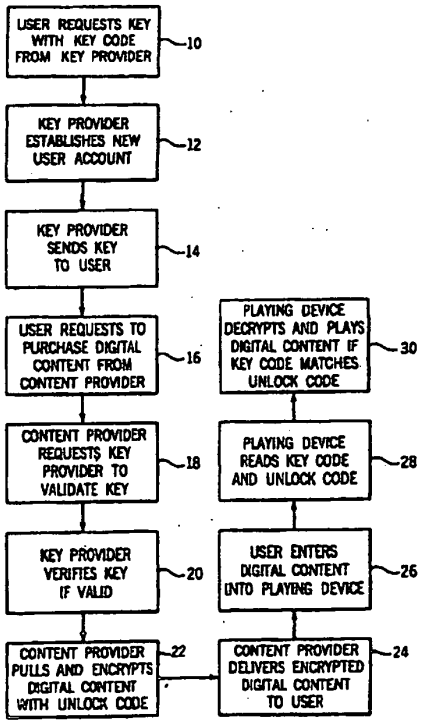
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)



(57) Abstract: One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.

WO 2005/086802 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
26 January 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/07535

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 17/60
US CL : 705/51
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/51

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20020124251 A1 (Hunter ET AL.) 05 September 2002 (05.09.2002) PARAGRAPHS 0001-0017 AND 0014	1-18
X	US 20030079133 A1 (Breiter ET AL.) 24 April 2003 (24.04.2003) PARAGRAPHS 0018 AND 0025.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 October 2005 (07.10.2005)	06 DEC 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. 571-272-3600

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

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 07 APR 2005
Applicant's or agent's file reference 2012.008WO1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/38124	International filing date (*day/month/year*) 15 November 2004 (15.11.2004)
Applicant MARGENT DEVELOPMENT, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Michelle L. Eason for Gilberto Barron Telephone No. 571-272-3799

(See notes on accompanying sheet)

Form PCT/ISA/220 (January 2004)

P a20

Schwegman, Lundberg
Woessner & Kluth, P.A.
APR 18 2005
CMG RECEIVED

RECEIVED
APR 11 2005
PORTFOLIO IP

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

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

(PCT Rule 44.1)

Applicant's or agent's file reference 2012.008WO1	Date of mailing *(day/month/year)* **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/38124	International filing date *(day/month/year)* 15 November 2004 (15.11.2004)
Applicant MARGENT DEVELOPMENT, LLC	

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

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

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

For more detailed instructions, see the notes on the accompanying sheet.

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

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

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer for Michelle L. Eason Gilberto Barron Telephone No. 571-272-3799

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PORTFOLIO I.P.
APR 11 2005
RECEIVED

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 2012.008WO1	**FOR FURTHER ACTION** see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US04/38124	International filing date (*day/month/year*) 15 November 2004 (15.11.2004)	(Earliest) Priority Date (*day/month/year*) 17 November 2003 (17.11.2003)
Applicant MARGENT DEVELOPMENT, LLC		

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

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

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
      ☐ The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**, D✓ 5/7/05
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 2
      ☐ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☒ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/38124

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d)).

NEW ABSTRACT

A Personal Digital Key Digital Content Security System (PDK-DCSS) is used to protect computers from unauthorized use and protect the digital content (110) stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are 1) a standard hard drive device (108), with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and 2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: 1) hard drive (108) access control for providing Drive-Level and Sector-Level protection and 2) operating system-level independent file protection for providing File-Level and Network-Level protection.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/38124

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30
US CL : 713/193
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/193

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,385,596 B1 (WISER et al) 07 May 2002, fig.1b block 106,120,130 and associated text; col.4, lines 3-13; col.3, lines 5-10; col.4, lines 12-27, 51-67; col.5, lines 11-17; fig.2 and 4,9b-13 and associated text; col.8, lines 46-56; col.18, lines 66-67; col.19, lines 1-25;col.6, lines 4-65.	1-4,7-12-14, 17-20
Y	PAGET, THE SECURITY BEHIND SECURE EXTRANETS,ENTERPRISE SYSTEM JOURNAL,14,12,74, December 1999. entire reference	1-4, 7-14 and 17-20
Y	US 6,632,992 B2 (HASEGAWA) 14 October 2003, col.3, lines 22-39.	3 and 13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
17 March 2005 (17.03.2005)

Date of mailing of the international search report
07 APR 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Gilberto Barron

Telephone No. 571-272-3799

Form PCT/ISA/210 (second sheet) (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	07 APR 2005
Applicant's or agent's file reference 2012.008WO1	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/38124	15 November 2004 (15.11.2004)	17 November 2003 (17.11.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): G06F 11/30 and US Cl.: 713/193

Applicant

MARGENT DEVELOPMENT, LLC

1. This opinion contains indications relating to the following items:

- [X] Box No. I — Basis of the opinion
- [ ] Box No. II — Priority
- [ ] Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV — Lack of unity of invention
- [X] Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI — Certain documents cited
- [ ] Box No. VII — Certain defects in the international application
- [ ] Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

06/07/05

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron for Michelle Rent Telephone No. 703-305-3900

Form PCT/ISA/237 (cover sheet) (January 2004)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International Application No.
PCT/US04/38124

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ in written format

☐ in computer readable form

c. time of filing/furnishing

☐ contained in international application as filed.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-20	YES
	Claims NONE	NO
Inventive step (IS)	Claims 5, 6, 15 and 16	YES
	Claims 1-4, 7-14 and 17-20	NO
Industrial applicability (IA)	Claims 1-20	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (January 2004)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1, 2, 4, 7-12, 14, 17-20 lacks an inventive step under PCT Article 33(3) as being obvious over Wiser et al (6, 385, 596 B1) in view of Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999).

As per claims 1, 2, 4, 7-12, 14 and 17-20 Wiser et al (6, 385, 596 B1) teach a method, system of securing a hard drive (see fig.1b, blocks 106, 120 and 130; col.4, lines 3-13) of a computer, comprising: detecting a key with a receiver/decoder circuit associated with the hard drive; validating the detected key with the receiver/decoder circuit; and permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected key is validated (see col.3, lines 5-10; col.4, lines 15-18 where the passport corresponds to Applicant's key; col.4, lines 12-27, 51-67; col.5, lines 11-17; col.8, lines 46-56 where decryption process is being done and where the decoding or decrypting circuit is inherent part of the system in order to do the decoding and decryption; Also see the entire reference for more detail);wherein the receiver/decoder circuit resides in the computer (see fig.9b-13 and associated text); wherein the validating step includes determining whether or not the detected key is associated with the hard drive (see fig.1b and associated text; col.3, lines 37-39; col.5, lines 11-17; col.18, lines 66-67 and col.19, lines 1-25); wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive in order to provide sector-level protection (see col.6, lines 4-65; fig.9b and associated text where the storing corresponds to applicant's write and retrieving media files corresponds to applicant's read); wherein the key associated with the hard drive is initially delivered with the hard drive (see fig.2-4 and associated text); wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer (see fig.1b; 2 and associated text); wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to perform the detecting, validating, and decrypting steps (see abstract; col.3-4); wherein the validating step includes determining whether or not the detected key is associated with the file (fig.1b, 2 and associated text; col.3-4). but do not explicitly disclose the key is a physical, portable key. However Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999) disclose the key is a physical portable key (see the entire reference pages with close attention to where the passport and digital certificate that contains the key are installed on a smart card on the second page where examiner considers such smart card as corresponding to Applicant's physical, portable key). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Paget's portable key such as the smart card in Wiser's secure access to on-line music files on the storage (hard disk) in order to extends extranet access and authority to users based on their roles and business privileges, while ensuring confidentiality and integrity of the data users send, receive and access.
Claims 3 and 13 lacks an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hasegawa (6,632,992 B2).

As per claims 3 and 13 Wiser et al (6, 385, 596 B1) in view of Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999) teach all limitation of the method, system of claims 1, 9, 17 and 22 as applied above but do not explicitly disclose wireless communication. However Hasegawa (6,632,992 B2) wireless communication (see col.3, lines 22-39). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hasegawa's wireless communication in Wiser's secure access to on-line music files on the storage (hard disk) in view of Paget's portable key such as the smart card in order to extends extranet access and authority to users based on their roles and business privileges, while ensuring confidentiality and integrity of the data users send, receive and access without the use of wires or cables.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Claims 5, 6, 15 and 16 meets the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest disabling of the storage or hard-disk in case of non validation of the physical key.

Form PCT/ISA/237 (Supplemental Box) (January 2004)

PATENT COOPERATION TREATY

RECEIVED
FEB 26 2007
FENWICK & WEST

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

11163/PCT

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)
Applicant PROXENSE, LLC	

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

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

   When The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. (571) 272-3600

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

M

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 22 FEB 2007
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. (571) 272-3600

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)	(Earliest) Priority Date (*day/month/year*) 01 December 2004 (01.12.2004)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 7 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/43447

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06Q 99/00**(2006.01);**H04K 1/00**(2006.01);**H04L 9/00**(2006.01)

USPC: 705/59
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0109580 A1 (SHREVE ET AL.) 15 AUGUST 2002 (15.08.2002) PARAGRAPKS 0001 TO 0007.	1-55
X	US 2002/0073042 A1 (MARIITZEN ET AL.) 13 JUNE 2002 (13.06.2002) PARAGRAPHS 0001-0005.	1-55
X	US 5,991,749 A (MORRILL, JR) 23 NOVEMBER 1999 (23.11.1999), COLUMN 1 LINE 5-58.	1-55

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 November 2006 (14.11.2006)

Date of mailing of the international search report
22 FEB 2007

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
James Trammel

Telephone No. (571) 272-3600

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

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	22 FEB 2007
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US05/43447	30 November 2005 (30.11.2005)	01 December 2004 (01.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **G06Q 99/00**(2006.01);**H04 K 1/00;H04 L 9/ 00**

USPC: 705/59

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	15 November 2006 (15.11.2006)	James Tramme Telephone No. (571) 272-3600

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/43447

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/43447

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-55	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-55	NO
Industrial applicability (IA)	Claims 1-55	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Morrill, Jr (US 5,991,749 A). Morrill, in at least column 1, lines 25-58 discloses a system for collecting funds by passing within a proximity of a wireless computing and transactional device.

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Maritzen et al. (US 2002/0073042 A1). Maritzen, in at least paragraphs 0001-0006, discloses conducting e-commerce transactions across wireless devices.

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Shreve et al. (US 2002/0109580 A1). Shreve, in at least paragraphs 0001-0007 discloses remote keyless entry devices for granting access to secure domains.

RECEIVED
MAR 15 2007
FENWICK & WEST

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)	(Earliest) Priority Date (*day/month/year*) 20 December 2004 (20.12.2004)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 2 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/46843

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/32**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,041,410 (HSU et al), 21 March 2000, Column 4, lines 15-56, Column 5, line 1 to Column 6, line 24, and Column 6, line 42 to Column 7, line 34	1, 4-11, 15, 18 --- 2, 3, 12-14, 16, 17, 19-21
Y	US 2004/0129787 (SAITO et al) 8 July 2004, Paragraphs 40-56, 81-91, 91-101, and 164	2, 3, 12-14, 16, 17, 19-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2007 (18.01.2007)	01 MAR 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

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

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

	Date of mailing (*day/month/year*) 01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US05/46843	20 December 2005 (20.12.2005)	20 December 2004 (20.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/32**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	18 January 2007 (18.01.2007)	Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 2, 3, 12-14, 16, 17, and 19-21	YES
	Claims 1, 4-11, 15, and 18	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-21	NO
Industrial applicability (IA)	Claims 1-21	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:
Claims 1, 4-11, 15, and 18 lack novelty under PCT Article 33(2) as being anticipated by Hsu (US 6041410 A) 21 March 2000.

Regarding Claim 1,
Hsu discloses a method for verifying a user during authentication of an integrated device, comprising the steps of:
Persistently storing biometric data for the user in a tamper-resistant format (Column 4, lines 15-25);
Responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (Column 4, lines 26-56);
Comparing the scan data to the biometric data to determine whether the data match (Column 4, lines 26-56); and
Wirelessly sending a code for authentication (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9).

Regarding Claim 10,
Claim 10 is a device claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 4,
Hsu discloses that the code uniquely identifies the integrated device (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 5,
Hsu discloses that the code indicates that the biometric verification was successful (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 6,
Hsu discloses that persistently storing biometric data comprises permanently storing biometric data (Column 4, lines 15-25; and Column 5, lines 1-47).

Regarding Claim 11,
Claim 11 is a device claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 7,
Hsu discloses that the biometric data and the scan data are both based on a fingerprint scan by the user (Column 4, lines 15-56).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

Regarding Claim 8,
Hsu discloses establishing a secure communication channel prior to sending the code for authentication (Column 6, line 42 to Column 7, line 34).

Regarding Claim 9,
Hsu discloses receiving a request for the code without a request for biometric verification (Column 5, line 57 to Column 6, line 24); and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data (Column 5, line 57 to Column 6, line 24).

Regarding Claim 15,
Hsu discloses a method for authenticating a verified user, comprising:
Receiving a code associated with a biometrically verified user (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Requesting authentication of the code (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Receiving an authentication result (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34); and
In response to the authentication result being positive, providing access to an application (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 18,
Hsu discloses establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key (Column 6, line 42 to Column 7, line 34).

Claims 2, 3, 12-14, 16, 17, and 19-21 lack an inventive step under PCT Article 33(3) as being obvious over Hsu in view of Saito (US 20040129787 A1) 8 July 2004.

Regarding Claim 2,
Hsu does not disclose that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.
Saito, however, discloses that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 12,
Claim 12 is a device claim that corresponds to method claim 2 and is rejected for the same reasons.

Regarding Claim 3,
Hsu does not disclose registering an age verification for the user in association with the code.
Saito, however, discloses registering an age verification for the user in association with the code (Paragraphs 82, 83, and 164). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 13,
Claim 13 is a device claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 14,
Hsu does not disclose that the verification module comprises an LED to be activated for requesting the biometric scan.
Saito, however, discloses that the verification module comprises an LED to be activated for requesting the biometric scan (Paragraphs 40-56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 16,
Hsu does not disclose registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority.

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Saito, however, discloses registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 17,
Hsu as modified by Saito does discloses the method of claim 16, in addition, Saito discloses registering a date of birth or age with the trusted authority (Paragraphs 82, 83, and 164).

Regarding Claim 19,
Hsu discloses a system comprising:
A biometric key to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code (Column 4, lines 15-56; and Column 5, line 1 to Column 6, line 9);
An authentication module to authenticate the user for access to an application (Column 7, lines 17-34);
But does not disclose sending the code to a trusted authority for authentication.
Saito, however, discloses an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 20,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9); and Saito discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Paragraphs 40-56; and 81-91

Regarding Claim 21,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that if the biometric key cannot verify the scan data as being from the user, it does not send the code (Column 5, lines 1-47).

RECEIVED
PATENT DOCKETING

OCT 06 2008

Fenwick & West

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 03 OCT 2008
Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11102	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

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

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

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

For more detailed instructions, see the notes on the accompanying sheet.

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

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

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Gilberto Barron Telephone No. (571) 272-1018

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US07/11102	International filing date *(day/month/year)* 07 May 2007 (07.05.2007)	(Earliest) Priority Date *(day/month/year)* 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 2 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☒ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. ____
   ☐ as suggested by the applicant. ☒ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.

Form PCT/ISA/210 (first sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11102

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/00**(2006.01),**1/00**(2006.01)

USPC: 713/168;713/170;713/182

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/168;713/170;713/182

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	U.S. 2003/0127511 A1 (KELLY et al.) 10 July 2003 (10.07.2003), paragraph 0037.	1-31
Y	U.S. 2006/0022046 A1 (IWAMURA) 02 February 2006 (2.02.2006), paragraph 0013.	1-10,12,14-31
Y	U.S. 5,416,780 A (PATEL) 16 May 1995(16.05.1995), column 7 lines 39-68.	11
Y	U.S. 2003/0139190 A1 (STEELBERG et al.) 24 July 2003 (24.07.2003), abstract and paragraph 0053.	13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 2008 (11.06.2008)	03 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner of Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Gilberto Barron Telephone No. (571)270-1018

Form PCT/ISA/210 (second sheet) (July 1998)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	03 OCT 2008
Applicant's or agent's file reference 12785 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/11102	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01),**1/00**(2006.01)
USPC: 713/168;713/170;713/182

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	01 October 2008 (01.10.2008)	Gilberto Barron Telephone No. (571)270-1018

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11102

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11102

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-31	YES
	Claims NONE	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-31	NO
Industrial applicability (IA)	Claims 1-31	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:

Claims 1-10, 12, and 14-31 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046). With respect to claim 1, a method for differentiating between a first personal digital key (PDK) and a second PDK within a proximity zone of an external device, comprising:

obtaining a first differentiation metric (see Kelly column 7 lines 32-59 i.e. set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410) associated with the first PDK (see Kelly column 7 lines 32-33 i.e. smart card) after it enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader);

obtaining a second differentiation metric associated with the second PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 the next user that comes and gets his smartcard scanned);

responsive to the first PDK being most likely associated with the transaction, executing an authentication test for the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example); and

authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics. Iwamura teaches that with the increase popularity in wireless smartcards devices will is more and more likely that multiple smart cards will be in communication range of a terminal. Iwamura teaches that when many smart cards exist in the communication range a specific carrier is selected by a shock absorbing mechanism so that the process can be correctly performed i.e. determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics (see paragraph 0013). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have modified Kelly with a system that allows many smartcards in communication range while still making sure the process is carried out correctly. Therefore one would have been motivated to have selected the smartcard based on first and second differentiation metrics of the smartcards

With respect to claim 2, further comprising receiving an input to initiate an authentication of an individual (see Kelly column 7

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 3, further comprising: receiving a first profile sample from the first PDK, wherein the profile sample comprises a subset of information from a first profile in the first PDK computed according to a first function (see Kelly figure 6 and column 7 lines 32-59 i.e. the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); computing an input sample from the received input according to the first function (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and responsive to the first profile sample not matching the input sample, indicating that the first PDK does not satisfy the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 4, further comprising: receiving a second profile sample from the first PDK (see Kelly column 7 lines 32-59 (see column 7 lines 32-33 the next user that comes and gets his smartcard scanned): comparing the second profile sample to the input sample (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 5, wherein the first profile sample is received at a predetermined period of time after the first PDK enters the proximity zone (see Kelly column 7 lines 32-33 right after the card is inserted into the reader).

With respect to claim 6, Kelly teaches wherein the input is a biometric input and wherein executing the authentication test further comprises: receiving a biometric profile from the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received biometric profile to the biometric input (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24); and responsive to the biometric profile matching the biometric input, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach wirelessly receiving data from the first PDK. Iwamura teaches wirelessly receiving data from the smart card. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have been able a use wireless smartcards to communicate with a device to increase the flexible of smart card. Therefore one would have been motivated to have used wireless smart cards (see Iwamura paragraph 0017).

With respect to claim 7, wherein the input is a personal identification number (PIN) and wherein executing the authentication test further comprises: wirelessly receiving a PIN profile from the first PDK (see column 8 lines 8-17); comparing the received PIN profile to the PIN input (see column 8 lines 8-17); and responsive to the PIN profile matching the PIN input, indicating that the authentication test is satisfied (see Kelly column 8 lines 8-17).

With respect to claim 8, wherein executing the authentication test further comprises: wirelessly receiving a picture profile from the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received picture profile to the individual (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24); and responsive to the picture profile matching the appearance of the individual, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 9, further comprising: responsive to the authentication test not being satisfied, determining whether the second PDK is next most likely to be associated with the individual based on the differentiation metrics; executing the authentication test for the second PDK; and authorizing the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 10, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

With respect to claim 12, wherein the detection duration metric includes a length of time the first PDK is within the proximity zone of the external device (see Kelly column 7 lines 32-33).

With respect to claim 14, an apparatus for differentiating between a first personal digital key (PDK) and a second PDK within a proximity zone, comprising:

a receiver/decoder circuit adapted to obtain a first differentiation metric associated with the first PDK when the first PDK enters the proximity zone and obtain a second differentiation metric associated with the second PDK when the second PDK enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader); and

a processor coupled to the receiver decoder circuit, the processor for determining whether the first PDK is most likely to be associated with a transaction based on the differentiation metrics, executing an authentication test for the first PDK responsive to determining that the first PDK is most likely associated with the transaction, and authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 15, further comprising a memory coupled to the receiver/decoder circuit, the memory adapted to buffer the first and second differentiation metrics (see Kelly column 3 lines 37-52).

With respect to claim 16, further comprising an input device adapted to receive an input from an individual to initiate the transaction (see Kelly column 7 lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 17. The apparatus of claim 16, wherein the input device comprises at least one of a keypad, a touch screen, a biometric reader and a pointing device (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 18. The apparatus of claim 17, wherein the biometric reader is further adapted to obtain a representation of physical or behavioral characteristics derived from the individual (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 19. The apparatus of claim 17, wherein the biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer and a voice analyzer (see Kelly column 7 lines 32-59 i.e. one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 20, wherein the receiver/decoder circuit is further adapted to wirelessly receive a profile sample from the first PDK, wherein the profile sample comprises a subset of information computed by applying a first function to a profile of the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 21, wherein the processor is further configured to compute an input sample by applying the first function to the received input, and determine if the input sample matches the buffered profile sample associated with the first PDK (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 22, wherein the receiver/decoder circuit automatically receives the profile sample at a fixed period of time after the first PDK enters the proximity zone (see Kelly column 7 lines 32-33 right after the card is inserted into the reader).

With respect to claim 23, wherein the processor is further adapted to determine whether the second PDK is next most likely to be associated with the individual based on the differentiation metrics responsive to the authentication test not being satisfied, execute the authentication test for the second PDK, and authorize the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

With respect to claim 24, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

With respect to claim 25, further comprising a screen coupled to the receiver/decoder circuit, the screen adapted to display an image received from the PDK (see Kelly figure 10).

With respect to claim 26, a computer readable storage medium for differentiating between a plurality of personal digital keys (PDKs) within a proximity zone of an external device, structured to store instructions executable by a processing system, the instructions when executed cause the processing system to:

obtaining a first differentiation metric associated with the first PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 i.e. a user may be required to input his/her smart card into smart card reader);

obtaining a second differentiation metric associated with the second PDK after it enters the proximity zone (see Kelly column 7 lines 32-33 the next user that comes and gets his smartcard scanned);

responsive to the first PDK being most likely associated with the transaction, executing an authentication test for the first PDK (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example); and

authorizing the transaction responsive to the first PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

Kelly does not teach determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics. Iwamura teaches that with the increase popularity in wireless smartcards devices will is more and more likely that multiple smart card will be in communication range of a terminal. Iwamura teaches that when many smart cards exist in the communication range a specific carrier is selected by a shock absorbing mechanism so that the process can be correctly performed i.e. determining whether the first PDK is most likely to be associated with a transaction based on the first and second differentiation metrics (see paragraph 0013). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have modified Kelly with a system that allows many smartcards in communication range while still making sure the process is carried out correctly. Therefore one would have been motivated to have selected the smartcard based on first and second differentiation metrics of the smartcards

With respect to claim 27, the instruction when executed further causing the processing system to receive an input to initiate an authentication of an individual (see Kelly column 7 lines 32-59 i.e. a user may be required to input his/her smart card into smart card reader/writer 26 as well as have one or more of the user's immutable characteristics (fingerprint, image, etc.) recorded).

With respect to claim 28, the instructions when executed further causing the processing system to: receiving a first profile sample from the first PDK, wherein the profile sample comprises a subset of information from a first profile in the first PDK computed according to a first function (see Kelly figure 6 and column 7 lines 32-59 i.e. the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); computing an input sample from the received input according to the first function (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and responsive to the first profile sample not matching the input sample, indicating that the first PDK does not satisfy the authentication test (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 29, wherein the input is a biometric input and wherein the instructions when executed further cause the processing system to: wirelessly receiving a biometric profile from the first PDK (see column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410); comparing the received biometric profile to the biometric input (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices ~~22~~ and 24); and responsive to the biometric profile matching the biometric input, indicating that the authentication test is satisfied (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 30, the instructions when executed further causing the processing system to: responsive to the authentication test not being satisfied, determine whether the second PDK is next most likely to be associated with the individual based

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

on the differentiation metrics; execute the authentication test for the second PDK; and authorize the transaction responsive to the second PDK satisfying the authentication test (see Kelly column 7 lines 32-59 i.e. compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410); and determining if the second profile sample matches the input sample (see Kelly column 7 lines 32-59 i.e. Data read from frequent flyer smart card 400 or a smart card boarding pass 410 is then passed to processor 12 and a comparison performed. Processor 12 may, for example, compare the set of data obtained from frequent flyer smart card 400 or a smart card boarding pass 410 with the information obtained from one or more of the biometric/image capture devices 22 and 24. The result of this comparison is the decision whether the traveler is physically the same individual as that described on frequent flyer smart card 400 or smart card boarding pass 410. If the comparison is positive, processor 12 indicates this to an access control interface (not shown), which then would open a door or a gate, for example).

With respect to claim 31, wherein the first differentiation metric is based on at least one of a distance metric, a detection duration metric, and a location metric (see Kelly column 7 lines 32-33).

Claims 11 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046) in further view of Patel (U.S. 5,416,780). Kelly nor Iwamura teach with respect to claim 11, wherein the distance metric is determined based on at least one of bit error rate, packet error rate, signal strength. Patel teaches wherein the distance metric is determined based on at least one of bit error rate, packet error rate, signal strength (see column 7 lines 39-68). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have chosen the base station based on the best signal strength between the smartcard and the reader to increase the chance that the message gets sent correctly (see column 7 lines 39-68). Therefore one would have been motivated to have the smartcard with the best signal strength.

Claims 13 lack an inventive step under PCT Article 33(3) as being obvious over Kelly et al (U.S. 7,090,126) in view of Iwamura (U.S. 2006/0022046) in further view of Steelberg et al (U.S. 2003/0139190).

Kelly nor Iwamura teach with respect to claim 13, wherein the location metric is determined using coordinate triangulation. Steelberg teaches the uses triangulation to help set secure radio frequency communication between smartcard and other device (see abstract and paragraph 0053). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used triangulation to help set secure radio frequency communication between smartcard and other device. Therefore one would have been motivated to have used triangulation to help set secure radio frequency communication between smartcard and other device (see abstract and paragraph 0053).

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

Fenwick & West LLP
APR 25 2008
RECEIVED

PCT

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

(PCT Rule 44.1)

Applicant's or agent's file reference 12786 PCT	Date of mailing (*day/month/year*) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

25000

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

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

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

For more detailed instructions, see the notes on the accompanying sheet.

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

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

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 23 APR 2008
Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 2 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11103

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPAT, US-PGPUB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0104006 A1 (Boate et al.) 01 August 2002 (01.08.2002), [0011], [0012], [0014], [0027], [0035], [0043].	1-20
A,E	US 7,249,177 B1 (MILLER) 24 July 2007	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 April 2008 (08.04.2008)

Date of mailing of the international search report
23 APR 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
SUMAN DEBNATH
DEBORAH A. THOMAS
PARALEGAL SPECIALIST
Telephone No. 571 270 9922

Form PCT/ISA/210 (second sheet) (April 2007)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	23 APR 2008
Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US07/11103	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04K 1/00**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	08 April 2008 (08.04.2008)	SUMAN DEBNATH Telephone No. 571 270 9922

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11103

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11103

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-20	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-20	NO
Industrial applicability (IA)	Claims 1-20	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:

Claims 1-20 lack novelty under PCT Article 32(2) as being anticipated by Boate et al. (Pub. No.: US 2002/0104006 A1), hereinafter "Boate".

As to claim 1, Boate discloses a method for electronic transaction processing comprising: wirelessly receiving data from a personal digital key (PDK) ([0011], [0012]); receiving a biometric input ([0012], [0027]); authenticating the personal digital key ([0012], [0035]); authenticating the biometric input ([0012], [0043]); and performing a transaction responsive to the personal digital key and the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 2, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis ([0027], lines 1-11).

As to claim 3, Boate discloses wherein wirelessly receiving data from a personal digital key includes receiving biometric data ([0012]), and authenticating the biometric input includes comparing the biometric data to the biometric input for match ([0012], [0043]).

As to claim 4, Boate discloses wherein the biometric data is a portion or subset of an entire biometric data set for an attribute ([0027]).

As to claim 5, Boate discloses wherein wirelessly receiving data from a personal digital key includes establishing a secure communication channel between the PDK and a reader, and wherein a profile is sent from the PDK to the reader ([0012], [0035]).

As to claim 6, Boate discloses wherein the profile includes a PDK identification number and one from the group of financial information, credit card information and personal identification information ([0027]).

As to claim 7, Boate discloses wherein authenticating the personal digital key begins before authenticating the biometric input ([0012], [0027]).

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

As to claim 8, Boate discloses wherein authenticating the biometric input begins before authenticating the personal digital key ([0012], [0027]).

As to claim 9, Boate discloses wherein authenticating the personal digital key includes receiving data from the personal digital key and comparing it against an external system ([0027]).

As to claim 10, Boate discloses wherein the external system is one from the group of a central registry, a validation database and a private registry ([0014]).

As to claim 11 Boate discloses further comprising authenticating a reader ([0012]).

As to claim 12, Boate discloses wherein wirelessly receiving, receiving the biometric input, authenticating the personal digital key, authenticating the biometric input are performed by a reader device ([0012]).

As to claim 13, Boate discloses wherein receiving the biometric input and authenticating the biometric input are performed by the personal digital key ([0012], [0027]).

As to claim 14, Boate discloses wherein receiving authenticating the biometric input is performed by the personal digital key and the reader ([0012], [0027], [0035]).

As to claim 15, Boate discloses wherein performing a transaction comprises: initiating the transaction; communicating with another system to authorize and approve the transaction; and presenting the status for the transaction ([0012], [0027], [0035]).

As to claim 16, Boate discloses a method for electronic transaction authentication comprising: wirelessly receiving data from a reader ([0011], [0012]); receiving a biometric input ([0012], [0027]); authenticating the reader authenticating the biometric input ([0012], [0043]); and transmitting a signal authorizing a transaction responsive to the reader and the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 17, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a NA analysis, a signature analysis, and a voice analysis ([0027], lines 1-11).

As to claim 18, Boate discloses wherein receiving the biometric input comprises obtaining a representation of physical or behavioral characteristics derived from the individual ([0027]).

As to claim 19, Boate discloses a method for electronic transaction processing comprising: wirelessly receiving a biometric reference from a personal digital key ([0012], [0027], [0043]); receiving a biometric input ([0012], [0027]); authenticating the biometric input ([0012], [0043]); and performing a transaction responsive to the biometric input being authenticated ([0012], [0027], [0035]).

As to claim 20, Boate discloses wherein receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis ([0027]).

PATENT COOPERATION TREATY

Fenwick & West LLP

JUN 30 200

RECEIVED

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 26 JUN 2008
25000 Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11104	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer /Tongoc Tran/ Telephone No. 571-272-3843

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11104	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

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

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

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 8
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/11104

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A personal digital key (PDK) 802 is programmed using a trusted programming device to initialize and/or register the PDK 802 for use. In one embodiment, the initialization and registration processes are administered by a specialized trusted Notary to ensure the processes follow defined security procedures. In a biometric initialization, the programming device acquires a biometric input 804 from a user and writes the biometric data to a tamperproof memory in the PDK 802. In registration, the programmer 810 communicates to one or more remote registers to create or update entries associated with the user PDK 802. Once initialized and registered, the PDK 802 can be used for various levels of secure authentication processes.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11104

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/0079133 A1 (BREITER et al.) 24 April 2003 (24.04.2003), Fig. 4 and 5, paragraphs [0082]-[0083].	1-24
Y	US 2002/0191816 A1 (MARITZEN et al.), 19 December 2002 (19.12.2002), paragraph 0056.	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2008 (10.05.2008)	26 JUN 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer /Tongoc Tran/ Telephone No. (571) 272-3843

Form PCT/ISA/210 (second sheet) (April 2007)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	26 JUN 2008
Applicant's or agent's file reference 12784 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/11104	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	10 May 2008 (10.05.2008)	/Tongoc Tran/ Telephone No. 571-272-3843

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-24	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-24	NO
Industrial applicability (IA)	Claims 1-24	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

V. 2. Citations and Explanations:

Claims 1-24 lack an inventive step under PCT Article 33(3) as being obvious over Breiter et al. (U.S> Patent Application Publication No. 2003/0079133, hereinafter Breiter) in view of Maritzen et al. (U.S. Patent Application Publication No. 2002/0191816, hereinafter Marizen).

With respect to claims 1 and 16, Breiter discloses a method and an apparatus of using a programmer to initialize a personal digital key (PDK) for use in secure authentication (e.g. rights wallet, Fig. 4, 5, 7), comprising:

reading user information from a user PDK to determine if the user is authorized for initialization (e.g. paragraph]0082], user PDK- rights wallets);

reading notary information from a notary PDK to determine if the notary is authorized to administer the initialization (e.g. [0082]-0083], certificate authority).

acquiring a credential from the user, wherein the acquisition is witnessed by the notary ; and responsive to the user and notary being authorized (e.g. paragraph, [0082]),

Breiter does not explicitly disclose but the credential information is biometric information and storing a biometric profile based on the acquired biometric input to the user's PDK (e.g. Maritzen, paragraph, [0056]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the acquiring rights wallet taught by Breiter with acquiring biometrics information and storing as user profile taught by Martizen to ensure secure authentication of user in order to prevent unauthorized access to secure information.

With respect to claims 2 and 17. Breiter amd Maritzen disclose the method and apparatus of claims 1 and 16, wherein determining if the user is authorized for initialization comprises:

detecting the user PDK(e.g. paragraph, [0082]);

checking a status of the user PDK in a registry; and responsive to the status being in good standing, determining that the user is authorized for initialization (e.g. Breiter, paragraph, [0082]).

With respect to claims 3 and 18. Breoter and Maritzen disclose the method and apparatus of claims 2 and 17, wherein the user PDK is in good standing if the user PDK has not been reported as lost, stolen, expired, or revoked (e.g. Breiter, paragraph, [0082]).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11104

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

With respect to claims 4 and 19, Breiter and Maritzen disclose the method and apparatus of claims 2 and 17, wherein the user PDK is in good standing if the user PDK has never been initialized (e.g. Breiter, paragraph, [0082]).

With respect to claims 5 and 20, Breiter and Maritzen disclose the method and apparatus of claims 1 and 17, wherein acquiring the biometric input comprises:
scanning the biometric input from a user associated with the user PDK; and performing a transformation on the biometric input to generate the biometric profile (e.g. Marizen, paragraph, [0056]).

With respect to claims 6 and 21, Breiter and Maritzen disclose the method and apparatus of claims 5 and 16, Breiter and Marizen disclose further comprising:
checking the quality of the scanned biometric input; and responsive to the quality not being satisfactory, re-scanning the biometric input (e.g.. Marizen, paragraph, 0056]).

With respect to claims 7 and 22, Breiter and Maritzen disclose the method and apparatus of claims 1 and 16, further comprising
storing initialization history data to the programmer, wherein initialization history data comprises at least one of a user PDK ID, a notary ID, a programmer ID, and a site ID (e.g. Breiter, paragraph, [0069], [0082]).

With respect to claim 8, Breiter and Maritzen disclose the method of claim 1, further comprising writing initialization history data to the user PDK, wherein initialization history data comprises at least one of a user PDK ID, a notary ID, a programmer ID, and a site ID (e.g. Breiter, paragraph, [0082]).

With respect to claim 9, Breiter and Maritzen disclose the method of claim 1, further comprising:
receiving a hardware authentication request from the user PDK; transmitting programmer information to the user PDK; and responsive to the user PDK determining that the programmer is a valid device, receiving authorization from the user PDK to continue initialization (e.g. Breiter, paragraph, [0082]).

With respect to claim 10, Breiter and Maritzen disclose he method of claim 1, wherein determining if the notary is authorized to administer initialization comprises: detecting the notary PDK; checking a status of the notary PDK in a registry; and responsive to the status being in good standing, determining that the notary is authorized to use the programmer for initialization of the user PDK (e.g. Breiter, paragraph, [0082]-[0083]).

With respect to claim 11, Breiter and Maritzen disclose the method of claim 10, wherein the notary PDK is in good standing if the notary PDK has not been reported as lost, stolen, expired, or revoked (e.g. Breiter, paragraph [0082]-[0083]).

With respect to claim 12, Breiter and Maritzen disclose the method of claim 1, further comprising determining if the programmer is in good standing (e.g. Breiter, paragraph, [0082], [0083]).

With respect to claim 13, Breiter and Maritzen disclose the method of claim 12, wherein the programmer is in good standing if the programmer has not been reported as lost, stolen, expired, or revoked and the programmer does not comprise altered software (e.g. Breiter, paragraph, [0082]-[0083]).

With respect to claim 14, Breiter and Maritzen disclose the method of claim 1, wherein the notary administers the initialization process from a remote location (e.g. Breiter, paragraph, [0082]).

With respect to claim 15, Breiter and Maritzen disclose the method of claim 1, further comprising transmitting registry information to a remote registry to add or update a registry entry, wherein the registry information comprises at least one of a user PDK ID, purchasing information, and personal information (e.g. Breither, paragraph, [0082]).

With respect to claim 23, Breiter and Maritzen disclose the apparatus of claim 16, wherein the biometric reader is adapted to obtain a representation of physical or behavioral characteristics derived from the individual (e.g. Maritzen, paragraph, [0056]).

With respect to claim 24, Breiter and Maritzen disclose the apparatus of claim 16, wherein the biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer, and a voice analyzer (e.g. Maritzen, paragraph, [0056]).

Claims 1-24 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

RECEIVED
PATENT DOCKETING

OCT 23 2008

Fenwick & West

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 20 OCT 2008
Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11105	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

25000 -

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450	Hosuk Song
Facsimile No. (571) 273-3201	Telephone No. 5712722100

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11105	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 4 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US07/11105

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A Personal Digital Key stores one or more profiles(e.g., a biometric profile) in a tamper-proof memory that is acquired in a secure trusted process. Biometric profiles comprise a representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK(102). The PDK wirelessly transmits the biometric profile over a secure wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric profile to a biometric input(104) acquired at the point of transaction in order to determine if the transactionshould be authorized.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01);**H04L 9/32**(2006.01)

USPC: 713/182,186;726/2;380/270
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182,186; 726/2;380/270

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 7,249,177 B(MILLER) 24 July 2007 (24.07.2007), column 3 lines 28-42; column 4,lines 19-25; column 5,lines 1-17	1-42
A	US 6,070,796 A(SIRBU) 06 June 2000 (06.06.2000), column 7,lines 7-40; column 9,lines 25-55.	1-42
X	US 6,850,147 B(PROKOSKI et al) 01 February 2005 (01.02.2005), column 4,lines 39-62; column 6,lines 46-67; column 11,lines 1-22.	1-42

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2008 (30.09.2008)	20 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Hosuk Song Telephone No. 5712722100

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

Continuation of B. FIELDS SEARCHED Item 3:
EAST, foreign patent databse
search terms: biometric, fingerprint,iris,key, password, wireless, authentication, authorization,access,control,tamper-proof,memory,storage.

Form PCT/ISA/210 (extra sheet) (April 2007)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	20 OCT 2008
Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/11105	07 May 2007 (07.05.2007)	05 May 2006 (05.05.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04K 1/00**(2006.01);**H04L 9/32**(2006.01)
USPC: 713/182,186;726/2;380/270

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	29 September 2008 (29.09.2008)	Hosuk Song Telephone No. 5712722100

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Form PCT/ISA/237(Box No. I) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-42	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-42	NO
Industrial applicability (IA)	Claims 1-42	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient**.

V. 2. Citations and Explanations:
Claims 1-42 lack novelty under PCT Article 33(2) as being anticipated by Prokoski et al(US 6,850,147).
Claim 1: Prokoski disclose wirelessly receiving a biometric profile from a personal digital key (PDK), wherein the biometric profile is uniquely associated with an individual in (col.5,lines 30-56). Prokoski disclose receiving a biometric input; comparing the biometric profile to the biometric input and authorizing a transaction responsive to the biometric profile matching the biometric input in (col.7,lines 35-59).
Claim 2: Prokoski disclose obtaining a representation of physical or behavioral characteristics derived from the individual in (fig.1).
Claim 3: Prokoski disclose receiving the biometric input comprises performing at least one of a fingerprint scan, a retinal scan, an iris scan, a facial scan, a palm scan, a DNA analysis, a signature analysis, and a voice analysis in (fig.6).
Claim 4: Prokoski disclose performing a device authentication to verify that the PDK is a valid device responsive to the PDK entering a proximity zone in (fig.4).
Claim 5: Prokoski disclose performing a challenge-response authentication to verify the PDK is valid wherein the PDK further verifies validity of an external device in (fig.6).
Claim 6: Prokoski disclose receiving available profile types from the PDK and comparing the available profile types to required profile types of authentication in (col.10,lines 15-29). Prokoski disclose responsive to the available profile types being sufficient indicating that the PDK is valid and responsive to the available profile types not being sufficient indicating that the PDK is not valid in (fig.4).
Claim 7: Prokoski disclose establishing a secure communication channel with a remote registry in (col.10,lines 30-41). Prokoski disclose transmitting PDK information to the remote registry wherein the PDK information is uniquely associated with the PDK receiving validity information from the remote registry and determining if a transaction should be authorized based on the validity information and the comparison between the biometric profile and biometric input in(fig.6).
Claim 8:Prokoski disclose remote registry is a Central Registry comprising a secured centrally-located database administered by a trusted third-party organization in (fig.4).
Claim 9: Prokoski disclose remote registry is a private registry comprising a database administered by a private controlling entity in (fig.5).
Claim 10: Prokoski disclose receiving purchasing information from the PDK, the purchasing information comprising at least one of bank information, credit card information,debit card information, ATM card information and coupon information in (col.2,lines 35-64).
Claim 11: Prokoski disclose determining if the purchasing information is valid by querying a remote validation database in (fig.6).
Claim 12: Prokoski disclose receiving a picture from the PDK comprising an image of the individual;displaying the image on a screen and prompting an administrator to confirm or deny the identity of the individual based on the appearance of the individual and the displayed image in (col.11,lines 1-22).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/11105

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Claim 13: Prokoski disclose acquiring a personal identification number from the individual;receiving a PIN profile from the PDK and determining if the acquired personal identification number matches the received PIN profile in (fig.4).
Claim 14: Prokoski disclose computing a representation of the biometric input based on a mathematical hash of the biometric input and comparing the representation of the biometric input to the biometric profile in (fig.3).
Claim 15: Prokoski disclose a receiver/decoder circuit adapted to wirelessly receive a biometric profile from a personal digital key(PDK) wherein the biometric profile is uniquely associated with an individual in (fig.3). Prokoski disclose a biometric reader adapted to receive a biometric input and a processor coupled to the receiver/decoder circuit and the biometric reader the processor adapted to compare the biometric profile to the biometric input and indicate that a transaction should be authorized responsive to the biometric profile matching the biometric input in (fig.4).
Claim 16: Prokoski disclose a establishing a secure communication channel with a remote registry; transmit PDK information to the remote registry wherein the PDK information is uniquely associated with the PDK and receive validity information from the remote registry in (fig.6).
Claim 17: Prokoski disclose a credit card terminal input/output coupled to the receiver/decoder circuit, the credit card terminal input/output adapted to communicate with a credit card terminal in (col.2,lines 50-64).
Claim 18: Prokoski disclose biometric reader is further adapted to obtain a representation of physical or behavioral characteristics derived from the individual in (col.11,lines 7-13).
Claim 19: Prokoski disclose biometric reader comprises at least one of a fingerprint scanner, a retinal scanner, an iris scanner, a face scanner, a palm scanner, a DNA analyzer, a signature analyzer, and a voice analyzer in (col.6,lines 54-65).
Claim 20: Prokoski disclose receiver/decoder circuit is further adapted to receive the biometric profile in an encrypted format over a secure wireless channel, and decrypt the biometric profile to an unencrypted format in (fig.5).
Claim 21: Prokoski disclose receiver/decoder circuit is adapted to detect a PDK in response to the PDK entering a proximity zone of the receiver/decoder circuit and request the PDK to transmit the biometric profile in (fig.4).
Claims 22,26-28: Prokoski disclose a memory adapted to store a biometric profile in a tamper-proof format, wherein the biometric profile is uniquely associated with an individual and a transceiver coupled to the memory, the transceiver adapted to wirelessly receive a request from an external device to transmit the biometric profile to the extenal device and wirelessly transmit the biometric profile over a secure wireless channel to the extenal device in (fig.1).
Claim 23: Prokoski disclose memory further stores initialization information comprising at least one of a programmer ID, a notary ID, and a site ID associated with an initialization process in(fig.2).
Claim 24: Prokoski disclose memory is further adapted to store at least one of purchasing information, registration information and personal information in (col.11,lines 50-62).
Claim 25: Prokoski disclose a programmer interface adapted to write the biometric profile to the memory during a trusted initialization process in(fig.3).
Claim 29,32-37: Prokoski disclose storing a biometric profile in a tamper-proof memory, wherein the biometric profile is uniquely associated with an individual and wirelessly receiving a request from an external device to transmit the biometric profile to the external device in (fig.1). Prokoski disclose responsive to receiving the request wirelessly transmitting the biometric profile over a secure wireless channel to the external device wherein the external device authenticates an individual for a transaction based on a comparison between the biometric profile and a biometric input acquired from the individual in (fig.3).
Claim 30: Prokoski disclose encrypting the stored biometric profile for transmission over the secure wireless channel in (fig.2).
Claim 31: Prokoski disclose storing at least one of purchasing information, registration information and personal information in (fig.6).
Claim 38: Prokoski disclose wirelessly receiving uniquely identifying information from a personal digital key(PDK) and analyzing the uniquely identifying information to determine if the PDK is valid in (col.3,lines 28-42,57-63). Miller disclose receiving profile information from the PDK indicating types of profiles stored in the PDK and determining if the types of profiles are compatible with allowable authentication types in (col.5,lines 45-57). Prokoski disclose performing one or more authentication tests to determine if a profile is valid and authorizing a transaction responsive to determining that the PDK is valid, determining that the types of profiles are compatible and determining that the profile is valid in (col.10,lines 15-29).
Claim 39: Prokoski disclose wirelessly receiving a biometric profile from the PDK, wherein the biometric profile is uniquely associated with an individual in (fig.3). Prokoski disclose acquiring a biometric input and determining that the profile is valid responsive to the acquired biometric input matching the received biometric profile in (fig.4).
Claim 40: Prokoski disclose wirelessly receiving a Personal Identification Number(PIN) profile forn the PDK, wherein the PIN profile is uniquely associated with an individual;acquiring a PIN input and determining that the profile is valid responsive to the acquired PIN matching the received PIN profile in (fig.6).
Claim 41: Prokoski disclose wirelessly receiving a picture profile from the PDK, wherein the picture profile is uniquely associated with an image of an individual;acquiring an image and determining that the profile is valid responsive to the acquired image matching the received picture profile in (col.11,lines 2-13).
Claim 42: Prokoski disclose receiving a registry profile from the PDK wherein the registry profile is uniquely associated with an individual and establishing a secure communication channel with a remote registry in (fig.1). Prokoski disclose transmitting the registry profile to the remote registry;receiving status information from the remote registry and determining that the profile is valid responsive to the status information indicating a valid registry entry in (fig.4).
Claims 1-42 meet the criteria set out in PCT Article 33(4), and thus meet industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Acknowledgement Receipt

EFS ID:	21487689
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	12-FEB-2015
Filing Date:	23-OCT-2014
Time Stamp:	16:49:05
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) Form (SB08)	04540US_IDS.pdf	619218 955604c99c923eab699611fc502c78d5c6ce89bc	no	22

Warnings:	
Information:	

2	Foreign Reference	01_WO0062505.pdf	939694 5ce5cb0dd11bbc758e1d30a5d1fa00979eba2784	no	27
Warnings:					
Information:					
3	Foreign Reference	02_WO0122724.pdf	1257552 2397b42fa8bf41be284186526a9ec6992979c976	no	32
Warnings:					
Information:					
4	Foreign Reference	03_WO0175876.pdf	1238267 68efaf81bd7f3ffd88395b255bbae522b85fd252	no	28
Warnings:					
Information:					
5	Foreign Reference	04_WO0177790.pdf	818043 c7e3a024ce24e36efcf80cfa54c59b8ac6f44b4c	no	20
Warnings:					
Information:					
6	Foreign Reference	05_WO2005050450.pdf	1758377 84ec9eca7924e958684bf6046532d2a980bcd6e2	no	49
Warnings:					
Information:					
7	Foreign Reference	06_WO2005086802.pdf	2017652 b79310d08b09d4211693aa74154e6a726f13895c	no	58
Warnings:					
Information:					
8	Non Patent Literature	01_AllianceActivities.pdf	226093 3a149c485022af159b17b0edd455d458d0173ac4	no	3
Warnings:					
Information:					
9	Non Patent Literature	02_AmrFarouk_AuthenticationMechanismsInGrid.pdf	1786086 f9bd310f701ec58b2788f8a851986f1080f7ef72	no	6
Warnings:					
Information:					
10	Non Patent Literature	03_Antonoff_VisitingVideoValley.pdf	1001904 8fa85f3153915fcbae89a24e5c2f9590a3bbd561	no	3
Warnings:					
Information:					

11	Non Patent Literature	04_ApplyingBiometricstoDoorAccess.pdf	346855 f9af7321aecb4b2def71495ba661f4e5167a4c36	no	5
Warnings:					
Information:					
12	Non Patent Literature	05_BioPayLLC_FrequentlyAskedQuestions.pdf	231993 96c8f4b9366666f073abd42470936e6450a9496e	no	5
Warnings:					
Information:					
13	Non Patent Literature	06_Blum_DigitalRightsManagementMaySolveTheNapster.pdf	349236 e1452e8c2f986cc194a4ada5edda2c522b186cb9	no	4
Warnings:					
Information:					
14	Non Patent Literature	07_DeBow_CreditDebitDebutsinMidwestSmartCardTest.pdf	657848 1773ef3ad9b896b2eb6aa53b63512d2bc935c3e3	no	4
Warnings:					
Information:					
15	Non Patent Literature	08_Dennis_DigitalPassportsNeedNotInfringeCivil.pdf	81856 4324c84fef98a5fb0f69735768bdf12b6f612522	no	2
Warnings:					
Information:					
16	Non Patent Literature	09_Fasca_TheCircuit.pdf	139107 c385ac718b7f0d2a6be3d6a9166377412cc5162a	no	2
Warnings:					
Information:					
17	Non Patent Literature	10_FirecrestShowsHowTrulyCommerciallyMindedCompanies.pdf	173133 f542234fb4a64551aea511b133ab47ad9f91bc46	no	2
Warnings:					
Information:					
18	Non Patent Literature	11_Kontzer_ThomsonBetsOnSmartCardsForVideo.pdf	67757 8e125353da0d334992e578d9d9890a1c8a950a70	no	1
Warnings:					
Information:					
19	Non Patent Literature	12_Lake_DownloadingforDollars.pdf	290663 ad7ef08e8937515910ef783ce7b9adec1e6a7e6f	no	2
Warnings:					
Information:					

20	Non Patent Literature	13_Lewis_SonyAndVisaInOnLineEntertainmentVenture.pdf	56440 e183f812be16d563399278260deffed202fadc35	no	1
Warnings:					
Information:					
21	Non Patent Literature	14_McIver_IdentificationandVerificationWorkingTogether.pdf	347011 7d958fbf0dfeba680cb6fb033aeaa0d90c8f45f7	no	5
Warnings:					
Information:					
22	Non Patent Literature	15_MicronasAndThomsonMultimediaShowcaseaNewCopy.pdf	169904 f021567ffe10585d21577b16178ebd3caadeb44e	no	3
Warnings:					
Information:					
23	Non Patent Literature	16_Nilsson_MatchOnCardForJavaCards.pdf	1011494 e50233adfa1bb35486bc68af3ceec3fab74903b5	no	5
Warnings:					
Information:					
24	Non Patent Literature	17_Nordin_MatchOnCardTechnology.pdf	1530705 504809efc706248c6b00b2ed6932d630deaaa0dc	no	7
Warnings:					
Information:					
25	Non Patent Literature	18_Paget_TheSecurityBehindSecureExtranets.pdf	324885 09fdc48f283744598ffdbd7c23e56d80294e149d	no	4
Warnings:					
Information:					
26	Non Patent Literature	19_PCTUS0438124.pdf	431799 b9d8cee6f85b9a37c4a265baf9ab46b08ae0a82e	no	10
Warnings:					
Information:					
27	Non Patent Literature	20_PCTUS0543447.pdf	341979 e06a0bc860468257522f92cbb0888a0b29911987	no	7
Warnings:					
Information:					
28	Non Patent Literature	21_PCTUS0546843.pdf	538413 0ebb0ba9323405efb1c8b3abbe0f9ac8b7462b6b	no	10
Warnings:					
Information:					

29	Non Patent Literature	22_PCTUS0711102.pdf	779621 bc08b8e1785656880d0c1b5ad988bf8c06146bd2	no	11
Warnings:					
Information:					
30	Non Patent Literature	23_PCTUS0711103.pdf	478058 4913218c747373b0b4ffa13151f026946d921db0	no	9
Warnings:					
Information:					
31	Non Patent Literature	24_PCTUS0711104.pdf	415819 8eaa9fea7d2fddf128f023eab6bd0a5cdeac7bc6	no	9
Warnings:					
Information:					
32	Non Patent Literature	25_PCTUS0711105.pdf	463359 10ca7e6029cc9e7dd891da26293de857acd025f5	no	10
Warnings:					
Information:					
33	Non Patent Literature	26_Pope_OasisDigitalSignatureServices.pdf	500950 96b3b3bf7bb7dd24d1fa936136f3b429a033b648	no	4
Warnings:					
Information:					
34	Non Patent Literature	27_SAFModuleTMALookIntoStrongAuthentication.pdf	404905 174befaccf905371360dc459482830f14f516f9d	no	8
Warnings:					
Information:					
35	Non Patent Literature	28_Sapsford_EBusinessSoundWavesCouldHelp.pdf	175123 242dee98e1ff7afed5dd004f8a66b0095eacdc91	no	2
Warnings:					
Information:					
36	Non Patent Literature	29_SayHelloToBluetooth.pdf	1126006 3a79860984b0abd13548a7704847a2462fb5f587	no	5
Warnings:					
Information:					
37	Non Patent Literature	30_SmartCardsAndBiometricsWhitePaper.pdf	310708 ffb7e11a22feacf7fd0bfac41ca78587156b6f61	no	7
Warnings:					
Information:					

38	Non Patent Literature	31_ThomsonMultimediaUnveilsCopyProtectionProposalDesigned.pdf	161763 595b77a62fa25ae58ac89df597cc16b6659f645e	no	2
Warnings:					
Information:					
39	Non Patent Literature	32_VanWinkle_BluetooththeKingofConnectivity.pdf	557066 b9829d8fc03ba8bc082d22b494ceca99b802de70	no	6
Warnings:					
Information:					
40	Non Patent Literature	33_Wade_UsingFingerprintsToMakePaymentsAtPOS.pdf	330268 991ab43f676f3ba58851acbdee21daf42148391a	no	3
Warnings:					
Information:					
41	Non Patent Literature	34_Wallace_TheInternetUnplugged.pdf	311563 82efeea8e7a8de75a3077741d26e9b75a2837d99	no	3
Warnings:					
Information:					
42	Non Patent Literature	35_Weber_InTheAgeOfNapster.pdf	162882 593bc896376b21ca23a73ade41fd5f6c024b6e68	no	3
Warnings:					
Information:					
43	Non Patent Literature	36_WhatIsAFile.pdf	42536 143edf491eb43706355e5ed7eec7e34aaa84b5d6	no	1
Warnings:					
Information:					
44	Non Patent Literature	37_Yoshida_ContentProtectionPlanTargetsWirelessHome.pdf	132557 e0702c3d6f06c7b588e5e523bb54dc715e92bf26	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	25107148		

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
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

POA ACCEPTANCE LETTER

OC000000073211543

Date Mailed: 02/05/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/29/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/ltaba/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

89194

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.*, a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	02/20/14
Name	John J. Gibbi	Telephone	
Title and Company	Chief Executive Officer Proxense, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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:	21344445
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	29-JAN-2015
Filing Date:	23-OCT-2014
Time Stamp:	14:35:30
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	Power of Attorney	04540US_20150129_POA_Transmittal.pdf	162114 375339c90d320dad76e348a2e2e21de098c6394b	no	2
Warnings:					
Information:					

2	Power of Attorney	04540US_20150129_POA.pdf	2293497 4f7c72ed2550548de95fc950d085d0a6243dbe8a	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	2455611	

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

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

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

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	14/521,982
Filing Date	October 23, 2014
First Named Inventor	John J. Giobbi
Title	Biometric Personal Data Key (PDK) Authentication
Art Unit	2437
Examiner Name	Not Yet Known
Attorney Docket Number	10001-04540 US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Paige Alsbury/	Date (Optional)	January 29, 2015
Name	Paige M. Alsbury	Registration Number	72,965
Title (if Applicant is a juristic entity)	Agent for Applicant		
Applicant Name (if Applicant is a juristic entity)	Proxense, LLC		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of One (1) forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

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
14/521,982	10/23/2014	2431	800	10001-04540 US	20	3

CONFIRMATION NO. 8239

UPDATED FILING RECEIPT

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

OC000000072630197

Date Mailed: 01/05/2015

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**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005
and claims benefit of 60/637,538 12/20/2004

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

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

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: December 23, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72,965

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF AN APPLICATION

Sir/Madam:

Responsive to the Notice of Missing Parts dated November 3, 2014, received in the above-identified application,

☒ Enclosed is:

☒ payment in the amount of $800 for the:

☒ $70 basic filing fee;

(continued)

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

☒ $300 search fee;

☒ $360 examination fee; and

☒ $70 late fee surcharge.

☒ Applicant claims small entity status under 37 C.F.R. § 1.27.

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 23, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72965
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (801) 258-9837
Fax: (801) 355-0160
Email: palsbury@patentlawworks.net

Electronic Patent Application Fee Transmittal

Application Number:	14521982
Filing Date:	23-Oct-2014
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Paige McDede Alsbury/Esther Kim
Attorney Docket Number:	10001-04540 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt	
EFS ID:	21057231
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	23-DEC-2014
Filing Date:	23-OCT-2014
Time Stamp:	18:55:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$800
RAM confirmation Number	19396
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	04540US_ResponseToMissingParts.pdf	60014 8633c37ee47dcb615dbbc1a3979218e1e2186813	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37036 ac4d81ad91e577171018c00d14360338d7bf2590	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	97050		

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
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FORMALITIES LETTER

OC000000072479254

Date Mailed: 12/22/2014

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on to the Notice to File Missing Parts (Notice) mailed 11/03/2014 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice. A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

Applicant is given **TWO MONTHS** from the date of the Notice to File Missing Parts (Notice) mailed 11/03/2014 within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee was not received.
- The application examination fee was not received.
- Surcharge as set forth in 37 CFR 1.16(f) was not received.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of the Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

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, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". 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.

/ltaba/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/521,982

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	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	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))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		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($)	ADDITIONAL FEE($)	OR	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.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: December 12, 2014 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination of the above-identified patent application, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (New) A method comprising:

persistently storing biometric data of a legitimate user and an ID code on the integrated device;

responsive to receiving a request for a biometric verification of a user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for authentication by an agent that is a third-party trusted authority; and

responsive to receiving an access message from the agent indicating that the agent successfully authenticated the user as the legitimate user based on the ID code, allowing the user to perform an action.

3. (New) The method of claim 1, further comprising:

registering an age verification for the user in association with the ID code.

4. (New) The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

5. (New) The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (New) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (New) The method of claim 1, wherein the action includes accessing an application.

8. (New) The method of claim 1, wherein the action includes completing a transaction.

9. (New) The method of claim 1, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

10. (New) The method of claim 1, further comprising:

responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

11. (New) An integrated device comprising:

a persistent storage media that stores biometric data of a user and an ID code;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for authentication by a third party that operates a trusted authority; and

a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code sent to the third party and allowing the user to perform an action.

12. (New) The integrated device of claim 11, wherein the ID code is transmitted to the trusted authority over a network.

13. (New) The integrated device of claim 11, wherein an age verification is registered in association with the device ID code.

14. (New) The integrated device of claim 11, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

15. (New) A system, comprising:

an integrated hardware device that stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the device ID code; and

an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the ID code and allows the user to perform an action; and

the trusted authority operated by a third party, the trusted authority storing a list of legitimate codes and determining the authentication of a user based on a comparison of the device ID received and the list.

16. (New) The system of claim 15, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify scan data as being from the legitimate user, the integrated hardware device does not send the ID code.

17. (New) The system of claim 15, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

18. (New) The system of claim 15, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

19. (New) The system of claim 15, wherein the action includes accessing one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (New) The system of claim 15, wherein the action includes completing a financial transaction.

21. (New) The system of claim 15, wherein the action includes accessing an application.

REMARKS

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 12, 2014 By: /Matthew M. Holmes/

Matthew M. Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

MMH:jam

Electronic Acknowledgement Receipt

EFS ID:	20946020
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	12-DEC-2014
Filing Date:	23-OCT-2014
Time Stamp:	16:10:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		04540US_PreliminaryAmendment.pdf	74644 7b4874bad12e698fb2f30b744749091de014f3b0	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	6
Warnings:			
Information:			
	Total Files Size (in bytes):	74644	

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/521,982	Filing Date 10/23/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 12/12/2014

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 17	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LDRC
/ADRIANE WINSTON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/521,982	10/23/2014	2431	0.00	10001-04540 US	1	1

CONFIRMATION NO. 8239

CORRECTED FILING RECEIPT

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

OC000000072075728

Date Mailed: 12/01/2014

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**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005
and claims benefit of 60/637,538 12/20/2004

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

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

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	14/521,982
FILING DATE:	October 23, 2014
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2431
ATTY. DKT. NO:	10001-04540 US
CONFIRMATION NO:	8239

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: November 25, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72,965

COMMISSIONER FOR PATENTS
OFFICE OF INITIAL PATENT EXAMINATION
CUSTOMER SERVICE CENTER
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

REQUEST FOR CORRECTED FILING RECEIPT

Sir/Madam:

Enclosed is a copy of the Official Filing Receipt. It contains the following errors:

1. The Domestic Priority data as claimed by applicant is missing a priority claim.

This application is a CON of 13/710,109, filed on December 10, 2012, which is a CON of 11/314,199, filed on December 20, 2005, which claims benefit of 60/652,765, filed on February 14, 2006 and claims the benefit of 60/637,538, filed on December 20, 2004. The Official Filing

Receipt is currently missing the last priority claim of 60/652,765. This priority claim was listed in the Application Data Sheet as-filed, however the prior Application Number was inadvertently omitted.

Attached is a Marked-Up Application Data Sheet indicating the required changes as well as the first page of the specification as-filed, which properly indicates the priority claim in question.

Please issue a corrected Filing Receipt rectifying this error.

Respectfully submitted,
JOHN J. GIOBBI

Dated: November 25, 2014 By: /Paige Alsbury/

Paige M. Alsbury, Reg. No. 72965
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (801) 258-9837
Fax: (801) 355-0160
Email: palsbury@patentlawworks.net

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	J.	Giobbi	

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

City	Bend	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	State/Province	OR
Postal Code	97701	Country	US

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

Correspondence Information:

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

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

Customer Number	89194		
Email Address	docketing@patentlawworks.net	Add Email	Remove Email

Application Information:

Title of the Invention	Biometric Personal Data Key (PDK) Authentication		
Attorney Docket Number	10001-04540 US	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Filing By Reference :

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

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

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89194		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13710109	2012-12-10

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13710109	Continuation of	11314199	2005-12-20	8352730	2013-01-08

Prior Application Status	Expired	Remove

EFS Web 2.2.11

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11314199	Claims benefit of provisional	60652765	2005-02-14
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
* 11314199	Claims benefit of provisional	60637538	2004-12-20

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

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

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

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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 instant patent application is filed access to the instant 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 instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant 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 instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

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

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

○ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Proxense, LLC		
Mailing Address Information For Applicant:			
Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	**State/Province**	OR
Country	US	Postal Code	97701
Phone Number		Fax Number	

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Email Address	

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

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

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

Signature	/Paige Alsbury/			Date (YYYY-MM-DD)	2014-11-25
First Name	Paige	Last Name	Alsbury	Registration Number	72965

Additional Signature may be generated within this form by selecting the Add button.

MARKED UP APPLICATION DATA SHEET

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent C o o p eration 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:	20803702
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	25-NOV-2014
Filing Date:	23-OCT-2014
Time Stamp:	20:01:11
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	Request for Corrected Filing Receipt	04540US_RequestForCorrected.pdf	57472 0d8ebe438d500df348a30ed1991fab52b2f3dbf4	no	2

Warnings:	
Information:	

2	Application Data Sheet	04540US_MarkedUpADS.pdf	87446 1d1473e4f014063c31681e560d97bf915ea5f19c	no	7

Warnings:	
Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	144918

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/521,982	10/23/2014	2431	0.00	10001-04540 US	1	1

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FILING RECEIPT

OC000000071643421

Date Mailed: 11/03/2014

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**

Inventor(s)

John J. Giobbi, Bend, OR;

Applicant(s)

Proxense, LLC, Bend, OR

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/710,109 12/10/2012 PAT 8886954
which is a CON of 11/314,199 12/20/2005 PAT 8352730
which claims benefit of 60/652,765 02/14/2005

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/31/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/521,982**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

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

Title

Biometric Personal Data Key (PDK) Authentication

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

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 (1-866-999-4258).

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).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/521,982

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	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	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))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		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($)	ADDITIONAL FEE($)	OR	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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FORMALITIES LETTER

OC000000071643422

Date Mailed: 11/03/2014

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).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

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, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". 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.

/zretta/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/521,982	10/23/2014	John J. Giobbi	10001-04540 US

CONFIRMATION NO. 8239

89194
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

IMPROPER CFR REQUEST

OC000000071655436

Date Mailed: 11/03/2014

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Continuity, Priority Claims, Petitions, and Non-Publication Requests

In response to your request for a corrected Filing Receipt, the Office is unable to comply with your request because:

- One or more of the benefit claims under 35 U.S.C. § 120 cannot be included on the Filing Receipt since applicant did not specify whether the application is a continuation, divisional or continuation-in-part of the prior application. Applicant must submit a new application data sheet (ADS) that sets forth the relationship, and the ADS must be accompanied by a petition under 37 CFR 1.78 if filed after the time period set forth in 37 CFR 1.78.

Improper Benefit Claim(s) to Prior-Filed Provisional Application(s)

The benefit claim(s) to prior-filed provisional application(s) is improper because the instant application was not filed within twelve (12) months from the filing date of the provisional application, and there is no indication of an intermediate nonprovisional or international application designationg the United States that is directly claiming the benefit of the provisional application and filed within 12 months of the filing date of the provisional application. Applicant should review each benefit claim submitted and, if appropriate, provide the proper reference to the prior-filed applications (including an indication of any intermediate application that is directly claiming the benefit of the provisional application and filed with 12 months of the filing date of the provisional application) as required by 37 CFR 1.78.

Alternatively, if the instant application (or intermediate application) was filed within 14 months of the prior provisional application, applicant may file a petition (in the instant application or the intermediate application, as appropriate) to restore the benefit of the provisional application if the delay in filing the instant application (or intermediate application) within the 12 month time period was unintentional. See 37 CFR 1.78 for the requirements of a petition to restore the benefit of the provisional application.

For applications filed on or after September 16, 2012, applicant must submit a corrected application data sheet (ADS) to include a specific reference.

Timeliness: The required reference for each benefit claim must be filed during the pendency of the instant application and within the later of: (1) four months from the actual filing date of the instant application, or the national stage commencement date if the instant application is a national stage application under 35 U.S.C. 371; or (2) sixteen months from the filing date of the prior-filed application. Failure to timely file the required reference is considered a waiver of any benefit claim, unless a grantable petition to accept an unintentionally

delayed claim under 37 CFR 1.78, the petition fee set forth in 37 CFR 1.17(m), and the required reference are filed.

/tnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	J.	Giobbi	

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

City	Bend	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	State/Province	OR
Postal Code	97701	Country i	US

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

Correspondence Information:

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

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

Customer Number	89194		
Email Address	docketing@patentlawworks.net	Add Email	Remove Email

Application Information:

Title of the Invention	Biometric Personal Data Key (PDK) Authentication		
Attorney Docket Number	10001-04540 US	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Filing By Reference :

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

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

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89194		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13710109	2012-12-10

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13710109	Continuation of	11314199	2005-12-20	8352730	2013-01-08

Prior Application Status	Expired	Remove

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
11314199	Claims benefit of provisional	60652765	2005-02-14
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Claims benefit of provisional	60637538	2004-12-20
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

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

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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 instant patent application is filed access to the instant 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 instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant 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 instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

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

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Proxense, LLC		
Mailing Address Information:			
Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	**State/Province**	OR
Country [i]	US	Postal Code	97701
Phone Number		Fax Number	

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

Email Address	

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

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/Matthew Holmes/			Date (YYYY-MM-DD)	2014-10-23
First Name	Matthew	Last Name	Holmes	Registration Number	65160

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04540 US
	Application Number	
Title of Invention	Biometric Personal Data Key (PDK) Authentication	

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

INVENTOR: JOHN J. GIOBBI

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority, under 35 U.S.C. § 120, to U.S. Patent Application No. 13/710,109 filed December 10, 2012 and entitled "Biometric Personal Data Key (PDK) Authentication" which claims priority to U.S. Patent Application No. 11/314,199, filed December 20, 2005 and entitled "Biometric Personal Data Key (PDK) Authentication," which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on December 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on February 14, 2005, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

[0003] Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allow-

ing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A uses often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

[0004] Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

[0005] Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

[0006] Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

[0007] The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, an integrated device includes a persistent storage to persistently stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format, and a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending a code for authentication.

[0008] In one embodiment, a method for verifying a user during authentication of an integrated device, includes persistently storing biometric data for the user in a tamper-resistant format; responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data to the biometric data to determine whether the data match; and responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication.

[0009] Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance the operations further include registering an age verification for the user in association with the code. For instance the operations further include establishing a

secure communication channel prior to sending the code for authentication. For instance the operations further include receiving a request for the code without a request for biometric verification, and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data. For instance, the features include: the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority; the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful; persistently storing biometric data includes permanently storing biometric data; the biometric data and the scan data are both based on a fingerprint scan by the user, an LED to be activated for requesting the biometric scan.

[0010] In one embodiment, a method for authenticating a verified user, includes receiving a code associated with a biometrically verified user; requesting authentication of the code; receiving an authentication result; and in response to the authentication result being positive, providing access to an application.

[0011] In one embodiment, a system includes an integrated device (e.g. a biometric key) to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code; and an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application.

[0012] Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance, the operations further include registering the code with a trusted authority, wherein requesting authentication of the code includes providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority. For instance the operations further include registering a date of birth or age with the trusted authority. For instance the operations further include establishing a secure communications channel with an integrated device, wherein the code associated with the biometrically verified user is received from the integrated device. For instance the features include: the integrated device receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data; when the integrated device cannot verify the scan data as being from the user, it does not send the code.

[0013] Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the integrated device can be authenticated for an application that is open to the public (i.e., in an open loop system).

[0014] The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

[0016] FIG. 1 is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

[0017] FIG. 2 is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

[0018] FIG. 3 is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

[0019] FIG. 4 is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

[0020] FIG. 5 is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

[0021] FIG. 6 is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

[0022] FIG. 7 is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0023] Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a fingerprint of a subject can be compared against previously-recorded biometric data for verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

[0024] Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

[0025] FIG. 1 is a schematic diagram illustrating an example of a biometric key 100 for providing authentication information for a biometrically verified user according to one embodiment of the present invention. In one embodiment, the biometric key 100 comprises a frame 110, a scan pad 120, and an LED 130. In one embodiment, biometric key 100 has a small form factor (e.g., the size of an automobile remote control) such that it can be unobtrusively carried by a user. In one embodiment, the biometric key 100 is integrated into another object or device. A

device having an integrated biometric key 100 is occasionally referred to herein as an "integrated device." For example, in one embodiment, the biometric key 100 is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key 100 unobtrusive to carry.

[0026] Frame 110 can be formed by plastic, metal or another suitable material. Frame 110 is shaped to secure scan pad 120, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame 110 is formed from a unitary molding to protect biometric data. Accordingly, frame 110 cannot be opened to expose the underlying components unless it is broken.

[0027] Scan pad 120 can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad 120 can be sized to fit a thumb or other finger. Biometric key 100 of the present embodiment includes LED 130 that lights up to request a fingerprint scan from a user. In one embodiment, LED 130 can also confirm that user verification and/or authentication has completed.

[0028] Biometric key 100 can authenticate a user for various purposes. For example, biometric key 100 can allow keyless entry into homes and autos. In another example, biometric key 100 can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key 100 can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key

100 operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

[0029] FIG. 2 is a block diagram illustrating biometric key 100 according to one embodiment of the present invention. Biometric key 100 comprises control module 210, biometric portion 220, RF communication module 230, persistent storage 240, and battery 250. Biometric key 100 can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key 100 comprises a modified key fob.

[0030] Control module 210 coordinates between several functions of biometric key 100. In one embodiment, control module 210 provides a verification code upon successful verification of the user. More specifically, once biometric portion 220 indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module 210 can trigger RF communication module 230 for sending a code indicating that the user was verified. In another embodiment, control module 210 can work in the opposite direction by detecting a request for verification from RF communication module 230, and then requesting verification of the user from biometric portion 210. Note that control module 210 of FIG. 2 is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key 100.

[0031] Biometric portion 220 comprises enrollment module 222, validation module 224, and biometric data base 226. In one embodiment, enrollment mod-

ule 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user. Further, enrollment module 222 registers biometric key 100 with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key 100 to be stored therein.

[0032] Validation module 224 can comprise scan pad 120 (FIG. 1) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module 214 determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module 224 can send comparison results to control module 210.

[0033] In other embodiments, validation module 224 can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.

[0034] Persistent storage 226 persistently stores biometric data from one or more users which can be provided according to specific implementations. In one embodiment, at least some of persistent storage 226 is a memory element that can be written to once but cannot subsequently be altered. Persistent storage 226 can include, for example, a ROM element, a flash memory element, or any other type

of non-volatile storage element. Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data). Furthermore, data can be stored in an encrypted form.

[0035] In one embodiment, persistent storage 226 also stores the code that is provided by the key 100 responsive to successful verification of the user. As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key 100. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments persistent storage 226 stores other data utilized during the operation of biometric key 100. For example, persistent storage 226 can store encryption/decryption keys utilized to establish secure communications links.

[0036] Radio frequency (RF) communication module 230 is, for example, a transceiver or other mechanism for wireless communication. RF communication module 230 can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication 220 can be optimized for low-power usage by, for example, using short-range transceivers. RF communi-

cation module 230 can actively send out connection requests, or passively detect connection requests.

[0037] Battery 260 can be a conventional power source suitable for the components of biometric key 100. Battery 260 can be either replaceable or rechargeable. Alternatively, battery 260 can be embedded within key 100 such that the key must be discarded or recycled upon expiration of the battery.

[0038] FIG. 3 is a block diagram illustrating a system 300 for providing authentication information for a biometrically verified user. System 300 comprises an authentication module 310 in communication with biometric key 100, a trusted key authority 320, and an application 330.

[0039] Authentication module 310 is coupled in communication with biometric key via line 311 (i.e., a wireless medium such as EM signals), and with trusted key authority 320 via line 312 (e.g., a secure data network such as the Internet, or a cell network). Authentication module 310 can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module 310 servers as a gatekeeper to application 330 by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module 310 provides the code to trusted key authority 320 in order to verify that it belongs to a legitimate key (e.g., when application 330 is security-critical). Authentication module

310 can send a message to application 330, or otherwise allow access to the application, responsive to a successful authentication by trusted key authority 320.

[0040] Application 330 is a resource that can be accessed by a verified and authenticated user. Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information. Application 330 can execute on the same system as authentication module 310 or on another system in communication with the system of the authentication module. In one embodiment, application module 330 allows access by a user after receiving a message from authentication module 310. At that point, application 330 can allow direct use by the user, or require that communications continue to pass through authentication module 310 for continued authentication.

[0041] Trusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. The list can be batched or updated each time a new user/key is enrolled. In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key. The profile describes the user associated with

the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority 320 is provided by a server or other computerized device.

[0042] In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority 320 provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority 320 can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

[0043] FIG. 4 is a flow chart illustrating a method 400 for authenticating a biometrically verified user using a trusted key authority (e.g., authority 320). A biometric key (e.g., biometric key 100) is registered 410 with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled 420 with the biometric key as described below with reference to FIG. 5.

[0044] In various situations, authentication of the key is needed 430 (e.g., by authentication module 310). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application 330). For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the bio-

metric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

[0045] The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user 440 as described below with reference to FIG. 6. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

[0046] The code is utilized to authenticate the biometric key itself 450, 460 as described below with reference to FIG. 7 and profile information is received. Responsive to successful authentication of the key, access is allowed 470 to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

[0047] FIG. 5 is a flow chart illustrating a method 500 for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks 510 an identification of the user and establishes a profile. The agent can be, for example, a government official, a nota-

ry, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

[0048] The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

[0049] The agent also collects and persistently stores 520 biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

[0050] FIG. 6 is a flow chart illustrating a method 600 for verifying a subject presenting the biometric key according to one embodiment of the present invention. In response to an authentication request, a user scan is requested 610 (e.g., by a blinking LED). Once the subject provides a fingerprint, scan data is received 620. Scan data is compared for a match 630 to previously-stored biometric data. If there is no match, then verification fails 650.

[0051] If there is a match, the subject is verified 640 as the user. The code indicating a successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230).

[0052] FIG. 7 is a flow chart illustrating a method 700 for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received 710. A request for authentication of the code is sent to the trusted key authority 720. The trusted key authority determines whether the code is authentic 730 (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). If authentication is successful, the trusted key authority sends an access message to the application to allow user access and/or provide additional information from the profile 740 (such as the user's age). If authentication is not successful, authentication fails 750 and the message to the application indicates that the user should be denied access.

[0053] In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order

to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

[0054] The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. The methods of the present invention may be performed in hardware, firmware, software, or any combination thereof operating on a single computer or multiple computers of any type. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

[0055] While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

[0056] In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

[0057] Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

[0058] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, prin-

cipally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0059] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0060] The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any

type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[0061] The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, as will be apparent to one of ordinary skill in the relevant art, the modules, features, attributes, methodologies, and other aspects of the invention can be implemented as software, hardware, firmware or any combination of the three. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

[0062] It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

CLAIMS

What is claimed is:

1. A method comprising:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

ABSTRACT

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

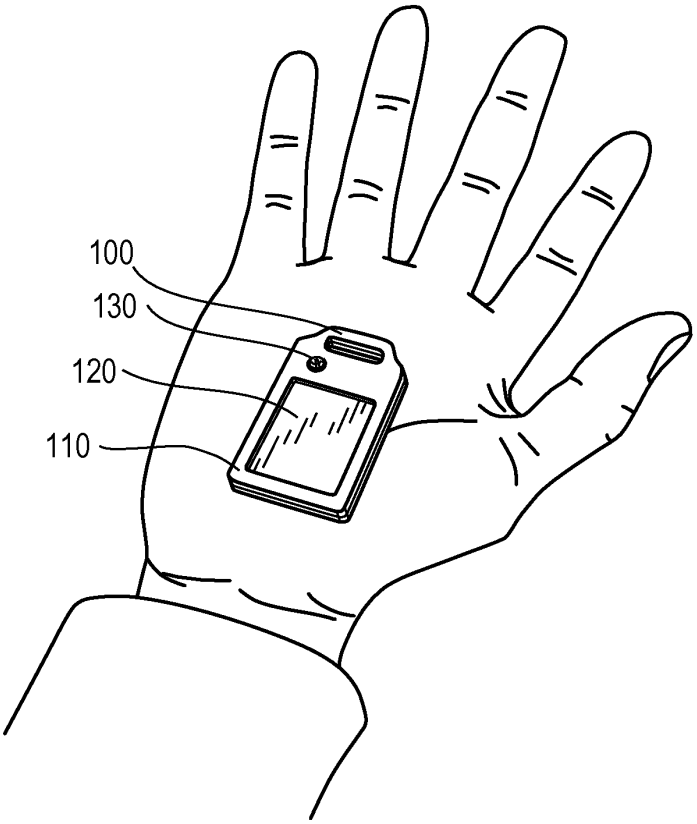

100
130
120
110

FIG. 1

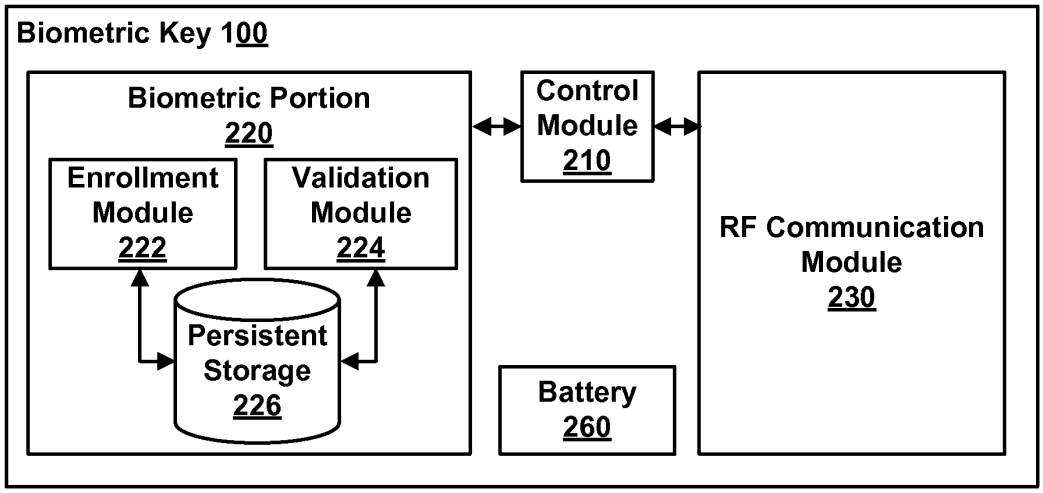

Biometric Key 100
Biometric Portion
220
Enrollment
Module
222
Validation
Module
224
Persistent
Storage
226
Control
Module
210
Battery
260
RF Communication
Module
230

FIG. 2

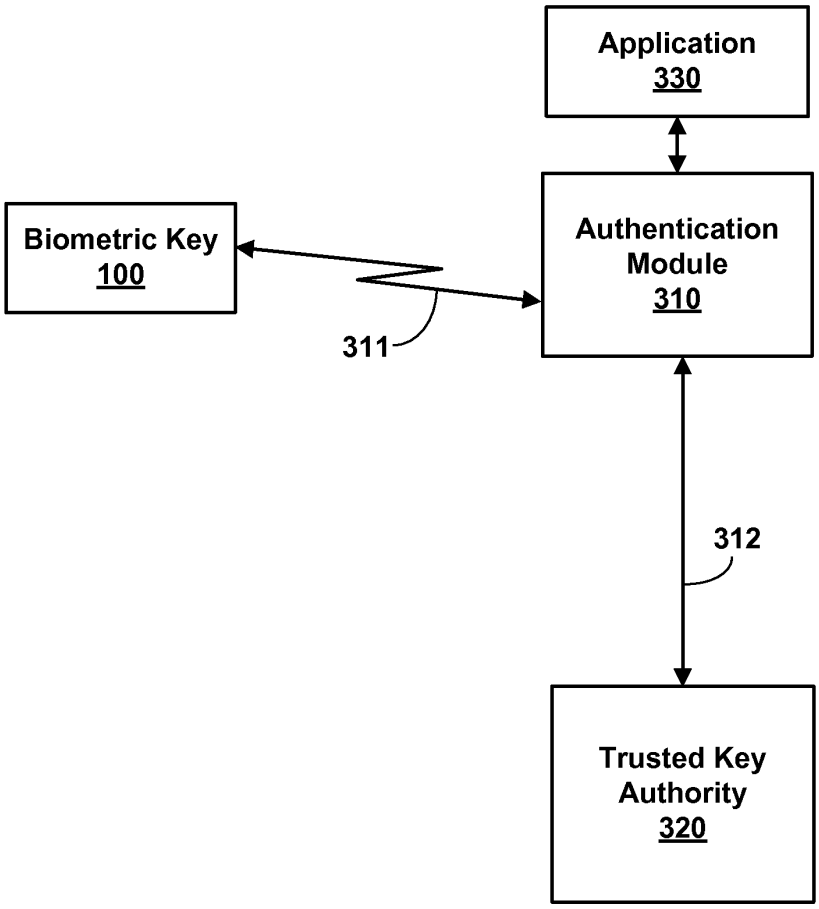

Application
330
Authentication
Module
310
Biometric Key
100
311
312
Trusted Key
Authority
320

FIG. 3

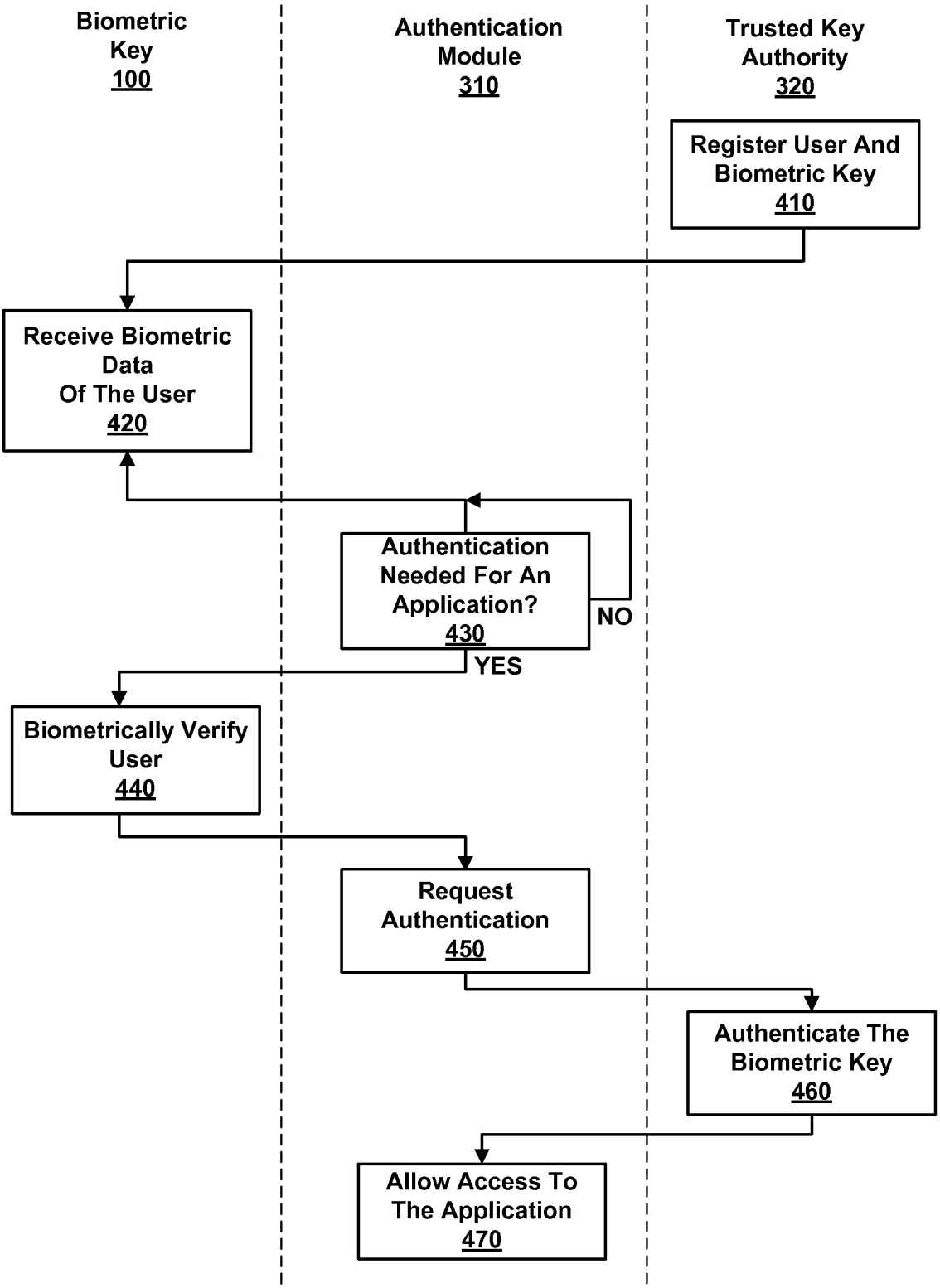

Biometric Key 100
Authentication Module 310
Trusted Key Authority 320
Register User And Biometric Key 410
Receive Biometric Data Of The User 420
Authentication Needed For An Application? 430
NO
YES
Biometrically Verify User 440
Request Authentication 450
Authenticate The Biometric Key 460
Allow Access To The Application 470

FIG. 4

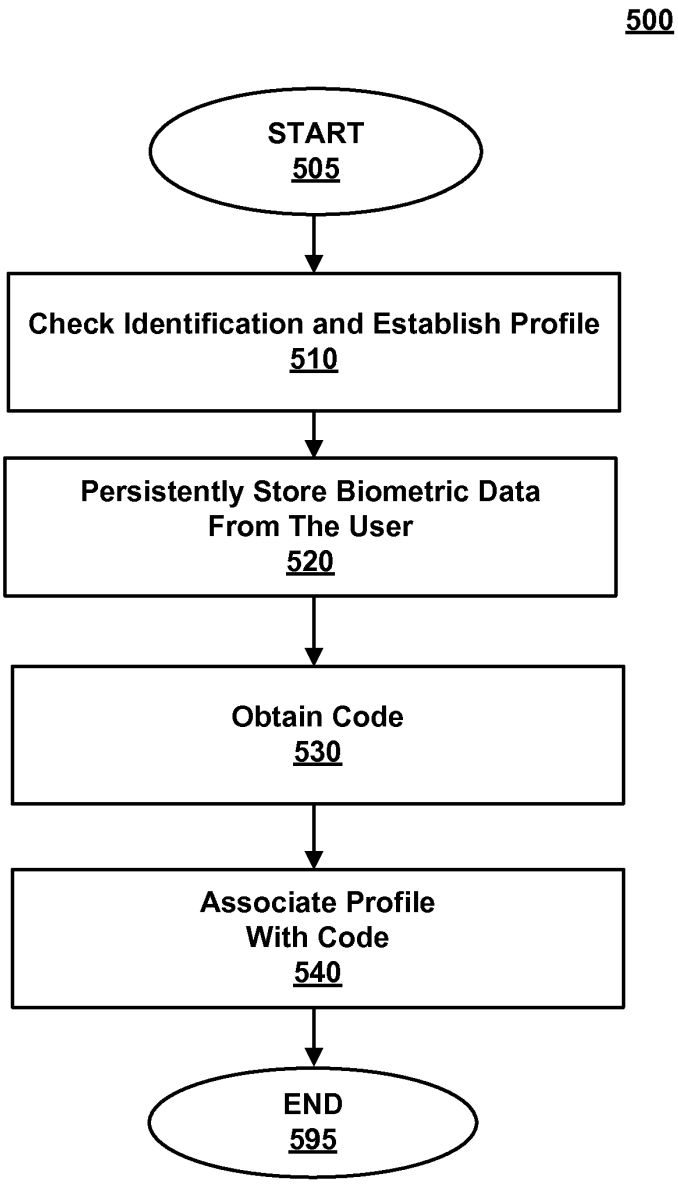

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data From The User
520
Obtain Code
530
Associate Profile With Code
540
END
595

FIG. 5

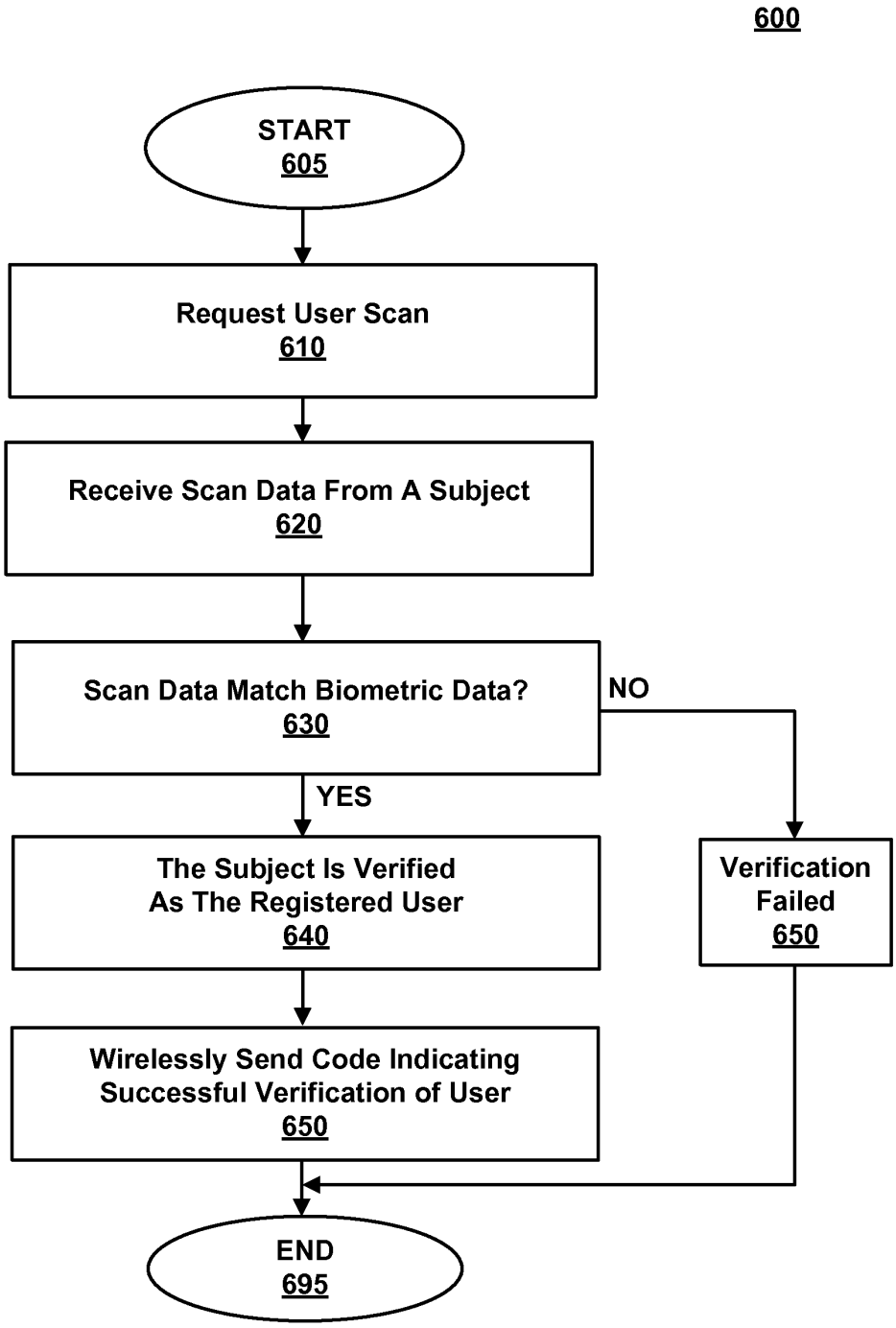

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

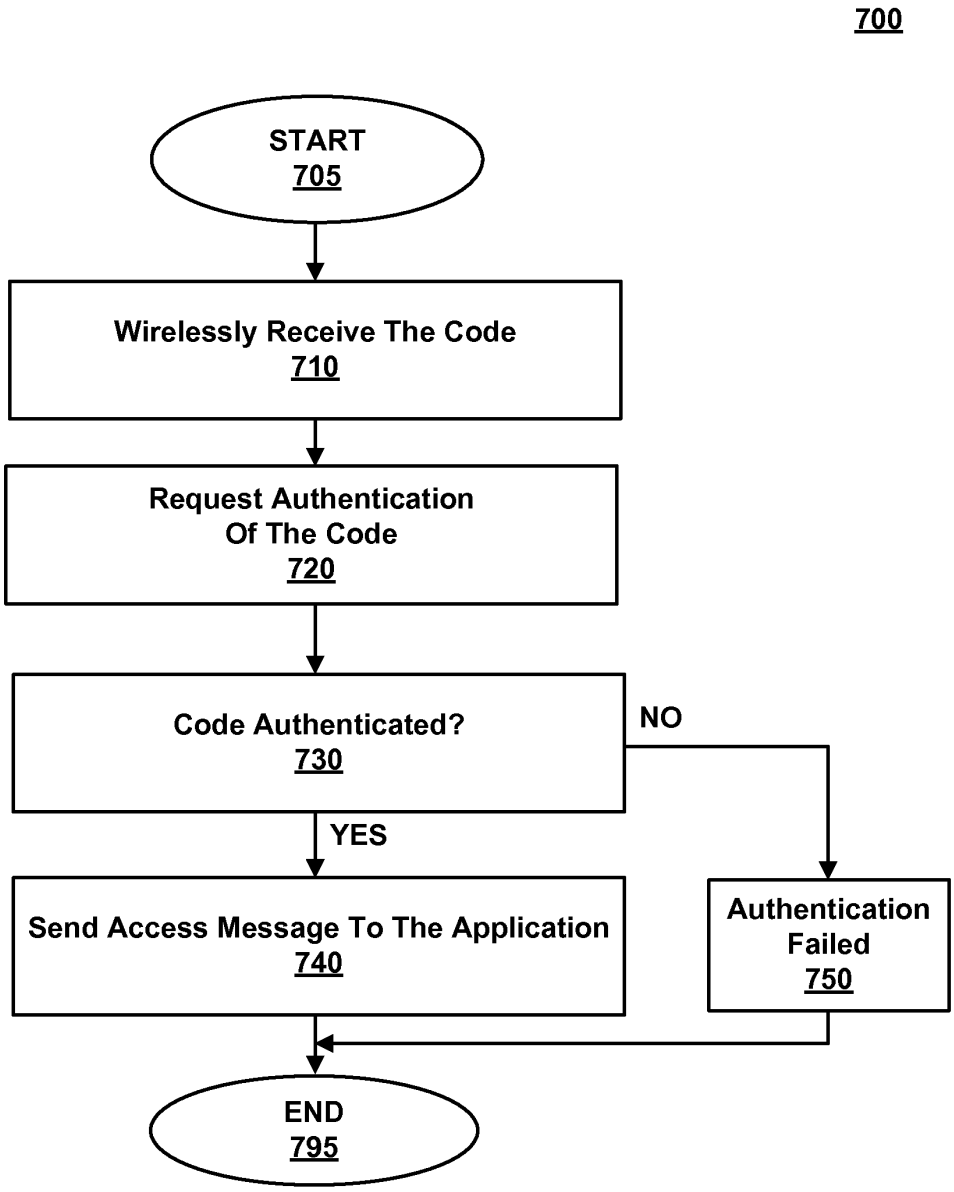

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

PTO/AIA/01 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Biometric Personal Data Key (PDK) Authentication

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

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.

LEGAL NAME OF INVENTOR

Inventor: John J. Giobbi Date (Optional): 12/10/12

Signature: _____

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	20499600
Application Number:	14521982
International Application Number:	
Confirmation Number:	8239
Title of Invention:	Biometric Personal Data Key (PDK) Authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04540 US
Receipt Date:	23-OCT-2014
Filing Date:	
Time Stamp:	15:28:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	04540US_ApplicationDataSheet.pdf	1561392 d439ba5a9030e9ff705e0bfaf6242f5753b1ae46	no	7

Warnings:	
Information:	

2		04540US_Specification.pdf	131764 d4416d847baa9c200f12c875894a94f73c821025	yes	25

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	23
Claims	24	24
Abstract	25	25

Warnings:

Information:

3	Drawings-only black and white line drawings	04540US_Drawings.pdf	82588 4e3c63c77aaff8bdc0ea838506ae2995153b1cff	no	6

Warnings:

Information:

4	Oath or Declaration filed	04540US_Declaration.pdf	446969 6c2442ad680b2b87db1c56f131567ba1b49df78a	no	2

Warnings:

Information:

Total Files Size (in bytes):	2222713

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.