IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

FIRST INVENTOR:	John J. Giobbi
APPLICATION NO:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO:	10001-02090 US
CONFIRMATION NO:	4469

CERTIFICATE OF EFS-WEB TRANSMISSION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being transmitted via the U.S. Patent and Trademark Office electronic filing system (EFS-Web) to the USPTO on the date below.

Date: August 23, 2022 By: /Greg T. Sueoka/
Greg T. Sueoka, Reg. No. 33,800

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

RESPONSE TO REQUEST FOR INFORMATION

Responsive to the Request for Information mailed on July 14, 2022, Petitioner responds as follows:

1) Petitioner confirms that the district court proceeding (Proxense LLC v. Samsung Electronics, Co. LTD and Samsung Electronics America, Inc., 6:21-CV-00210 (W.D. Tex.) is ongoing;

2) Petitioner is not aware of any additional ongoing court proceedings involving this patent at this time;

3) Petitioner has not notified the district court in the proceeding identified in 1) above that the petition was filed, so the Petitioner does not know whether the court would object to the USPTO issuing a decision on the petition filed March 3, 2022.

4) Petitioner is not aware of any other information including any documents or other evidence that may reasonably be deemed material to the decision on the petition.

The Office of Petitions is welcome to contact the undersigned as indicated below if there is any additional information needed, are any additional questions or concerns.

Respectfully submitted,
PROXENSE, LLC

Dated: August 23, 2022 By: /Greg T. Sueoka/

Greg T. Sueoka, Reg. No. 33,800
Attorney for Applicant
PATENT LAW WORKS LLP
310 East 4500 South, Suite 400
Salt Lake City, UT 84107
Tel.: (801) 258-9821
Fax: (801) 355-0160
Email: gsueoka@patentlawworks.net

GTS/kdl

Electronic Acknowledgement Receipt

EFS ID:	46468763
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Greg T. Sueoka
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	23-AUG-2022
Filing Date:	20-DEC-2005
Time Stamp:	15:59:43
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	Miscellaneous Incoming Letter	02090US_20220823_ResponsetoRequestforInformation.pdf	23024 550f393a57af689ce34cf28b19337b2e86493d6d	no	2

Warnings:

Information:	
Total Files Size (in bytes):	23024

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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

89194 7590 07/14/2022
Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City, UT 84107

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
07/14/2022	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

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 8,352,730 Issue Date: 08 Jan 2013 Application No. 11/314,199 Filing or 371(c) Date: 20 Dec 2005 Attorney Docket No. 10001-02090 US	:	REQUEST FOR INFORMATION

This is a request for clarifying information regarding the petition requesting the acceptance of a fee deficiency submission, filed under 37 CFR 1.28, on March 3, 2022.

On April 16, 2021, paper(s) was/were filed indicating that there is a district court proceeding which involves this patent.

In order to receive a decision on the petition filed on March 3, 2022, petitioner is required to respond to this notice with the following information: 1) a confirmation or denial that the district court proceeding is ongoing; 2) an identification of any other ongoing court proceeding(s) which involve this patent; 3) for any ongoing court proceeding identified in this notice or in the response, petitioner should additionally confirm that a) the court(s) has/have been alerted that the petition was filed and b) that the court(s) does/do not object to the USPTO issuing a decision on the petition filed March 3, 2022; and 4) any other information including any documents or other evidence that may reasonably be deemed material to the decision on the petition.

Telephone inquiries concerning this notice may be directed to Anna Pagonakis at (571) 270-3505.

/Cheryl Gibson-Baylor/
Cheryl Gibson-Baylor
Office of Petitions

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

FIRST INVENTOR:	John J. Giobbi
APPLICATION NO:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO:	10001-02090 US
CONFIRMATION NO:	4469

CERTIFICATE OF EFS-WEB TRANSMISSION UNDER 37 CFR § 1.8
I hereby certify that this correspondence is being transmitted via the U.S. Patent and Trademark Office electronic filing system (EFS-Web) to the USPTO on the date below.
Date: March 3, 2022 By: /Greg T. Sueoka/
Greg T. Sueoka, Reg. No. 33,800

MAIL STOP 16
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

NOTIFICATION OF LOSS OF SMALL ENTITY STATUS UNDER 37 CFR 1.27(g)(2) AND PAYMENT OF DEFICIENCY IN FEES

Sir/Madam:

This communication hereby notifies the United States Patent and Trademark Office that small entity status is not applicable for the above-identified patent application. The undersigned was made aware of the above-identified property having been licensed to a large entity since November 20, 2019. The undersigned is hereby taking action to rectify the situation and the pay

the fees associated with this application as a large entity. The amount of additional fees to be paid as a large entity are as follows:

Date Paid	Fee Code	Description	Amount Paid	Undiscounted Fee (Fee Code)	Amount Owed
07-06-2020	2552	For maintaining an original or any reissue patent, due at 7.5 years	$1800	$3600 (1552)	$1800
				Total Amount Owed:	$1800

The Director is hereby authorized to charge the above-identified fees totaling $1800, and any additional fees which may be required, including any petition fees, or credit any overpayment to Deposit Account No. 603148.

Respectfully submitted,

PROXENSE, LLC

Dated: March 3, 2022 By: /Greg T. Sueoka/

Greg T. Sueoka, Reg. No. 33,800
Attorney for Applicant
PATENT LAW WORKS LLP
310 East 4500 South, Suite 400
Salt Lake City, UT 84107
Tel.: (801) 258-9821
Fax: (801) 355-0160
Email: gsueoka@patentlawworks.net

GTS/kkt/kdl

Electronic Acknowledgement Receipt	
EFS ID:	45134794
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Greg T. Sueoka
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	03-MAR-2022
Filing Date:	20-DEC-2005
Time Stamp:	12:35:12
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	Petition for review by the Office of Petitions	02090US_20220303_NotificationofLossofSmallEntityStatus.pdf	25544 177e4b10fe929e113e7938783e21e7607566ce68	no	2

Warnings:

Information:	
Total Files Size (in bytes):	25544

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	REQUEST ID
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	157417

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 01/27/2022 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:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

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

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

DOCKET NO.	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.
11/314,199	01/08/2013	8352730	10001-02090 US	4469

89194 7590 12/18/2012
Patent Law Works/Proxense
165 South Main St
Suite 2
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 938 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;

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.

IR103 (Rev. 10/09)

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
11/314,199	20 December, 2005	GIOBBI, JOHN J.	10001-02090 US

		EXAMINER	
Patent Law Works/Proxense 165 South Main St Suite 2 Salt Lake City, UT 84111		PHY ANH VU	
		ART UNIT	PAPER
		2437	201212061

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

IDS dated 11/29/2012 has been considered on 12/6/2012.	
	/PHY ANH VU/ Examiner, Art Unit 2437

PTO-90C (Rev.04-03)

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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
/P.V./	1	7883417		2011-02-08	Bruzzese 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
/P.V./	1	20010044337		2001-11-22	Rowe et al.	
/P.V./	2	20020098888		2002-07-25	Rowe et al.	
/P.V./	3	20020103027		2002-08-01	Rowe et al.	
/P.V./	4	20040209690		2004-10-21	Bruzzese et al.	
/P.V./	5	20080188308		2008-08-07	Shepherd et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS	Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

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]
/P.V./	1	POPE, Oasis Digital Signature Services: Digital Signing without the Headaches, Internet Computing-IEEE, Vol. 10, 2006, pgs 81-84.	☐

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	12/06/2012

*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.

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 08/31/2012
Patent Law Works/Proxense
165 South Main St
Suite 2
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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

TITLE OF INVENTION: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	~~$870~~ $885	$300	$0	~~$1170~~ $1185	11/30/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2437	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. ~~XXXXXXXXXXXXXXXXXX~~.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Kanda Ishihara/ Date November 30, 2012

Typed or printed name Kanda V. Ishihara Registration No. 56,607

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Kanda Ishihara/JoLin Johnson
Attorney Docket Number:	10001-02090 US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	885	885

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1185**

Electronic Acknowledgement Receipt	
EFS ID:	14352211
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	30-NOV-2012
Filing Date:	20-DEC-2005
Time Stamp:	17:47:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1185
RAM confirmation Number	6555
Deposit Account	
Authorized User	

File Listing:

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

1	Issue Fee Payment (PTO-85B)	02090US_IssueFeeTransmittal.pdf	549415 24978b93c6773dad24a28df4460e73f0f8c8bf74	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32028 efe40d5a0d5067268a572fe1526925037f31383c	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	581443	

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

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

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

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

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

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	7883417		2011-02-08	Bruzzese 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	20020098888		2002-07-25	Rowe et al.	
	3	20020103027		2002-08-01	Rowe et al.	
	4	20040209690		2004-10-21	Bruzzese et al.	
	5	20080188308		2008-08-07	Shepherd et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

FOREIGN PATENT DOCUMENTS	Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

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	POPE, Oasis Digital Signature Services: Digital Signing without the Headaches, Internet Computing-IEEE, Vol. 10, 2006, pgs 81-84.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	/Kanda Ishihara/	Date (YYYY-MM-DD)	2012-11-29
Name/Print	Kanda Ishihara	Registration Number	56607

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 Patent Application Fee Transmittal	
Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Kanda Ishihara/JoLin Johnson
Attorney Docket Number:	10001-02090 US
Filed as Small Entity	

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt	
EFS ID:	14342115
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	29-NOV-2012
Filing Date:	20-DEC-2005
Time Stamp:	23:46:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	8106
Deposit Account	
Authorized User	

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)	02090US_PTOSB08a.pdf	612523 ea773751b46fc965b5a6549 43c1a464776edf645	no	4
Warnings:					
Information:					
2	Non Patent Literature	OasisDigitalSignatureServices.pdf	493955 30ae63c23bbc42f68d90ca0beb49e5ab009d41b3	no	4
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30477 e79f38da333e60d923daff10a64c6efa20c958a1	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1136955	

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

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

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

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

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 08/31/2012
Patent Law Works/Proxense
165 South Main St
Suite 2
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 08/31/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

TITLE OF INVENTION: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	11/30/2012

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

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

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

89194 7590 08/31/2012
Patent Law Works/Proxense
165 South Main St
Suite 2
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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

TITLE OF INVENTION: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	11/30/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
VU, PHY ANH TRAN	2437	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 credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

89194 7590 08/31/2012
Patent Law Works/Proxense
165 South Main St
Suite 2
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 08/31/2012

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

The Patent Term Adjustment to date is 676 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 676 day(s).

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

-- 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 *The Request for Continued Examination 1/15/2012*.

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

3. ☒ The allowed claim(s) is/are *1-3,5,7-10,12-15 and 17-21*.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 3/2/2012; 5/2/2012
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/PHY ANH VU/
Examiner, Art Unit 2437

DETAILED ACTION

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given by Applicant's representative Kanda Ishihara on August 20th, 2012.

Replace claims 1, 2, 5, 8-10, 12, 14-15, and 18-25 with the amendments below:

Claim 1:

A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the 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 a storage element on the integrated device that is unable to be subsequently altered; **wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.**

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 **from the plurality of codes** and **the** other data values ~~**from the plurality of codes and other data values**~~ for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

responsive to authentication of the one or more codes and **the** other data values by the agent, receiving an access message from the agent allowing the user access to an application**, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.**

Claim 2:

The method of claim 1, wherein the one or more codes and **the** other data values are transmitted to the agent over a network.

Claim 5:

The method of claim 1, wherein the one or more codes and **the** other data values indicate that the biometric verification was successful.

Claim 8:

The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and **the** other data values for authentication.

Claim 9:

The method of claim 1, further comprising:

receiving a request for the one or more codes and **the** other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and **the** other data values without a request for biometric verification, sending the one or more codes and **the** other data values without requesting the scan data.

Claim 10:

An integrated device for verifying a user during authentication of the integrated device, comprising:

a ~~**persistent storage**~~ **memory** ~~**to store**~~ **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 **memory** that is unable to be subsequently altered; **wherein the biometric data is selected from a group consisting of a palm print, a retinal scan,**

an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

a **verification unit** ~~**verification module**~~, in communication with the **memory** ~~**persistent storage**~~, ~~**to**~~ receive**s** scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly **sends** ~~**sending**~~ one or more codes **from the plurality of codes** and **the** other data values ~~**from the plurality of codes and other data values**~~ for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and **the** other data values includes the device ID code; and

responsive to the agent authenticating the one or more codes and the other data values, a radio frequency **communicator**, ~~**communication module for receiving**~~ **receives** an access message from the agent allowing the user access to an application, ~~**responsive to the agent authenticating the one or more codes and the other data values.**~~ **wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.**

Claim 12:

The integrated device of claim 10, wherein the one or more codes and **the** other data values are transmitted to the agent over a network.

Claim 14:

The integrated device of claim 10, wherein the **verifier** ~~**verification module**~~ comprises: an LED to be activated for requesting the biometric scan.

Claim 15:

A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes **from a plurality of codes** and other data values ~~**from a plurality of codes and other data values**~~ including a device ID code, wherein the plurality of codes and **the** other data values comprises the ~~**comprising a**~~ device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified **user**, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and **the** other data values by the agent, wherein the authentication determines whether the one or more codes and **the** other data values are legitimate;

receiving an access message from the agent; and

in response to a positive access message, allowing the **biometrically** **verified** user access to an application, **wherein the application is selected from a group**

consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

Claim 18:

The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and **the** other data values associated with the biometrically verified user is received from the biometric key.

Claim 19:

A system, comprising:

a biometric key ~~to~~ store**s** biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes **from the plurality of codes** and other data values ~~from the plurality of codes and other data values,~~ wherein the one or more codes and **the** other data values include~~s~~ the device ID code**, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a**

hand geometry, a facial recognition, a signature recognition and a voice recognition; and

an **authentication unit** ~~**authentication module**~~ ~~**to**~~ receive**s** the plurality of codes and **the** other data values and send the plurality of codes and **the** other data values to agent for authentication to determine whether the one or more codes and **the** other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the **authentication unit** ~~**authentication module**~~ receiving an access message from the agent allowing the user to access **an** ~~**the**~~ application, **wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.**

Claim 20:

The system of claim 19, wherein the biometric key receives an authentication request from the **authentication unit** ~~**authentication module**~~, and in response, requests a biometric scan from the user to generate the scan data.

Claim 21:

The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and **the** other data values.

Claim 22-cancelled.

Claim 23-cancelled.

Claim 24-cancelled.

Claim 25-cancelled.

Examiner's Statement for Reasons of Allowance

Claims 1-3, 5, 7-10, 12-15, and 17-21 are allowed, while claims 4, 6, 11, 16, and 22-25 are cancelled.

The present invention is directed to methods and devices for verifying a user during authentication of an integrated device.

The closest prior arts cited are generally directed to various aspects of verifying users during authentication of a device. However, none of the cited arts found alone or in combination suggests or teaches the elements of the independent claims. For instance, no parts of the cited arts teach or suggest limitations in a first embodiment of the invention which verifying a user during authentication of an integrated device, comprising the steps of: persistently storing biometric data of the 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 a storage element on the integrated device that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; 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 from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file. The cited prior arts also do not teach or suggest limitations in the second embodiment of the invention which authenticating a verified user using a computer processor configured to execute method steps, comprising: receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with

a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices; requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are legitimate; receiving an access message from the agent; and in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

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 for 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 7:30-11:30, TH- F 8-4:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on 571-272-3867. 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 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/314,199	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2002/0150282	10-2002	Kinsella, David J.	382/124
*	B	US-2005/0074126	04-2005	Stanko, Joseph A.	380/279
*	C	US-2004/0129787	07-2004	Saito et al.	235/492
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

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	11314199
Filing Date	2005-12-20
First Named Inventor	John J. Giobbi
Art Unit	2437
Examiner Name	Phy Anh Vu
Attorney Docket Number	10001-02090 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	20020014954	A1	2002-02-07	FITZGIBBON, James J. et al.	
/P.V./	2	20020178063	A1	2002-11-28	GRAVELLE, Kelly 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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Vu
	Attorney Docket Number	10001-02090 US

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	United States Office Action, U.S. Patent Application No. 11/292,330, December 2, 2011, 25 pages.	☐
/P.V./	2	United States Office Action, U.S. Patent Application No. 11/744,831, December 16, 2011, 38 pages.	☐
/P.V./	3	United States Office Action, U.S. Patent Application No. 11/744,832, February 7, 2012, 32 pages.	☐

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	08/22/2012

*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.

EFS Web 2.1.17

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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
/P.V./	1	6018739	A	2000-01-25	McCOY, Mike et al.	
/P.V./	2	6983882	B2	2006-01-10	CASSONE, Jean	
/P.V./	3	7218944	B2	2007-05-15	CROMER, Daryl Carvis et al.	
/P.V./	4	7715593	B1	2010-05-11	ADAMS, William Mark 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
/P.V./	1	20020014954	A1	2002-02-07	FITZGIBBON, James J. et al.	
/P.V./	2	20020140542	A1	2002-10-03	PROKOSKI, Francine et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

/P.V./	3	20020178063	A1	2002-11-28	GRAVELLE, Kelly et al.	
/P.V./	4	20030172037	A1	2003-09-11	JUNG, Changwoo et al.	
/P.V./	5	20050251688	A1	2005-11-10	NANAVATI, Samir et al.	
/P.V./	6	20100117794	A1	2010-05-13	ADAMS, William Mark	
/P.V./	7	20110126188	A1	2011-05-26	BERNSTEIN, Daniel M. 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]
/P.V./	1	United States Office Action, U.S. Patent Application No. 11/292,330, December 2, 2011, 25 pages.	☐

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

/P.V./	2	United States Office Action, U.S. Patent Application No. 11/745,249, February 2, 2012, 36 pages.	☐
/P.V./	3	United States Office Action, U.S. Patent Application No. 11/744,832, February 7, 2012, 32 pages.	☐
/P.V./	4	United States Office Action, U.S. Patent Application No. 11/292,330, April 6, 2012, 22 pages.	☐

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	08/22/2012

*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
		(list near5 code) with ((legitimate or registered) near5 (device or fob or system)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:50
		713/176.ccls. and (S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:05
		(transmit$4 or send$4) near10 ((access near5 (grant$4 or permit$4))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
		()	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/05 20:15
		S20 ((authenticat$3 or verif$6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
L1	1326	382/115.ccls. and (biometric)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2012/08/22 21:36
L4	18	("6018739" "6983882" "7218944" "7715593" "20020014954" "20020140542" "20020178063" "20030172037" "20050251688").pn.	US-PGPUB; USPAT; DERWENT	OR	ON	2012/08/22 21:49
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42

S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21
S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59

S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif$6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S25	5	713/186.ccls. and ((authenticat$4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat$4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50
S27	31	713/186.ccls. and ((authenticat$4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51

S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat$4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S31	562	713/186.ccls. and (authenticat$4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat$4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S33	228	713/186.ccls. and (authenticat$4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat$4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat$4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49
S37	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42
S38	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S39	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43

S40	71	713/176.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S41	0	713/176.ccls. and (biometric$6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S42	52	713/176.ccls. and (biometric$6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S43	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S44	102	S43 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S45	9	S43 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48
S46	15	(john near4 giobbi).inv. and (biometric$4 with authenticat$4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S47	7	(john near4 giobbi).inv. and (biometric$4 with authenticat$4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S48	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 10:08
S49	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:30
S50	1	"20060143441".pn. and (palm near4 print)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S51	1	"20060143441".pn. and (casino near4 machine)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31

S52	157	713/155,159.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:25
S53	121	S52 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:26
S54	192	713/176.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:39
S55	154	S54 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S56	20	S55 and (LED)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S57	106	726/27.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S58	75	S57 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S59	9	(giobbi near4 john).in. and ((authenticat$4) and (biometric$6)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:47
S60	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/05 17:51
S61	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 13:21
S62	6719	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
S63	561	S62 and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56

S64	248	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4)) and ((authenticat$4) near10 (biometric))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S65	134	S64 and @ad<"20050201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S66	56	713/186.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:01
S67	68	713/176.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:06
S68	86	713/155,159.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S69	80	S68 NOT S67	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S70	77	S69 NOT S66	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S71	68	726/27.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:17
S72	68	(john near5 giobbi).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S73	0	(john near5 giobbi).in. and biometri	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S74	31	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:23
S75	1	11/871150	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:43

S76	42	(list near5 code) with ((legitimate or registered) near5 (device or fob or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:50
S77	24	S76 and @ad<"20051220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:51
S78	2	"4993068".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 20:07
S79	26	("4993068" "5917913" "6016476" "6038334" "6121544" "6256737" "7191466" "7529944" "20020023032" "20020138767" "20030036425" "20030046552" "20030054881").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/02/24 20:08
S80	1	713/155,159.ccls. and (device or fob) with (registered or authoriz$7) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:52
S81	9	713/155,159.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:54
S82	17	726/27.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:01
S83	0	726/27.ccls. and (biometric near "10" (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:03
S84	0	726/27.ccls. and (biometric near10 (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S85	0	726/27.ccls. and (biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S86	0	(biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S87	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04

S88	107	S87 and @ad<"20041220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:05
S89	805	340/5.52-5.53.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S90	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S91	33	S89 and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S92	9	382/115.ccls. and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:40
S93	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
S94	0	713/176.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
S95	14	713/186.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
S96	16	"380"/$.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:15
S97	13	(proxense).as. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:18
S98	5	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 10:45
S99	2	"6185316".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:26

S100	3	"6219439".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:27
S101	2	"6363485".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:28
S102	2	"20020150282".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:29
S103	2	"20020158750".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:33
S104	2	"5416780".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:34
S105	2	"5894551".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:35
S106	2	"6042006".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:35
S107	2	"6070796".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:36
S108	5	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:43
S109	1	12/651085	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 16:16
S110	377	fob with (stor$3 or contain$3) with (ID or code or account)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:46
S111	29	S110 and "713"/$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:47

S112	0	S111 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:48
S113	19	S111 and @ad<"20051220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:48
S114	77	713/156,159,186.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:43
S115	0	S114 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:44
S116	8	S114 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:44
S117	31	726/27-30.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:46
S118	3	S117 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
S119	41	382/115.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
S120	4	S119 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
S121	0	wo "2003/017559"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2012/08/22 13:48
S122	1	wo "2003017559"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2012/08/22 13:48
S123	0	(biometric) with (consist$3 with (palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2012/08/22 14:00

		(voice near4 recognition)).clm.				

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
		713/156,159,186 with (palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:05
L2	26	382/115.ccls. and (fob)	USPAT; UPAD	ADJ	ON	2012/08/22 21:37
L3	0	((palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 21:47
S124	0	(biometric) with (consist$3 with (palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:00
S125	0	(application or software or device or machine) with (consist$3 with (casino adj machine) with(keyless near2 lock) with (garage near2 door near4 open$3) with (atm near2 machine) with (hard$drive) with (computer near2 software) with (website) with (file)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:03
S126	47	713/156,159,186.ccls. and (fob)	USPAT; UPAD	ADJ	ON	2012/08/22 14:04
S127	0	713/156,159,186.ccls. and ((palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:05
S128	0	726/27-30.ccls. and ((palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:05
S129	0	"382"/$.ccls. and ((palm near4 print) with (retinal near4 scan) with (iris near2 scan) with (hand near2 geometry) with (facial near2 recognition) with (signature near3 recognition) with (voice near4 recognition)).clm.	USPAT; UPAD	ADJ	ON	2012/08/22 14:05

8/22/2012 10:01:08 PM
C:\Users\pvu3\Documents\EAST\Workspaces\11314199.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
713	155,159,176, 186	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011; 8/22/2012	PVU
726	27-30	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011; 8/22/2012	PVU
382	115	2/25/2011; 9/29/2011; 8/22/2012	PVU
340	5.52-5.53	2/25/2011	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Google Search	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011; 8/22/2012	PVU
East text search	6/1/2010; 11/9/2010; 2/25/2011; 8/22/2012	PVU
Inventor names search for double patenting issues	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011	PVU
PLUS search	6/1/2010	PVU
Allowable subject matters approved by primary	8/22/2012	PVU

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
713	156,159,186	8/22/2012	PVU
726	27-30	8/22/2012	PVU
382	All	8/22/2012	PVU

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

ORIGINAL		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
713	155	G	0	6	G	21 / 00 ()					

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	182	186			

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

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	13	17												
2	2	14	18												
3	3	15	19												
	4	16	20												
4	5	17	21												
	6		22												
5	7		23												
6	8		24												
7	9		25												
8	10														
	11														
9	12														
10	13														
11	14														
12	15														
	16														

/PHY ANH VU/ Examiner.Art Unit 2437 (Assistant Examiner)	(Date)	**Total Claims Allowed:** 17	
/MATTHEW SMITHERS/ Primary Examiner.Art Unit 2437 (Primary Examiner)	08/24/2012 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 4

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009	06/01/2010	11/08/2010	02/25/2011	09/23/2011	08/22/2012		
1	1	✓	✓	✓	✓	✓	✓	=		
2	2	✓	✓	✓	✓	✓	✓	=		
3	3	✓	✓	✓	✓	✓	✓	=		
	4	✓	-	-	-	-	-	-		
4	5	✓	✓	✓	✓	✓	✓	=		
	6	✓	-	-	-	-	-	-		
5	7	✓	✓	✓	✓	✓	✓	=		
6	8	✓	✓	✓	✓	✓	✓	=		
7	9	✓	✓	✓	✓	✓	✓	=		
8	10	✓	✓	✓	✓	✓	✓	=		
	11	✓	-	-	-	-	-	-		
9	12	✓	✓	✓	✓	✓	✓	=		
10	13	✓	✓	✓	✓	✓	✓	=		
11	14	✓	✓	✓	✓	✓	✓	=		
12	15	✓	✓	✓	✓	✓	✓	=		
	16	✓	-	-	-	-	-	-		
13	17	✓	✓	✓	✓	✓	✓	=		
14	18	✓	✓	✓	✓	✓	✓	=		
15	19	✓	✓	✓	✓	✓	✓	=		
16	20	✓	✓	✓	✓	✓	✓	=		
17	21	✓	✓	✓	✓	✓	✓	=		
	22			✓	✓	✓	✓	-		
	23			✓	✓	✓	✓	-		
	24			✓	✓	✓	✓	-		
	25			✓	✓	✓	✓	-		

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/314,199	12/20/2005	

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 08/28/2012

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 17	Minus	** 21	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

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

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

Legal Instrument Examiner:
/JEFFERY L. OLSEN/

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.

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	6018739	A	2000-01-25	McCOY, Mike et al.	
	2	6983882	B2	2006-01-10	CASSONE, Jean	
	3	7218944	B2	2007-05-15	CROMER, Daryl Carvis et al.	
	4	7715593	B1	2010-05-11	ADAMS, William Mark 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	20020014954	A1	2002-02-07	FITZGIBBON, James J. et al.	
	2	20020140542	A1	2002-10-03	PROKOSKI, Francine et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	3	20020178063	A1	2002-11-28	GRAVELLE, Kelly et al.	
	4	20030172037	A1	2003-09-11	JUNG, Changwoo et al.	
	5	20050251688	A1	2005-11-10	NANAVATI, Samir et al.	
	6	20100117794	A1	2010-05-13	ADAMS, William Mark	
	7	20110126188	A1	2011-05-26	BERNSTEIN, Daniel M. 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	United States Office Action, U.S. Patent Application No. 11/292,330, December 2, 2011, 25 pages.	☐

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	2	United States Office Action, U.S. Patent Application No. 11/745,249, February 2, 2012, 36 pages.	☐
	3	United States Office Action, U.S. Patent Application No. 11/744,832, February 7, 2012, 32 pages.	☐
	4	United States Office Action, U.S. Patent Application No. 11/292,330, April 6, 2012, 22 pages.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John Joseph Giobbi
	Art Unit	2131
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	/Kanda Ishihara/	Date (YYYY-MM-DD)	2012-05-02
Name/Print	Kanda V. Ishihara	Registration Number	56,607

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:	12687966
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	02-MAY-2012
Filing Date:	20-DEC-2005
Time Stamp:	22:59:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	02090US_SB08a.pdf	612989 dd3a3c3b9c0309eca1090e9005fa72830c3906e7	no	5

Warnings:

Information:

2	Non Patent Literature	02007US_NFOA.pdf	2211122 cfb4f56a02d90fcd8877e7f76eb87bc1b7925712	no	36
Warnings:					
Information:					
3	Non Patent Literature	02094US_NFOA.pdf	5564865 ceba4467ab7d44d2b2dc72cf422680353677f08a	no	32
Warnings:					
Information:					
4	Non Patent Literature	02224US_FOA.pdf	3940314 50ac8746b4ef8d7adddde09f4914e96cf69308e40	no	25
Warnings:					
Information:					
5	Non Patent Literature	02224US_NFOA.pdf	3588722 80ffe8aba0c1630316915286d8665ca907642b85	no	22
Warnings:					
Information:					
			Total Files Size (in bytes):	15918012	

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

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

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

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

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

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	11314199
Filing Date	2005-12-20
First Named Inventor	John J. Giobbi
Art Unit	2437
Examiner Name	Phy Anh Vu
Attorney Docket Number	10001-02090 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	20020014954	A1	2002-02-07	FITZGIBBON, James J. et al.	
	2	20020178063	A1	2002-11-28	GRAVELLE, Kelly 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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Vu
	Attorney Docket Number	10001-02090 US

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	United States Office Action, U.S. Patent Application No. 11/292,330, December 2, 2011, 25 pages.	☐
	2	United States Office Action, U.S. Patent Application No. 11/744,831, December 16, 2011, 38 pages.	☐
	3	United States Office Action, U.S. Patent Application No. 11/744,832, February 7, 2012, 32 pages.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Vu
	Attorney Docket Number	10001-02090 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	/Kanda Ishihara/	Date (YYYY-MM-DD)	2012-03-02
Name/Print	Kanda V. Ishihara	Registration Number	56607

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:	12215828
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	02-MAR-2012
Filing Date:	20-DEC-2005
Time Stamp:	19:51:29
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	Non Patent Literature	02224US_FOA.pdf	862101 bad7575321c50df8bf0f4ac590da32992b88b3db	no	25

Warnings:

Information:

2	Non Patent Literature	02094USNFOA.pdf	5572096 f54b2289c1922dce267dcc91387dfa4fb7da46a4	no	32
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	02090SB08A.pdf	612463 6629a7cd842be2a4ab6edb2ab3063debaa4a6095	no	4
Warnings:					
Information:					
4	Non Patent Literature	02092USOA.pdf	6221282 b6eed760a122000c55a2756be88a3f1c58c76099	no	38
Warnings:					
Information:					
			Total Files Size (in bytes):	13267942	

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

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

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

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

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11314199	Filing Date	2005-12-20	Docket Number (if applicable)	10001-02090 US	Art Unit	2437
First Named Inventor	John J. Giobbi			Examiner Name	Phy Anh Tran Vu		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☒ Other Amendment F filed on December 5, 2011

☐ Enclosed

☐ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Kanda Ishihara/	Date (YYYY-MM-DD)	2012-01-05
Name	Kanda V. Ishihara	Registration Number	56607

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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.

Electronic Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Kanda Ishihara/Susanne Lindberg
Attorney Docket Number:	10001-02090 US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	2801	1	465	465
		Total in USD ($)		**465**

Electronic Acknowledgement Receipt

EFS ID:	11771270
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	05-JAN-2012
Filing Date:	20-DEC-2005
Time Stamp:	18:48:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$465
RAM confirmation Number	5366
Deposit Account	
Authorized User	

File Listing:

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

1	Request for Continued Examination (RCE)	02090_US_RCE.pdf	697872 5fdb8fa96e147f8026c8e33ad3fe03501247d6fd	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30282 5abc26c60ea6a2af31c0d962049b6586c04f2127	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	728154	

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/314,199	12/20/2005	

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/05/2012

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

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

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

Legal Instrument Examiner:
/VIOLA ROGERS/

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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

89194 7590 12/30/2011
Patent Law Works/Proxense
165 South Main St
Suite 2
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
12/30/2011	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
kishihara@patentlawworks.net
jnakao@patentlawworks.net

PTOL-90A (Rev. 04/07)

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 11/314,199	**Applicant(s)** GIOBBI, JOHN J.
	Examiner PHY ANH VU	**Art Unit** 2437

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

THE REPLY FILED 05 December 2011 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-3, 5, 7-10, 12-15, and 17-25*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Eleni A Shiferaw/
Supervisory Patent Examiner, Art Unit 2437

/PHY ANH VU/
Examiner, Art Unit 2437

Continuation of 3. NOTE: At least the amendments made in claims 1-3, 5, 7, 8-10, 12-13, 15, 18-19 and 21 raised new issues that require further search and/or consideration.

DO NOT ENTER. PAV
12/22/2011

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090 US

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 Pacific Time Zone of the United States on the local date shown below:
Dated: December 5, 2011 By: /Kanda Ishihara/
Kanda V. Ishihara, Reg. No. 56,607

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

AMENDMENT F

Sir/Madam:

Responsive to the Office Action mailed on October 5, 2011, which sets a shortened statutory period for response that expires on January 5, 2012, please enter the following amendment and consider the following remarks.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090 US

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 Pacific Time Zone of the United States on the local date shown below:

Dated: December 5, 2011 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607

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

AMENDMENT F

Sir/Madam:

Responsive to the Office Action mailed on October 5, 2011, which sets a shortened statutory period for response that expires on January 5, 2012, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the 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 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 data values from the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

responsive to authentication of the one or more codes and other data values [[code]]by the agent, receiving an access message from the agent allowing the user access to an application.

2. (Currently Amended) The method of claim 1, wherein the one or more codes and other data values are ~~code is~~ transmitted to the agent over a network.

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

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

4. (Canceled).

5. (Currently Amended) The method of claim 1, wherein the one or more codes and other data values indicate ~~code indicates~~ that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Currently Amended) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values [[code]]for authentication.

9. (Currently Amended) The method of claim 1, further comprising:

receiving a request for the one or more codes and other data values [[code]]without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values [[code]]without a request for biometric verification, sending the one or more codes and other data values [[code]]without requesting the scan data.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store 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 storage that is unable to be subsequently altered;

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 one or more codes and other data values from the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes

uniquely identifying legitimate integrated devices, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module for receiving an access message from the agent allowing the user access to an application, responsive to the agent authenticating the one or more codes and other data values[[code]].

11. (Canceled).

12. (Currently Amended) The integrated device of claim 10, wherein the one or more codes and other data values are ~~code is~~ transmitted to the agent over a network.

13. (Currently Amended) The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the ~~comprising a~~ device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and other data values [[code]] by the agent, wherein the authentication determines ~~and the authentication determining~~ whether the one or more codes and other data values are ~~code is~~ legitimate;

receiving an access message from the agent; and

in response to a positive access message, allowing the user access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:

registering a date of birth or age with the agent.

18. (Currently Amended) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and other data values [[code]]associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:

a biometric key to store biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending 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 includes the device ID code; and

an authentication module to receive the plurality of codes and other data values and send the plurality of codes and other data values to agent for authentication to determine whether the one or more codes and other data values are ~~code is~~ legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication module receiving an access message from the agent allowing the user to access the application.

20. (Original) The system of claim 19, wherein 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.

21. (Currently Amended) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and other data values[[code]].

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated October 5, 2011 (herein, "OA"). Claims 1-3, 5, 8-10, 12, 13,15, 18, 19 and 21 are amended. Claims 1-3, 5, 7-10, 12-15 and 17-25 are pending upon entry of this amendment.

Response to Claim Objections

Claim 15 is objected to because of the following informality: Claim 15 recites requesting authentication of the code by the agent and the authentication determining whether the code is legitimate." The Examiner, on page 4 of the OA, suggests that claim 15 recite ". . . requesting authentication of the code by the agent and determining whether the code is legitimate." Applicants have amended claim 15 to correct the informalities. Claim 15 now recites, in part, "requesting authentication of the one or more codes and other data values by the agent, wherein the authentication determines whether the one or more codes and other data values are legitimate." The Examiner is, therefore, asked to withdraw the objection to claim 15.

Response to Rejections Under 35 U.S.C. § 112, Second Paragraph

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-3, 5, 7-9, 10, 12-14, 15, and 17-19 are all rejected for reciting "the code" or depending on a claim that recites "the code" when it is unclear which one of the plurality of codes is being referred to. Independent claims 1, 10, 15 and 19 have been amended such that

"one or more codes and data values from the plurality of codes and other data values" are sent for authentication, "wherein the one or more codes and other data values includes the device ID code." All instances of "the code" in the claims have been amended to be either recite the "one or more codes and other data values" or the "device ID code." The Examiner is, therefore, asked to withdraw the 112, second paragraph, rejections of claims 1-3, 5, 7-9, 10, 12-14, 15, and 17-19.

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), Stanko (US 2005/0074126-hereinafter Stanko) and in view of Beenau et al. (US 2004/0230488 A 1-hereinafter Beenau).

As amended, independent claim 1 recites in part:

> persistently storing biometric data of the 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 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; . . .
> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality . . . wherein the one or more codes and other data values includes the device ID code; and
> responsive to authentication of the one or more codes and other data values by the agent, receiving an access message from the agent allowing the user access to an application.

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated

device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, one or more of the plurality of codes and other data values, including a device ID code uniquely identifying the integrated device are wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0007], [0009], [0031], and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on one or more of the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the one or more of the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." The Examiner argues, on pages 2-4 of the OA,

argues that Hsu teaches "persistently storing . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." Specifically, the Examiner argues, on page 2 of the OA, that "tamper proof format" is disclosed:

> In response, Examiner respectfully disagrees. As disclosed, the fob in Hsu is a device that is highly resistant to reverse engineering, cloning and other techniques for tampering (*column 7, lines 63-65*). Therefore, information stored on the fob is tamper-proof, thus cannot be altered. The fob in Hsu stores at least private key of fob and

Respectfully, the Examiner is incorrect. "Highly resistant to . . . tampering" is not the same as "tamper proof" as "proof" by general definition indicates a greater degree of imperviousness than "resistant." Moreover, even assuming a common definition of "highly resistant to tampering" and "tamper proof," Hsu does not suggest or disclose, among other things, that what makes its device highly resistant to tampering is the format in which the information is stored on the device. For example, the high resistance to tampering may merely refer to the fact that the communications to/from the device of Hsu are encrypted thereby making it difficult to clone communications or reverse engineer the contents of the communication. Because Hsu fails to disclose or suggest that the format of the data stored on its device contributes to the device's high resistance to tampering, Hsu fails to disclose or suggest "persistently storing . . . in a tamper proof format" as recited by claim 1.

Neither Stanko nor Beenau remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose storing biometric

information in a tamper proof format. Beenau discloses storing biometric information on the database of a fob, but does not disclose that the biometric information is stored in a tamper proof format. At paragraph [0145] and [0161], Beenau discloses that biometric information can be stored in a secure database 212. At paragraph [0062], Beenau discloses that database 214 may be the same configuration as database 212 and that account data and/or unique fob identification code may be encrypted prior to storage on database 214. However, the fact that database 214 may be similar to database 212 does not mean that database 212 can be similar to database 214 and encrypt prior to storage. Additionally, there is no disclosure or suggestion that biometric information is or can be encrypted prior to storage. Moreover, there is no disclosure or mention that the biometric information is tamper proof in that new biometric information cannot be written or that existing biometric information cannot be modified. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

The Examiner argues on pages 3-4 of the OA:

> In response, Examiner respectfully submits that contrasting to Applicant's argument, column 5, lines 19-29 of Hsu does not disclose the biometric data stored in fob can be altered. On the contrary, column 5 lines 19-29 discloses when a fob is lost or damaged, the enrollment process can be repeated, which means additional fingerprints can be added and enrolled onto a different fob (because the old fob has been lost or damaged, that is, not working anymore). As such, it does not make sense if the enrollment is repeated on a lost or not-working fob. Therefore, Applicant's argument is not persuasive.

Respectfully, the Examiner is incorrect and mischaracterizes the disclosure of Hsu. Column 5, lines19-21 disclose:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For

Hence, Hsu discloses that biometric is **normally** not repeated unless the fob is lost or damaged. Hsu does not disclose or suggest, among other things, that enrollment is **unable** to be repeated absent the loss of or damage to the fob. Hsu discloses a common practice and not a feature/limitation of the technology. For example, the enrollment of Hsu may not **normally** be repeated unless the fob is lost or damaged because an individual's fingerprints remain relatively unchanged for long periods of time eliminating the desire to re-enroll and not because the person is unable to re-enroll biometric information. In fact, the enrollment process of Hsu consists of flipping a switch on the device to an enrollment mode, so there is no indication that this switch cannot be flipped at any point in time allowing the enrollment of additional or other biometric information. Hsu col. 2, lines 10-14. By contrast, the biometric data stored on the Applicant's device is **unable** to be subsequently altered, thereby beneficially increasing security and eliminating the potential for tampering.

Neither Stanko nor Beenau remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose biometric information written to a storage element on the integrated device that is "unable to be subsequently altered." Beenau discloses storing biometric information on the database of a fob, but does not disclose that the database is written to a storage element on the fob that is unable to be subsequently altered. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Applicant's claim 1 is patentable over the cited references for additional reasons. Applicant's invention biometrically verifies the user at the integrated device prior to using a third-party trusted authority to authenticate the integrated device (based on one or more codes and other data values including the device ID code), and, responsive to authentication of the integrated device, allows the user access to an application. The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device.

By contrast, Hsu biometrically verifies the user at the integrated device before generating and encrypting a CRC based on the biometric information. The CRC is used for authentication at a door, which is not a third-party trusted authority, but is more similar to Applicant's "application." In other words, Hsu does not provide two level authentication because Hsu verifies biometric information only (encryption does not verify the integrated device itself) and access is allowed/disallowed by the "door" without using a third-party trusted authority. Applicant's integrated device verifies both biometric data and the integrated device itself, and requires authentication by a third-party trusted authority.

Stanko does not disclose or suggest verifying biometric data and at an integrated device prior to verifying the integrated device. Stanko discloses that an authentication server receives credentials, which may include biometrics, and the authentication server verifies the received credentials. Stanko, therefore, does not disclose verifying an integrated device itself nor does

Stanko disclose verifying biometric information at the integrated device prior to authenticating the integrated device itself at a third-party trusted authority.

Beenau, at paragraph [0081], discloses that a fob's unique identification code is sent to the reader, which authenticates the fob's unique identification code. By contrast, Applicant's invention relies on a third-party trusted authority to verify the device ID. Moreover, Beenau discloses that the fob's unique identification code is sent responsive to an interrogation signal and without prior biometric verification of the user. By contrast, Applicant's invention transmits the device ID code after successful biometric verification. The fob's unique identification code is verified, thereby allowing a user the ability to conduct transactions. Paragraph [0141] discloses that biometric information is used only as a secondary verification to complete transactions. By contrast, Applicant's invention uses the biometric verification as the primary, i.e., the first in time, verification. In paragraph [0141] requiring biometric secondary authentication, access has already been obtained (i.e., to obtain the spending limit) the biometric secondary authentication merely allows the execution of a transaction. By contrast, Applicant's invention requires biometric verification and device verification to precede access.

The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device as recited by claim 1. Therefore, claim one is patentably distinct from the cited references and allowance of claim 1 is requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2,

5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23 depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 18 and 23. Also, claims 20, 21 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20, 21 and 25. Hence, claims 12, 18, 20, 21 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Beenau, Stanko, and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with the 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 5, 2011 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicant
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9835
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

Electronic Acknowledgement Receipt

EFS ID:	11541513
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	05-DEC-2011
Filing Date:	20-DEC-2005
Time Stamp:	14:15:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		02090_US_Amendment_F.pdf	311004 c3d20723876c3dc2d46e6cbafa85a845d125bd66	yes	16

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Copy Claims/Response to Suggested Claims	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	16
Warnings:			
Information:			
	Total Files Size (in bytes):	311004	

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
11/314,199	12/20/2005	☐ To be Mailed

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 12/05/2011

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

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

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

Legal Instrument Examiner:
/DONNA SMALLS LOGAN/

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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090 US	4469

89194 7590 10/05/2011
Patent Law Works/Proxense
165 South Main St
Suite 2
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
10/05/2011	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
gsueoka@patentlawworks.net
kishihara@patentlawworks.net

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *05 July 2011*.

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

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

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

Disposition of Claims

5)☒ Claim(s) *1-3,5,7-10,12-15 and 17-25* 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) *1-3,5,7-10,12-15 and 17-25* is/are rejected.

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

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

Application Papers

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

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/26/2011*.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This office Action is in response to the amendment filed 7/5/2011.

Response to Arguments

Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection.

In addition, to further clarify Examiner's position, Applicants' arguments are addressed below:

On pages 9-11, Applicant argues that the cited references do not disclose or suggest "persistently storing biometric data of the 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 a storage element on the integrated device that is unable to be subsequently altered".

In response, Examiner respectfully disagrees. As disclosed, the fob in Hsu is a device that is highly resistant to reverse engineering, cloning and other techniques for tampering (*column 7, lines 63-65*). Therefore, information stored on the fob is tamper-proof, thus cannot be altered. The fob in Hsu stores at least private key of fob and account number of user (*correspond to plurality of codes*) (*column 5, lines 60-63*; *column 6, lines 35-37; column 7, lines 6-7*), and door's public key (*secret decryption value*) for each use of the door (*column 7, lines 13-16, 47-51*). Public-key cryptography is a cryptographic system requiring two separate keys is well known in the art, where if one key is used to encrypt, then only the other can be used to decrypt. The private key

of the fob uniquely identifies the device because if the fob receives messages encrypted with the fob's public key, then its private key is the only key that can be used to decrypt those messages. Furthermore, as discussed above about Public-key cryptography, in one scenario, a public key can be used as an encryption key, while in another scenario, that same public key can be used as a decryption key. Therefore, the door's public key corresponds to the recited "decryption value". Hsu also discloses the door generates a new public-private key set on every new use of the door (*column 7, lines 13-16*), and transmits the public key to the fob. The purpose of generating a new public key and transmits the new public key to the fob for each transaction is to keep others from predicting or knowing which key is being used for communication between the two parties. Therefore, the public key generated by the door is a secret public key. Thus, for the reasons discussed above, Applicant's argument is not persuasive.

On page 10, Applicant seems to argue that Applicant's invention is patentably distinct from Hsu because in Hsu reference, the stored biometric data can be altered, while the recited limitation in the claim calls for unable to be subsequently altered.

In response, Examiner respectfully submits that contrasting to Applicant's argument, column 5, lines 19-29 of Hsu does not disclose the biometric data stored in fob can be altered. On the contrary, column 5 lines 19-29 discloses when a fob is lost or damaged, the enrollment process can be repeated, which means additional fingerprints can be added and enrolled onto a different fob (because the old fob has been lost or damaged, that is, not working anymore). As such, it does not make sense

if the enrollment is repeated on a lost or not-working fob. Therefore, Applicant's argument is not persuasive.

Additionally, please see the rejection for claim 1 as details below.

Claim Objections

Claim 15 is objected to because of the following informalities:

Claim 15 recites "…requesting authentication of the code by the agent and **the authentication** determining whether the code is legitimate", which should be "…requesting authentication of the code by the agent and determining whether the code is legitimate". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1- are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites "responsive to authentication of **the code** by the agent..." in line 18. With the currently amended claim 1, it is unclear which one of the plurality of codes this limitation is referring to in this limitation.

Claims 2 -3, 5, and 7-9 are rejected for the same rationale as claim 1 above.

Claim 10 recites "...authenticating **the code**" in lines 16-17. It is unclear which one of the plurality of codes is being referred to in this limitation.

Claims 12-14 depend on claim 10, thus inherit the same 35 U.S.C. 112 rejection as their independent claim 10 above.

Claim 15 recites "...whether **the code** is legitimate" in line 10. It is unclear which one of the plurality of codes is being referred to in this limitation.

Claim 17 depend on claim 15, thus inherit the same 35 U.S.C. 112 rejection as their independent claim 15 above.

Claim 18 is rejected for the same rationale as claim 15 above.

Claim 19 recites "…whether the code is legitimate…" in line 12. It is unclear which one of the plurality of codes is being referred to in this limitation.

Claim Rejections - 35 USC § 103

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

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), Stanko (US 2005/0074126-hereinafter Stanko) and in view of Beenau et al. (US 2004/0230488 A1-hereinafter Beenau).

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 of the user and a plurality of codes and other data value comprising a device ID code uniquely identifying the 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 (*Figure 3, element 32; column 4, lines 15-25; column 5, lines 60- column 6, lines 16-24, 35-37; column 7, lines 6-9--wherein fob private key and account number correspond to the recited plurality of codes, and door's public key corresponds to other data value; Column 7, lines 17-34, and 63-65, wherein door public key corresponds to the recited other data value*);

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan (*column 4, lines 40-45, wherein scanned fingerprint is received from the sensor*);

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data (*column 4, lines 40-45; column 5, lines 29-31, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob*);

responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data value for authentication by an agent (*Figure 4, step 60; column 5, lines 60-63; column 6, lines 17-21, 35-37; column 7, lines 20-30, wherein the account number and private key are sent to the door*), that is a third-party trusted authority possessing a list of device ID codes uniquely identifying

legitimate integrated devices (*column 6, lines 10-14, 29-34; column 7, lines 5-6, wherein the door stores users' names and keys*); and

responsive to authentication of the code by the agent, allowing the user access (*column 7, lines 25-34, wherein once the fob's private key has been successfully authenticated by the registered public key, the CRC is retrieved, and access is granted*).

Hsu does not explicitly disclose the other data value being data values, and receiving an access message from the agent.

However, Beenau discloses other data values being data values (*[0155]-[0156], such as fob ID, fob operability information, fob manufacturing information and etc.*)

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the features disclosed by Beenau into the method of Hsu to provide a wide spectrum of identifications of a device to its authorized owner.

Hsu and Beenau do not disclose receiving an access message from the agent.

However, Stanko discloses receiving a grant message from a secure server ([*0055]*).

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

Regarding claim 2, Hsu also discloses wherein the code is transmitted to the agent over a network (*Figure 4, step 60; column 7, lines 24-34, wherein the account number and fob private key are transmitted to the door*).

Regarding claim 5, Hsu also discloses the code indicates that the biometric verification was successful (*column 7, lines 17-34, wherein the fob private key is used as one of the encryption keys when a match is found between the sensed fingerprint image and the reference image*).

Regarding claim 7, Hsu also discloses the biometric data and the scan data are both based on a fingerprint scan by the user (*column 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person*).

Regarding claim 8, Hsu also discloses establishing a secure communication channel prior to sending the code for authentication (*column 6, lines 42-67; column 7, lines 1-34, wherein exchanging of public keys are performed before the private key is sent for authentication*).

Regarding claim 9, Hsu also discloses receiving a request for the code without a request for biometric verification (*column 6, lines 35-41*); 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, lines 60-63; column 6, lines 35-41, wherein account number is transmitted without sensed image*).

Claim 10 is rejected for the same rationale as claim 1 above.

Claim 12 is rejected for the same rationale as claim 2 above.

Regarding claim 15, Hsu discloses a method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user (*column 5, lines 60-64; column 6 line 66-column 7, line 6, wherein fob's public key and account number correspond to the recited plurality of codes; column 7, lines 17-34, and 63-65, wherein door public key corresponds to the recited other data value*), device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices (*column 5, lines 60-64; column 6, lines 10-14, 29-34, and column 7, lines 5-6, wherein users' public keys are registered with the door*);

requesting authentication of the code by the agent and the authentication determining whether the code is legitimate (*column 7, lines 17-30, wherein upon receiving the encrypted CRC, the door determines whether or not the registered public key is legitimate by using to decrypt the encrypted CRC*); and

in response to a positive authentication result, providing access to an application (*column 7, lines 27-34, wherein one the registered public key successfully decrypts the encrypted CRC, user is granted access*).

Hsu does not explicitly disclose the other data value being data values, and receiving an access message from the agent.

However, Beenau discloses other data values being data values (*[0155]-[0156], such as fob ID, fob operability information, fob manufacturing information and etc.*)

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the features disclosed by Beenau into the method of Hsu to provide a wide spectrum of identifications of a device to its authorized owner.

Hsu and Beenau do not disclose receiving an access message from the agent.

However, Stanko discloses receiving a grant message from a secure server ([*0055]*).

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

Regarding claim 18, Hsu also 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, lines 29-34; column 7, lines 5-6*).

Claim 19 is rejected for the same rationale as claims 1 and 10 above.

Regarding claim 20, Hsu also discloses 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 19-25, 40-44*).

Regarding claim 21, Hsu also discloses if the biometric key cannot verify the scan data as being from the user, it does not send the code (*column 5, lines 42-47*).

Regarding claim 22, Hsu also discloses the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition (*column 4, lines 34-39*).

Regarding claim 23, Hsu also discloses the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file (*Figure 4*).

Claim 24 is rejected for the same rationale as claim 22 above.

Claim 25 is rejected for the same rationale as claim 22 above.

Claim Rejections - 35 USC § 103

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

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

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Beenau, Stanko, and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

Regarding claim 3, Hsu, Beenau and Stanko do not discloses registering an age verification for the user in association with the code.

However, Saito discloses registering an age verification for a user in association with a code (*[0082]-[0083][0164], wherein date of birth is registered with along with other personal data*).

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the teachings of Saito into the authentication method of Hsu, Beenau and Stanko in order to enhance the reliability and security of the authentication method.

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

Regarding claim 14, Hsu, Beenau and Stanko do not disclose verification module comprises: an LED to be activated for requesting the biometric scan.

However, Saito discloses a verification module comprises an LED to be activated for requesting the biometric scan (*[0040]-[0056], wherein an LED is used to prompt user for biometric data*).

One of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature of LED into the device of Hsu, Beenau and Stanko to provide a clear indication that a biometric data is required.

Claim 17 is rejected for the same rationale as claim 3 above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

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 7:30-11:30, TH-F 8-4:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eleni Shiferaw can be reached on 571-272-3867. 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 2437
/Eleni A Shiferaw/
Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/314,199	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0230488	11-2004	Beenau et al.	705/018
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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
/P.V./	1	5416780		1995-05-16	Patel	
	2	5894551		1999-04-13	Huggins et al.	
	3	6042006		2000-03-28	Van Tilburg et al.	
	4	6070796		2000-06-06	Sirbu	
	5	6523113		2003-02-18	Wehrenberg	
	6	6850147		2005-02-01	Prokoski et al.	
	7	6873975		2005-03-29	Hatakeyama et al.	
	8	6973576		2005-12-06	Giobbi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

/P.V./	9	7090126		2006-08-15	Kelly et al.	
	10	7137012		2006-11-14	Kamibayashi et al.	
	11	7249177		2007-07-24	Miller	
	12	7305560		2007-12-04	Giobbi	
	13	7574734		2009-08-11	Fedronic 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
/P.V./	1	20020026424		2002-02-28	Akashi	
	2	20020191816		2002-12-19	Maritzen et al.	
	3	20030054868		2003-03-20	Paulsen et al.	
	4	20030055689		2003-03-20	Block et al.	

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

/P.V./	5	20030079133		2003-04-24	Breiter et al.	
	6	20030127511		2003-07-10	Kelly et al.	
	7	20030139190		2003-07-24	Steelberg et al.	
	8	20030176218		2003-09-18	LeMay et al.	
	9	20040215615		2004-10-28	Larsson et al.	
	10	20060022046		2006-02-02	Iwamura	

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]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

/P.V./	1	International Search Report, PCT/US07/11103, April 23, 2008, 9 pages.	☐
	2	International Search Report, PCT/US07/11104, June 26, 2008, 9 pages.	☐
	3	International Search Report, PCT/US07/11102, October 3, 2008, 11 pages.	☐
	4	International Search Report, PCT/US07/11105, October 20, 2008, 10 pages.	☐
	5	"What is a File?", 4/30/1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed 3/11/2010 via http://waybackmachine.org/1 9980615000000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html.	☐

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	09/29/2011

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

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

EFS Web 2.1.17

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
713	155,159,176, 186	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011	PVU
726	27	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011	PVU
382	115	2/25/2011; 9/29/2011	PVU
340	5.52-5.53	2/25/2011	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Google Search	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011	PVU
East text search	6/1/2010; 11/9/2010; 2/25/2011	PVU
Inventor names search for double patenting issues	6/1/2010; 11/9/2010; 2/25/2011; 9/29/2011	PVU
PLUS search	6/1/2010	PVU

INTERFERENCE SEARCH

Class	Subclass	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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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
/P.V./	1	6185316		2001-02-06	Buffam	
	2	6219439		2001-04-17	Burger	
	3	6363485		2002-03-26	Adams 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
/P.V./	1	20020150282		2002-10-17	Kinsella	
/P.V./	2	20020158750		2002-10-31	Almalik	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	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	09/29/2011

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

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

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	77	713/156,159,186.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:43
L2	0	l1 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:44
L3	8	l1 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:44
L4	31	726/27-30.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:46
L5	3	l4 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
L6	41	382/115.ccls. and (fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
L7	4	l6 and @ad<"20011201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/29 10:47
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21

S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02

S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif $6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif $6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S25	5	713/186.ccls. and ((authenticat $4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50
S27	31	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51
S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat $4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17

S31	562	713/186.ccls. and (authenticat $4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat $4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S33	228	713/186.ccls. and (authenticat $4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat $4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat $4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49
S37	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42
S38	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S39	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S40	71	713/176.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S41	0	713/176.ccls. and (biometric$6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S42	52	713/176.ccls. and (biometric$6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S43	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46

S44	102	S43 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S45	9	S43 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48
S46	15	(john near4 giobbi).inv. and (biometric$4 with authenticat $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S47	7	(john near4 giobbi).inv. and (biometric$4 with authenticat $4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S48	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 10:08
S49	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:30
S50	1	"20060143441".pn. and (palm near4 print)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S51	1	"20060143441".pn. and (casino near4 machine)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S52	157	713/155,159.ccls. and (biometric$5) with authenticat $4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:25
S53	121	S52 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:26
S54	192	713/176.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:39
S55	154	S54 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S56	20	S55 and (LED)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40

S57	106	726/27.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S58	75	S57 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S59	9	(giobbi near4 john).in. and ((authenticat$4) and (biometric $6)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:47
S60	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/05 17:51
S61	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 13:21
S62	6719	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
S63	561	S62 and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
S64	248	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4)) and ((authenticat $4) near10 (biometric))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S65	134	S64 and @ad<"20050201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S66	56	713/186.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:01
S67	68	713/176.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:06
S68	86	713/155,159.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S69	80	S68 NOT S67	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11

S70	77	S69 NOT S66	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S71	68	726/27.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:17
S72	68	(john near5 giobbi).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S73	0	(john near5 giobbi).in. and biometri	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S74	31	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:23
S75	1	11/871150	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:43
S76	42	(list near5 code) with ((legitimate or registered) near5 (device or fob or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:50
S77	24	S76 and @ad<"20051220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:51
S78	2	"4993068".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 20:07
S79	26	("4993068" "5917913" "6016476" "6038334" "6121544" "6256737" "7191466" "7529944" "20020023032" "20020138767" "20030036425" "20030046552" "20030054881").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/02/24 20:08
S80	1	713/155,159.ccls. and (device or fob) with (registered or authoriz$7) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:52
S81	9	713/155,159.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:54

S82	17	726/27.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:01
S83	0	726/27.ccls. and (biometric near "10" (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:03
S84	0	726/27.ccls. and (biometric near10 (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S85	0	726/27.ccls. and (biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S86	0	(biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S87	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S88	107	S87 and @ad<"20041220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:05
S89	805	340/5.52-5.53.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S90	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S91	33	S89 and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S92	9	382/115.ccls. and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:40
S93	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
S94	0	713/176.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12

S95	14	713/186.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
S96	16	"380"/$.ccls. and S93	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:15
S97	13	(proxense).as. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:18
S98	5	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 10:45
S99	2	"6185316".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:26
S100	3	"6219439".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:27
S101	2	"6363485".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:28
S102	2	"20020150282".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:29
S103	2	"20020158750".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:33
S104	2	"5416780".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:34
S105	2	"5894551".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:35
S106	2	"6042006".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:35
S107	2	"6070796".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:36

S108	5	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 14:43
S109	1	12/651085	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/16 16:16
S110	377	fob with (stor$3 or contain$3) with (ID or code or account)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:46
S111	29	S110 and "713"/$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:47
S112	0	S111 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:48
S113	19	S111 and @ad<"20051220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/09/21 10:48

9/29/2011 10:49:00 AM
C:\ Documents and Settings\ pvu3\ My Documents\ EAST\ Workspaces\ 11314199.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009	06/01/2010	11/08/2010	02/25/2011	09/23/2011			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	-	-	-	-	-			
	5	✓	✓	✓	✓	✓	✓			
	6	✓	-	-	-	-	-			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	-	-	-	-	-			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓			
	15	✓	✓	✓	✓	✓	✓			
	16	✓	-	-	-	-	-			
	17	✓	✓	✓	✓	✓	✓			
	18	✓	✓	✓	✓	✓	✓			
	19	✓	✓	✓	✓	✓	✓			
	20	✓	✓	✓	✓	✓	✓			
	21	✓	✓	✓	✓	✓	✓			
	22			✓	✓	✓	✓			
	23			✓	✓	✓	✓			
	24			✓	✓	✓	✓			
	25			✓	✓	✓	✓			

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	6185316		2001-02-06	Buffam	
	2	6219439		2001-04-17	Burger	
	3	6363485		2002-03-26	Adams 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	20020150282		2002-10-17	Kinsella	
	2	20020158750		2002-10-31	Almalik	
If you wish to add additional U.S. Published Application citation information please click the Add button.						Add

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button Add								
NON-PATENT LITERATURE DOCUMENTS Remove								
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T[5]
	1							☐
If you wish to add additional non-patent literature document citation information please click the Add button Add								
EXAMINER SIGNATURE								
Examiner Signature						Date Considered		

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	/Kanda Ishihara/	Date (YYYY-MM-DD)	2011-08-26
Name/Print	Kanda V. Ishihara	Registration Number	56,607

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:	10828362
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	26-AUG-2011
Filing Date:	20-DEC-2005
Time Stamp:	19:56:22
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)	02090US_SB08_Cert.pdf	612302 55558bd9763df1c114653b98cbfb7b229225f709	no	4

Warnings:

Information:

Total Files Size (in bytes):	612302

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

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

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

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

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

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	5416780		1995-05-16	Patel	
	2	5894551		1999-04-13	Huggins et al.	
	3	6042006		2000-03-28	Van Tilburg et al.	
	4	6070796		2000-06-06	Sirbu	
	5	6523113		2003-02-18	Wehrenberg	
	6	6850147		2005-02-01	Prokoski et al.	
	7	6873975		2005-03-29	Hatakeyama et al.	
	8	6973576		2005-12-06	Giobbi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	9	7090126		2006-08-15	Kelly et al.	
	10	7137012		2006-11-14	Kamibayashi et al.	
	11	7249177		2007-07-24	Miller	
	12	7305560		2007-12-04	Giobbi	
	13	7574734		2009-08-11	Fedronic 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	20020026424		2002-02-28	Akashi	
	2	20020191816		2002-12-19	Maritzen et al.	
	3	20030054868		2003-03-20	Paulsen et al.	
	4	20030055689		2003-03-20	Block et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	5	20030079133		2003-04-24	Breiter et al.	
	6	20030127511		2003-07-10	Kelly et al.	
	7	20030139190		2003-07-24	Steelberg et al.	
	8	20030176218		2003-09-18	LeMay et al.	
	9	20040215615		2004-10-28	Larsson et al.	
	10	20060022046		2006-02-02	Iwamura	

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]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 US

	1	International Search Report, PCT/US07/11103, April 23, 2008, 9 pages.	☐
	2	International Search Report, PCT/US07/11104, June 26, 2008, 9 pages.	☐
	3	International Search Report, PCT/US07/11102, October 3, 2008, 11 pages.	☐
	4	International Search Report, PCT/US07/11105, October 20, 2008, 10 pages.	☐
	5	"What is a File?", 4/30/1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed 3/11/2010 via http://waybackmachine.org/1 9980615000000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090 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	/Kanda Ishihara/	Date (YYYY-MM-DD)	2011-08-26
Name/Print	Kanda V. Ishihara	Registration Number	56,607

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.

RECEIVED
PATENT DOCKETING

OCT 06 2008

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 Fenwick & West

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 these 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) 272-1618

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.
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.
   ☒ None of the figures

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 1992)

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:

- [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.

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)	Alberto Patron 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:

Form PCT/ISA/237(Box No. I) (April 2007)

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)

	Date of mailing (*day/month/year*)
25000- 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

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	Date of mailing of the international search report
08 April 2008 (08.04.2008)	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:

- [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.

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:

Form PCT/ISA/237(Box No. I) (April 2007)

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]).

Fenwick & West LLP

JUN 3 0 200

RECEIVED

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*) 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 /Tongue 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:

- [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.

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)	/Tangoc 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:
   - [x] the international application in the language in which it was filed
   - [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
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/US07/11104

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 Maritzen to ensure secure authentication of user in order to prevent unauthorized access to secure information.

With respect to claims 2 and 17, Breiter and 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, Breeter 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]).

Form PCT/ISA/237 (Supplemental Box) (April 2007)

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. Maritzen, paragraph, [0056]).

With respect to claims 6 and 21, Breiter and Maritzen disclose the method and apparatus of claims 5 and 16, Breiter and Maritzen 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. Maritzen, 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
25008- 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	

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 Hosuk Song 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.

Form PCT/ISA/210 (continuation of first sheet(3)) (April 2007)

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 douhts 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
30 September 2008 (30.09.2008)

Date of mailing of the international search report
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
FOR FURTHER ACTION	See paragraph 2 below
Applicant's or agent's file reference	11744 PCT

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:

- [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.

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)

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 Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Kanda Ishihara/JoLin Johnson
Attorney Docket Number:	10001-02090 US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	10828409
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090 US
Receipt Date:	26-AUG-2011
Filing Date:	20-DEC-2005
Time Stamp:	20:03:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	5449
Deposit Account	
Authorized User	

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)	02090US_SB08_Fee.pdf	613341 7976a3ff897311df354e2f0c0668623454fe4290	no	6
Warnings:					
Information:					
2	Non Patent Literature	ISR_PCTUS0711102.pdf	2443562 4d98390a940846854778 60dad1c27fac877067ff	no	11
Warnings:					
Information:					
3	Non Patent Literature	ISR_PCTUS0711103.pdf	1220692 0197852c1ef13e5287b02c024b1c75a722878d84	no	9
Warnings:					
Information:					
4	Non Patent Literature	ISR_PCTUS0711104.pdf	1410913 0f5e26f3ae2a4448ab787d8096edc3167a8b0cbf	no	9
Warnings:					
Information:					
5	Non Patent Literature	ISR_PCTUS0711105.pdf	1201510 5fa46d5d4b2405b68f676b50de6bb20b218fe391	no	10
Warnings:					
Information:					
6	Non Patent Literature	What_is_a_File.pdf	48557 35428ab05d98c68a94b0de7292c2ca3be874fe64	no	1
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	29894 ea109ac52ce8f70d0b204d556b92c141aaceb640	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	6968469	

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

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

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

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

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090 US

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 Pacific Time Zone of the United States on the local date shown below:

Dated: July 5, 2011 By: /Kanda Ishihara/

Kanda v. Ishihara, Reg. No. 56,607

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

AMENDMENT E

Sir/Madam:

Responsive to the Office Action mailed on March 2, 2011, which sets a shortened statutory period for response that expires on June 2, 2011. A petition for a one-month extension of time is submitted herewith.

Please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data ~~for~~ of the 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 ~~code~~ in a tamper-~~resistant~~ proof format written to ~~in~~ a storage element on the integrated device ~~that is written once and is not~~ that is unable to be subsequently altered ~~subsequently, wherein the code uniquely identifies the integrated device~~;

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 the plurality of codes and other data values ~~code~~ for authentication ~~to~~by an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices; and

responsive to authentication of the code by the agent, receiving an access message from the agent~~, to allow~~ allowing the user access.

2. (Previously Presented) The method of claim 1, wherein the code is transmitted to the agent over a network.

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

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

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

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.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data ~~for~~ 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 ~~code~~ in a tamper~~-resistant~~ proof format~~, the persistent storage being~~ written ~~once and~~ to the storage that is unable to be subsequently altered ~~being not altered subsequently, wherein the code uniquely identifies the integrated device~~;

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 the plurality of codes and other data values ~~code~~ for authentication ~~to~~ by an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices; and

a radio frequency communication module for receiving an access message from the agent ~~that enables~~ allowing the user access, responsive to the agent authenticating the code.

11. (Canceled).

12. (Previously Presented) The integrated device of claim 10, wherein the code is transmitted to the agent over a network.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value ~~code~~ associated with a biometrically verified user, the ~~code~~ device ID code being registered with an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the code by the agent and the authentication determining whether the code is legitimate;

receiving an access message from the agent; and

in response to a positive ~~the~~ access message~~ being positive~~, ~~providing~~ allowing the user access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:
registering a date of birth or age with the agent.

18. (Original) The method of claim 15, further comprising:
establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:
a biometric key to store biometric data ~~for~~ of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value ~~code~~ in a tamper ~~resistant~~ proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending-the plurality of codes and other data values ~~code, the code being associated with the verified user and uniquely identifying the biometric key~~; and
an authentication module to receive the plurality of codes and other data values ~~code~~ and send the plurality of codes and other data values ~~code~~ to agent for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication module receiving ~~from the agent~~ an access message from the agent ~~to an application to allow~~ allowing the user to access the application.

20. (Original) The system of claim 19, wherein 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.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated March 2, 2011 (herein, "OA"). Claims 1, 10, 15, and 19 are amended herein. No new matter is added in view of the amendments to claims 1, 10, 15, and 19. Claims 1-3, 5, 7-10, 12-15 and 17-25 are pending upon entry of this amendment.

Response to Claim Objections

Claims 1, 10, 15, and 19 were objected to because of the following informalities: Claims 1, 10, 15, and 19 recite "... a third-party trusted authority including a list of codes identifying legitimate integrated devices." The Examiner has suggested that the claims be corrected to recite "... a third-party trusted authority that possess or has a list of codes identifying legitimate integrated devices." Applicants have amended claims 1, 10, 15, and 19 to correct the informalities. The Examiner is asked to withdraw the objection to claims 1, 10, 15, and 19.

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), and in view of Stanko (US 2005/0074126-hereinafter Stanko). This rejection is overcome in view of the amended claims.

As amended, independent claim 1 recites in part:

> persistently storing biometric data of the user <u>and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value</u> in a tamper-proof format written to a storage element on the integrated device <u>that is unable to be subsequently altered</u>;
> 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 the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of the device ID codes uniquely identifying legitimate integrated devices; and

responsive to authentication of the code by the agent, receiving an access message from the agent allowing the user access.

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, the plurality of codes, which comprises a device ID code uniquely identifying the integrated device and a secret decryption value, is wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0007], [0009], [0031], and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal

identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing biometric data of the 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 a storage element on the integrated device that is unable to be subsequently altered."

Hsu merely discloses a fob storing reference biometric data, which may be subsequently altered, and a private encryption key. Hsu col. 1, line 66-col. 2, line 4; col. 2, lines 37-38; col. 2, lines 63-64; col 5, lines 19-21. Hsu stores a reference image upon enrollment that may be altered after enrollment. Hsu col. 5, lines 19-21. However, the claimed invention stores biometric data of the user and a plurality of codes and other data values in a storage element that is unable to be subsequently altered. As Hsu discloses a method allowing subsequent alteration of stored biometric data, Hsu does not disclose "persistently storing biometric data of the user and a plurality of codes and other data values . . . written to a storage element on the integrated device that is unable to be subsequently altered," as claimed.

Column 5, lines 19-29 of Hsu are cited in the OA and disclose:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For additional security and convenience, the user may be asked to enroll two fingerprints, to allow for continued access if the user injures a finger, for example. In a verification mode of operation, the pre-processed fingerprint image is input to the correlator **28**, as indicated by line **43**, where it is compared with the reference image obtained from storage **32** over line **44**. The correlator **28** uses an appropriate technique to

Hence, column 5, lines 19-29 of Hsu discloses storing biometric data during enrollment which "is normally not repeated unless the fob is lost or damaged," but it can be repeated thereby altering the stored biometric data. This is patentably distinct from "storing biometric data of the user and a plurality of codes and other data values . . . written to a storage element on the integrated device that is unable to be subsequently altered," as claimed.

Additionally, Hsu does not disclose or suggest at least an integrated device "storing biometric data of the 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" or "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication," as claimed.

Hsu merely discloses storing a single private key in addition to the biometric data on a fob. Hsu col. 1, lines 66- col. 2, line 4; col. 2 lines 37-38; and col. 2, lines 63-64. As Hsu discloses storing a single private key in addition to biometric data, Hsu does not disclose or suggest storing biometric data and a "plurality of codes and other data values." Furthermore, Hsu does not disclose or suggest "sending the plurality of codes and other data values for authentication," as claimed. Hsu discloses transmitting a cyclic redundancy code (CRC) from a portable device to a door. Hsu, col. 7 lines 17-34. The transmitted CRC, however, identifies a reference fingerprint image not the fob and is generated by the fob rather than stored in the fob.

Hsu, Abstract. Therefore, the CRC is not a code or other data value, as claimed, because it is not stored on the integrated device and is neither a device ID uniquely identifying the device nor a secret decryption value. Hsu discloses a fob with a private key which is neither a device ID nor sent for authentication. Additionally, Hsu does not disclose or suggest that the private key is unique, nor is a private key necessarily unique. Hsu also discloses that the private key is used for encrypting the CRC and not uniquely identifying the fob. Therefore, the private key is not a code or other data value, as claimed, because the private key at least is not sent for authentication, is not necessarily unique, and is not a device ID. As Hsu does not disclose even a single code or other data value, which is stored on an integrated device and sent for authentication as claimed, Hsu fails to disclose or suggest "a plurality of codes and other data values comprising a device ID uniquely identifying an integrated device and a secret decryption value." Therefore, Hsu fails to disclose at least "storing biometric data of the 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" or "sending the plurality of codes and other data values for authentication," as claimed.

Stanko fails to remedy the deficient disclosure of Hsu. Rather, Stanko discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. However, Stanko merely redirects a ticket digitally signed using an authentication server's private key to a secure server that verifies the digital signature to allow access to the secure server. Stanko, ¶ [0055]. Stanko uses authentication of user credentials by one secure server to allow an authenticated user to access additional secure servers without retransmitting the user credentials. Stanko, ¶¶ [0048]-[0050]. Thus, Stanko uses a single set of user credentials for authentication and does not then transmit a plurality of codes and other data

values comprising a device ID code uniquely identifying an integrated device and a secret decryption value to a third-party trusted authority including a list of device ID codes identifying legitimate integrated devices responsive to scan data matching stored biometric data on the integrated device. Hence, Stanko also fails to disclose or suggest "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of the device ID codes uniquely identifying legitimate integrated devices," as claimed.

In addition to failing to disclose or suggest multiple levels of authentication, Stanko fails to disclose or suggest either an integrated device storing a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value or sending the plurality of codes and other data values for authentication. Stanko merely discloses credentials including passwords, challenge-response, digital certificates, tokens, smart cards, or biometrics, or any combination thereof. Stanko ¶ [0047]. These credentials do not disclose a device ID or a secret encryption value. Therefore, Stanko does not disclose or suggest "storing biometric data of the user and a plurality of codes and other data values comprising a device ID code for uniquely identifying the integrated device and a secret decryption value."As Stanko does not disclose an integrated device storing codes and other data values, Stanko does not disclose the integrated device, "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication," as claimed.

Accordingly, the cited references, both alone and in combination, fail to disclose at least the claimed elements of "storing biometric data of the 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" or "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication." Thus, claim 1 is patentably distinct from the cited references, and reconsideration and withdrawal of its rejection is respectfully requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2, 5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23 depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 17, 18 and 23. Also, claims 20 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20 and 25. Hence, claims 12, 18, 20 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13, 14 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hsu and Stanko further in view of U.S. Patent Publication No. 2004/0129787 A1 to Saito et al. ("Saito"). This rejection is overcome in view of the amended claims.

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

Saito fails to remedy the deficient disclosure of Hsu. Rather, Saito discloses a smartcard system for biometric identification using ISO SmartCards. Saito, Abstract. Saito at least fails to at least disclose or suggest storing a plurality of codes and other data values comprising a device ID code uniquely identifying the ISO SmartCard and a secret decryption value in addition to biometric data on an ISO SmartCard. As Saito fails to disclose at least that the ISO SmartCard stores a plurality of codes and other data values, as claimed, it also does not disclose or suggest sending the plurality of codes for authentication. Like Hsu, Saito merely matches captured biometric data against multiple sources and does not also authenticate an integrated device by transmitting a device ID code uniquely identifying the integrated device to "an agent that is a third-party trusted authority possessing a list of device ID codes identifying legitimate integrated devices," as claimed. Saito merely verifies that captured biometric data matches locally stored data and, if the captured biometric data matches locally stored data, verifies that the captured biometric data matches data in a remote authentication system. Saito, ¶ [0008]. While Saito provides that the local match and remote match of the captured biometric data may be different, <u>only</u> biometric data is matched using the different systems. Saito, ¶ [0008]. There is no disclosure or suggestion in Saito of a device ID code uniquely identifying the integrated device or of a trusted-third party authority including a list of device ID codes identifying legitimate integrated devices. Hence, Saito also fails to disclose "responsive to a determination that the

scan data matches the biometric data, wirelessly sending the plurality of codes for authentication to an agent that is a third-party trusted authority possessing a list of device ID codes identifying legitimate integrated devices," as claimed.

Thus, claims 3, 13, 14 and 17 are patentably distinct from the cited references, both alone and in combination, and reconsideration and withdrawal of their rejection is respectfully requested.

CONCLUSION

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

Respectfully submitted,
JOHN J. GIOBBI

Dated: July 5, 2011 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9835
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

PTO/SB/22 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARMENT 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) **FY 2009** (*Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).*)	Docket Number (Optional) 10001-02090 US
Application Number 11/314,199	Filed December 20, 2005
For Biometric Personal Data Key (PDK) Authentication	
Art Unit 2437	Examiner Phy Anh Tran Vu

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	
☑ One month (37 CFR 1.17(a)(1))	$130	$65	$ 65.00
☐ Two months (37 CFR 1.17(a)(2))	$490	$245	$
☐ Three months (37 CFR 1.17(a)(3))	$1110	$555	$
☐ Four months (37 CFR 1.17(a)(4))	$1730	$865	$
☐ Five months (37 CFR 1.17(a)(5))	$2350	$1175	$

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☐ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

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

☑ attorney or agent of record. Registration Number 56,607

☐ attorney or agent under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Kanda Ishihara/	July 5, 2011
Signature	Date
Kanda V. Ishihara	801-258-9820
Typed or printed name	Telephone Number

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

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 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 Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Kanda Ishihara/JoLin Johnson
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**65**

Electronic Acknowledgement Receipt

EFS ID:	10454374
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	05-JUL-2011
Filing Date:	20-DEC-2005
Time Stamp:	18:07:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$65
RAM confirmation Number	5593
Deposit Account	
Authorized User	

File Listing:

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

1		02090US_AmendmentA.pdf	128318 0bf451022db78f54d00bb6e080bd7a7cf84e53f3	yes	16
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment Copy Claims/Response to Suggested Claims		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	16	
Warnings:					
Information:					
2	Extension of Time	02090US_PetitionforExtensionofTime.pdf	312648 7a905cd9ebc9d6985b8fa3cab22d27a92bffa42a	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	29837 58ca053f83e46602715940f45f8ee92f5f02919a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	470803		

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
11/314,199	12/20/2005	☐ To be Mailed

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 07/05/2011	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/PATRICIA LEWIS/

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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090	4469

89194 7590 03/02/2011
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
03/02/2011	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
gsueoka@patentlawworks.net
bbrannon@patentlawworks.net

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *19 January 2011*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-10,12-15 and 17-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-10,12-15, and 17-25* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/20/2010*.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/19/2011 has been entered.

Claim Objections

Claims 1, 10, 15, and 19 are objected to because of the following informalities:

Claims 1, 10, 15, and 19 recite "…a third-party trusted authority including a list of codes identifying legitimate integrated devices". It is suggested that the claims be corrected to recite "…a third-party trusted authority that possess or has a list of codes identifying legitimate integrated devices". Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 1/19/2011 have been fully considered but they are not persuasive.

Regarding claim 1, on pages 8-14, Applicant seems to argue that Hsu does not disclose "responsive to a determination that the scan data matches the biometric data,

wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices".

In response, Examiner respectfully disagrees. As disclosed in the previous Office Action, the fob's private key corresponds to the recited "*code*" that uniquely identifies the integrated device. Furthermore, Examiner respectfully submits that Hsu discloses the person's fingerprint is scanned and is compared with a reference fingerprint image stored in the fob (*Figure 4, step 60*; *Column 4, lines 40-45; Column 5, lines 29-31*). When the comparison results in a match, the fob's private key is used to encrypt the CRC, and the encrypted CRC is transmitted to the door (*agent*) for authentication (*corresponding to sending the code for authentication to an agent*). Hsu also discloses the door (*agent*) has a database which stores fob public encryption keys (*codes*) for each user that has registered to use the door (*Column 6, lines 10-14, 29-34; Column 7, lines 5-6*). The database stores more than one public encryption key, thus the multiple of public encryption keys corresponds to the recited "a list of codes". These public encryption keys are public keys that identify the users' devices that have been registered, thus authorized (*legitimate*). Therefore, contrasting to Applicant's argument, Hsu discloses "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices".

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 103

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

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), and in view of Stanko (US 2005/0074126-hereinafter Stanko).

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 and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device (*Column 4, lines 15-25; Column 6, lines 66- Column 7, lines 13, 56-57; Figure 3,*

element 32, column 5, lines 19-29-wherein fob's private key corresponds to a code that uniquely identifies the integrated device);

responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (*Col 4, lines 40-45, wherein scanned fingerprint is received from the sensor*);

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data (*Column 4, lines 40-45; Column 5, lines 29-31, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob*);

responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority (*Figure 4, step 60; Column 7, lines 20-30, wherein the private key is sent to the door)* including a list of codes identifying legitimate integrated devices (*Column 6, lines 10-14, 29-34; Column 7, lines 5-6*);

responsive to authentication of the code by the agent, allow user access (*Column 7, lines 25-34-wherein once the fob's private key has been successfully authenticated by the registered public key, the CRC is retrieved, and access is granted*)

Hsu does not explicitly disclose receiving an access message from the agent.

However, Stanko discloses receiving a grant message from a secure server (*[0055]*).

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

Regarding claim 2, Hsu also discloses the code is transmitted to the agent over a network (*Figure 4, step 60; Column 7, lines 24-34*).

Regarding claim 5, Hsu also discloses the code indicates that the biometric verification was successful (*Column 5, lines 42-51*).

Regarding claim 7, Hsu also discloses the biometric data and the scan data are both based on a fingerprint scan by the user (*Col 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person*).

Regarding claim 8, Hsu also discloses establishing a secure communication channel prior to sending the code for authentication (*Col 6, lines 42-67; Col 7, lines 1-34, wherein exchanging of keys is performed prior to sending the CRC, which corresponds to establishing a secure communication channel prior to sending the code for authentication*).

Regarding claim 9, Hsu also discloses 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 (*Fig. 4, step 60; Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" encrypted with the door's public key and the fob's private key which corresponds to a "code" is transmitted*).

Claim 10 is rejected for the same rationale as claim 1 above.

Claim 12 is rejected for the same rationale as claim 2 above.

Regarding claim 15, Hsu discloses a method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with an agent, wherein the agent is a third-party trusted authority (*Column 6, line 66-column 7, line 6, wherein the fob's public key corresponds to a code*), including a list of codes identifying legitimate integrated devices (*Column 6, lines 10-14, 29-34; Column 7, lines 5-6*));

requesting authentication of the code by the third-party trusted authority and the authentication determining whether the code is legitimate (*Column 7, lines 17-30, wherein upon receiving CRC which has been encrypted with the fob's private key, the door determines whether or not the registered public key is legitimate by using it to decrypt the encrypted CRC*);

in response to the authentication result being positive, providing access to an application (*Column 7, lines 27-34--wherein once the registered public key successfully decrypts the encrypted CRC, user is granted access*).

Hsu does not explicitly disclose receiving an access message from the agent ;

However, Stanko discloses receiving a grant message from a secure server (*[0055]*).

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

Regarding claim 18, Hsu also 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, lines 29-34; Col 7, lines 5-6*).

Claim 19 is rejected for the same rationale as claims 1 and 10 above.

Regarding claim 20, Hsu also discloses 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 19-25; 40-44*).

Regarding claim 21, Hsu also discloses if the biometric key cannot verify the scan data as being from the user, it does not send the code (*Column 5, lines 42-47,*

wherein the no-match signal is generated, no further processing is performed, thus no CRC will be generated, and available to send).

Regarding claim 22, Hsu also discloses the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition (*Column 4, lines 34-39*).

Regarding claim 23, Hsu also discloses the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file (*Figure 4*).

Claim 24 is rejected for the same rationale as claim 22 above.

Claim 25 is rejected for the same rationale as claim 22 above.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Stanko and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

Regarding claim 3, Hsu does not explicitly disclose registering an age verification for the user in association with the code.

However, Saito discloses registering an age verification for a user in association with a code (*[0082]-[0083][0164], wherein date of birth is registered along with other personal data*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the authentication method of Hsu and Stanko in order to enhance the reliability and security of the authentication.

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

Regarding claim 14, Hsu does not disclose the verification module comprises: an LED to be activated for requesting the biometric scan.

However, Saito discloses the verification module comprises an LED to be activated for requesting the biometric scan (*[0040]-[0056], wherein a LED is used to prompt user for biometric data*).

One or ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature of LED into the system of Hsu to provide a clear indication that a biometric data is required.

Claim 17 is rejected for the same rationale as claim 3 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 7:30-11:30, TH-F 8-4:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009	06/01/2010	11/08/2010	02/25/2011				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	-	-	-	-				
	5	✓	✓	✓	✓	✓				
	6	✓	-	-	-	-				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	-	-	-	-				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	-	-	-	-				
	17	✓	✓	✓	✓	✓				
	18	✓	✓	✓	✓	✓				
	19	✓	✓	✓	✓	✓				
	20	✓	✓	✓	✓	✓				
	21	✓	✓	✓	✓	✓				
	22			✓	✓	✓				
	23			✓	✓	✓				
	24			✓	✓	✓				
	25			✓	✓	✓				

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
713	155,159,176, 186	6/1/2010; 11/9/2010; 2/25/2011	PVU
726	27	6/1/2010; 11/9/2010; 2/25/2011	PVU
382	115	2/25/2011	PVU
340	5.52-5.53	2/25/2011	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Google Search	6/1/2010; 11/9/2010; 2/25/2011	PVU
East text search	6/1/2010; 11/9/2010; 2/25/2011	PVU
Inventor names search for double patenting issues	6/1/2010; 11/9/2010; 2/25/2011	PVU
PLUS search	6/1/2010	PVU

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Web Images Videos Maps News Shopping Gmail more ▾ Scholar Preferences | Sign in

Google scholar biometric fob Search Advanced Scholar Search

Scholar Articles and patents anytime include citations Create email alert

Results **1** - **10** of about **1,450**. (**0.11** sec)

Biometric safeguard method with a **fob**
SW Beenau, DS Bonalle, SW Fields... - US Patent App. 10/ ..., 2004 - Google Patents
US 20040252012A1 (19) United States (12) Patent Application Publication (io> Pub. NO.: US 2004/0252012 Al Beenau et al. (43) Pub. Date: Dec. 16,2004 (54) **BIOMETRIC** SAFEGUARD METHOD WITH A **FOB** (75) Inventors: Blayn W. Beenau, Peoria, AZ (US); David S. **...**
Cited by 25 - Related articles - All 4 versions

Personal identification **fob**
SP Hsu, JM Ling, AF Messenger... - US Patent 6,041,410, 2000 - Google Patents
... door 10. In the presently preferred embodi- ment of the invention, the **fob** 14 or similar portable device includes a **biometric** sensor, which, in the presently preferred embodiment of the invention, is a fingerprint sensor 16. It will **...**
Cited by 105 - Related articles - All 2 versions

Method and system for proffering multiple biometrics for use with a **FOB**
SW Beenau, DS Bonalle, SW Fields ... - US Patent ..., 2008 - Google Patents
Cited by 8 - Related articles - All 4 versions

An introduction evaluating **biometric** systems
PJ Phillips, A Martin, CL Wilson... - Computer, 2002 - ieeexplore.ieee.org
... And a key **fob** sensor must be scratch-, impact-, and spill-resistant. It also must be able to sustain an electrostatic discharge of greater than 25 kV—no small dose of voltage for a chip. **...** Authentec (http://www.authentec.com) makes FingerLoc, a **biometric** identification subsystem. **...**
Cited by 237 - Related articles - BL Direct - All 10 versions

Biometric security using a **fob**
SW Beenau, DS Bonalle, SW Fields... - US Patent ..., 2009 - Google Patents
Cited by 3 - Related articles - All 2 versions

System for **biometric** security using a **FOB**
SW Beenau, DS Bonalle, SW Fields... - US Patent App. 11/ ..., 2007 - Google Patents
US20080008359A1 (19) United States (12) Patent Application Publication GO) Pub. NO.: US 2008/0008359 Al Beenau et al. (43) Pub. Date: Jan. 10,2008 (54) SYSTEM FOR **BIOMETRIC** SECURITY USING A **FOB** (75) Inventors: Blayn W. Beenau, Peoria, AZ (US); David S. **...**
Related articles - All 8 versions

METHOD FOR REGISTERING **BIOMETRIC** FOR USE WITH A **FOB**
SW Beenau, DS Bonalle, SW Fields... - US Patent App. 10/ ..., 2004 - Google Patents
US 20040232224A1 (19) United States (12) Patent Application Publication (io> Pub. NO.: US 2004/0232224 Al Beenau et al. (43) Pub. Date: Nov. 25,2004 (54) METHOD FOR REGISTERING **BIOMETRIC** FOR USE WITH A **FOB** (75) Inventors: Blayn W. Beenau, Peoria, AZ (US); **...**
All 2 versions

SYSTEM FOR **BIOMETRIC** SECURITY USING A **FOB**
SW Beenau, DS Bonalle, SW Fields... - US Patent App. 11/ ..., 2007 - Google Patents
(I9) United States (12) Patent Application Publication Beenau et al. US 20100030633A1 (io) Pub. No.: US 2010/0030633 AI (43) Pub. Date: Feb. 4, 2010 (54) SYSTEM FOR **BIOMETRIC** SECURITY USING A **FOB** (75) Inventors: Blayn W. Beenau, Peoria, AZ (US); David S. **...**

[CITATION] Key **fob** with **biometric** scanner
TE Idsee - US Patent D625,100, 2010 - freepatentsonline.com
BioFob™ Security Device, Wireless **Biometric** Security product information, Sargent Assa Abloy, © 2008 Sargent Manufacturing, 2 pages (reprinted Feb. 25, 2008 from www.sargentlock.com/solutions/biofob/). MicroLatch™ product information, © 2008 Upek, **...**
Cached

Vehicle key **fob** with scanning device and display
CA Tieman, AC Nascimento, VL Brooks... - US Patent App. 12/ ..., 2008 - Google Patents
... [0006] The method also includes the step of capturing bar- code images. [0007] The step of capturing images further includes the step of capturing **biometric** information of a user. [0008] A **fob** for a vehicle remote keyless entry apparatus includes a housing, one or more input **...**
All 2 versions

Create email alert

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

biometric fob Search

Go to Google Home - About Google - About Google Scholar

©2011 Google

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
L2	0	713/176.ccls. and L1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
L3	14	713/186.ccls. and L1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:12
L4	16	"380"/$.ccls. and L1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:15
L5	13	(proxense).as. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 13:18
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21
S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48

S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03

S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif $6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif $6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S25	5	713/186.ccls. and ((authenticat $4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50
S27	31	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51
S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat $4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S31	562	713/186.ccls. and (authenticat $4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat $4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17

S33	228	713/186.ccls. and (authenticat $4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat $4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat $4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49
S37	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42
S38	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S39	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S40	71	713/176.ccls. and (biometric $6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S41	0	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S42	52	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S43	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S44	102	S43 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S45	9	S43 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48

S46	15	(john near4 giobbi).inv. and (biometric$4 with authenticat $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S47	7	(john near4 giobbi).inv. and (biometric$4 with authenticat $4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S48	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 10:08
S49	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:30
S50	1	"20060143441".pn. and (palm near4 print)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S51	1	"20060143441".pn. and (casino near4 machine)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S52	157	713/155,159.ccls. and (biometric$5) with authenticat $4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:25
S53	121	S52 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:26
S54	192	713/176.ccls. and (biometric $5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:39
S55	154	S54 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S56	20	S55 and (LED)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S57	106	726/27.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S58	75	S57 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44

S59	9	(giobbi near4 john).in. and ((authenticat$4) and (biometric $6)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:47
S60	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/05 17:51
S61	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 13:21
S62	6719	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
S63	561	S62 and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
S64	248	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4)) and ((authenticat $4) near10 (biometric))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S65	134	S64 and @ad<"20050201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
S66	56	713/186.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:01
S67	68	713/176.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:06
S68	86	713/155,159.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S69	80	S68 NOT S67	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S70	77	S69 NOT S66	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
S71	68	726/27.ccls. and S62	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:17

S72	68	(john near5 giobbi).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S73	0	(john near5 giobbi).in. and biometri	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
S74	31	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:23
S75	1	11/871150	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:43
S76	42	(list near5 code) with ((legitimate or registered) near5 (device or fob or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:50
S77	24	S76 and @ad<"20051220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 18:51
S78	2	"4993068".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/24 20:07
S79	26	("4993068" "5917913" "6016476" "6038334" "6121544" "6256737" "7191466" "7529944" "20020023032" "20020138767" "20030036425" "20030046552" "20030054881").pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	OR	ON	2011/02/24 20:08
S80	1	713/155,159.ccls. and (device or fob) with (registered or authoriz$7) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:52
S81	9	713/155,159.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 10:54
S82	17	726/27.ccls. and (device or fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:01
S83	0	726/27.ccls. and (biometric near "10" (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:03

S84	0	726/27.ccls. and (biometric near10 (device or fob)) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S85	0	726/27.ccls. and (biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S86	0	(biometric near10 fob) same (list near4 code)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S87	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:04
S88	107	S87 and @ad<"20041220"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:05
S89	805	340/5.52-5.53.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S90	436	(biometric near10 fob)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S91	33	S89 and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:35
S92	9	382/115.ccls. and S90	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2011/02/25 11:40

2/25/2011 1:21:00 PM
C:\Documents and Settings\pvu3\My Documents\EAST\Workspaces\11314199.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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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
/P.V./	1	4993068		1991-02-12	Piosenka et al.	
/P.V./	2	5917913		1999-06-29	Wang	
/P.V./	3	6016476		2000-01-18	Maes et al.	
/P.V./	4	6038334		2000-03-14	Hamid	
/P.V./	5	6121544		2000-09-19	Petsinger	
/P.V./	6	6256737		2001-07-03	Bianco et al.	
/P.V./	7	7191466		2007-03-13	Hamid et al.	
/P.V./	8	7529944		2009-05-05	Hamid	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020023032		2002-02-21	Pearson et al.	
/P.V./	2	20020138767		2002-09-26	Hamid et al.	
/P.V./	3	20030036425		2003-02-20	Kaminkow et al.	
/P.V./	4	20030046552		2003-03-06	Hamid	
/P.V./	5	20030054881		2003-03-20	Hedrick 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]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

/P.V./	1	United States Office Action, U.S. Patent Application No. 11,744,831, September 3, 2010, 27 pages.	☐

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	02/25/2011

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

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

EFS Web 2.1.17

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/314,199	Filing Date	2005-12-20	Docket Number (if applicable)	10001-02090	Art Unit	2437
First Named Inventor	John J. Giobbi			Examiner Name	Phy Anh Tran Vu		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☒ Other Amendment D filed on January 3, 2011

☐ Enclosed

- ☐ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2011-01-19
Name	Brian G. Brannon	Registration Number	57219

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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.

Electronic Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Brian Gregory Brannon/Connie Evenich
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**405**

Electronic Acknowledgement Receipt

EFS ID:	9259671
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	19-JAN-2011
Filing Date:	20-DEC-2005
Time Stamp:	19:03:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$405
RAM confirmation Number	5439
Deposit Account	
Authorized User	

File Listing:

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

1	Request for Continued Examination (RCE)	02090_RCE.pdf	697865 8c1d3f620060771523c7aa796aad48082550d51f	no	3
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30105 07a1a8e65303de4595c18bd707c5f1158184fac9	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	727970	

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
11/314,199	12/20/2005	☐ To be Mailed

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/19/2011

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

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

Legal Instrument Examiner:
/FRANCES Y. FIELDS/

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.
11/314,199	12/20/2005	John J. Giobbi	10001-02090	4469

89194 7590 01/18/2011
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
01/18/2011	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
gsueoka@patentlawworks.net
bbrannon@patentlawworks.net

PTOL-90A (Rev. 04/07)

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 11/314,199	**Applicant(s)** GIOBBI, JOHN J.	
	Examiner PHY ANH VU	**Art Unit** 2437	

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

THE REPLY FILED 03 January 2011 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-3, 5, 7-10, 12-15, and 17-25*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/PHY ANH VU/
Examiner, Art Unit 2437

Continuation of 3. NOTE: The newly added limitations to claims 1, 10, 15, and 19 raise new issues and need further search and/or consideration.

DO NOT ENTER: /P.V./
01/12/2011

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 Eastern Time Zone of the United States on the local date shown below:

Dated: January 3, 2011 By: /Brian G. Brannon/
Brian G. Brannon, Reg. No. 57,219

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

AMENDMENT D

Sir/Madam:

Responsive to the Office Action mailed on November 22, 2010, which sets a shortened statutory period for response that expires on February 22, 2011, please enter the following amendment and consider the following remarks.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 Eastern Time Zone of the United States on the local date shown below:

Dated: January 3, 2011 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

AMENDMENT D

Sir/Madam:

Responsive to the Office Action mailed on November 22, 2010, which sets a shortened statutory period for response that expires on February 22, 2011, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below. Please amend claims 1, 10, 15 and 19 as indicated herein.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;

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 the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>; and

responsive to authentication of the code <u>by the agent</u>, receiving an access message from the agent, to allow user access.

2. (Previously Presented) The method of claim 1, wherein the code is transmitted to the agent over a network.

3. (Original) The method of claim 1, further comprising:
registering an age verification for the user in association with the code.

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

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.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user and a code in a tamper-resistant format, the persistent storage being written once and being not altered subsequently, wherein the code uniquely identifies the integrated device;

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 the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices; and</u>

<u>a radio frequency communication module for receiving</u> ~~wherein responsive to authentication of the code, the agent transmits~~ an access message <u>from the</u>

agent that enables user access, responsive to the agent authenticating the code.

11. (Canceled).

12. (Previously Presented) The integrated device of claim 10, wherein the code is transmitted to the agent over a network.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices;

requesting authentication of the code by the agent and the authentication determining whether the code is legitimate;

receiving an access message from the agent; and

in response to the access message being positive, providing access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:

registering a date of birth or age with the agent.

18. (Original) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:

a biometric key to store biometric data for a user and a code 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 the code, the code being associated with the verified user and uniquely identifying the biometric key; and

an authentication module to receive the code and send the code to agent for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>, and responsive to the code being authenticated, the <u>authentication module receiving from the agent</u> ~~agent sending~~ an access message to an application to allow the user to access the application.

20. (Original) The system of claim 19, wherein 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.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated November 22, 2010 (herein, "OA"). Claims 1, 10, 15 and 19 are amended herein.

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,041,410 A1 to Hsu et al. ("Hsu") in view of U.S. Patent Publication No. 2005/0074126 to Stanko ("Stanko"). This rejection is overcome in view of the amended claims.

As amended, independent claim 1 recites in part:

> persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;
> 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 the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>; and
> responsive to to authentication of the code <u>by the agent</u>, receiving an access message from the agent, to allow user access. (emphasis added)

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data for a user and a code that uniquely identifies the integrated device in a storage element on the

integrated device. The code and biometric data are written once to the storage element and the storage element is not subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, the code, which uniquely identifies the integrated device, is wirelessly transmitted to an agent that is a third party trusted authority including a list of codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0038], [0039], [0042], [0043], [0049] and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating the code uniquely identifying the integrated device, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the code, the claimed invention beneficially prevents unauthorized user of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "responsive to a determination that the scan data matches the biometric data, wirelessly

sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices."

Hsu merely discloses a system and method for verifying the identity of a person seeking to access a protected property. Hsu, 1:50-53. To verify identify, Hsu transmits data between a user's handheld device and a door. Hsu, Figure 1; 4:15-25. However, while the claimed invention determines that scan data matches biometric data then sends the code uniquely identifying the integrated device for authentication to a third-party trusted authority including a list of codes identifying legitimate integrated devices, Hsu at most transmits a cyclic redundancy code (CRC) from a portable device to a door. Hsu, 7:17-34. The transmitted CRC, however, identifies a reference fingerprint image and does not identify the user's handheld device. Hsu does not disclose any additional data, such as a code, that uniquely identifies an integrated device. As Hsu only discloses data identifying the reference fingerprint image and does not disclose or suggest a code uniquely identifying an integrated device, Hsu does not disclose "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Figure 4 and column 7, lines 20-30 of Hsu are cited in the OA and disclose:

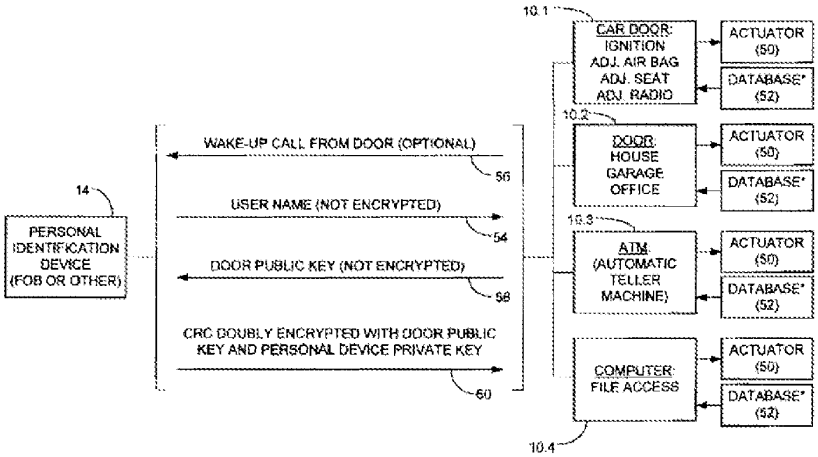


FIG. 4

without encryption, as indicated by line **58**. Then, if the fob **14** has validated the user's identification by successfully matching the sensed fingerprint image with the reference image, the fob performs two levels of encryption on the CRC that is generated. First, the encryption logic **34** in the fob **14** encrypts the CRC using the door's public key. Then the resulting encrypted CRC is doubly encrypted using the fob's private key. The doubly encrypted CRC is transmitted to the door **10**, where it is decrypted using the fob's public key and then using the door's private key to recover the CRC. The door **10** then compares this CRC with the CRC in

Hence, Figure 4 of Hsu merely discloses that the CRC is encrypted with the door's public key and the personal device's private key and the doubly-encrypted CRC is transmitted to the door. However, as depicted by Figure 4, the door does not include "a list of codes identifying legitimate integrated devices," but merely includes <u>user-specific</u> data such as names, public keys and CRCs. No device-specific data is maintained by the door, much less "a list of codes identifying legitimate integrated devices," as claimed. Similarly, column 7, lines 20-30 of Hsu disclose doubly encrypting the CRC and transmitting the doubly-encrypted CRC from the fob to the door. After decrypting the doubly-encrypted CRC, the door compares the CRC with stored CRCs. However, column 7, lines 20-30 of Hsu, and the remaining disclosure of Hsu, do not disclose or suggest that the door

includes "a list of codes identifying legitimate integrated devices," so there is consequently no disclosure of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

While the claimed invention both determines whether scan data matches persistently stored biometric data and authenticates a code uniquely identifying the integrated device using a third-party trusted authority including a list of codes identifying legitimate integrated devices, Hsu merely verifies whether a CRC identifying a fingerprint matches a stored CRC. Hence, Hsu merely verifies biometric data against two sources of stored biometric data and does not authenticate an integrated device by transmitting a code uniquely identifying the integrated device to an agent that "is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Stanko fails to remedy the deficient disclosure of Hsu. Rather, Stanko discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. However, Stanko merely redirects a ticket digitally signed using an authentication server's private key to a secure server that verifies the digital signature to allow access to the secure server. Stanko, ¶ [0055]. Stanko uses authentication of user credentials by one secure server to allow an authenticated user to access additional secure servers without retransmitting the user credentials. Stanko, ¶¶ [0048]-[0050]. Thus, Stanko uses a single set of user credentials for authentication and does not then transmit a code uniquely identifying an integrated device to a third-party

trusted authority including a list of codes identifying legitimate integrated devices responsive to scan data matching stored biometric data. Hence, Stanko also fails to disclose or suggest "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Accordingly, the cited references, both alone and in combination, fail to disclose at least the claimed element of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices." Thus, claim 1 is patentably distinct from the cited references, and reconsideration and withdrawal of its rejection is respectfully requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2, 5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23

depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 17, 18 and 23. Also, claims 20 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20 and 25. Hence, claims 12, 18, 20 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13, 14 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hsu and Stanko further in view of U.S. Patent Publication No. 2004/0129787 A1 to Saito et al. ("Saito"). This rejection is overcome in view of the amended claims.

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

Saito fails to remedy the deficient disclosure of Hsu. Rather, Saito discloses a smartcard system for biometric identification. Saito, Abstract. Like Hsu, Saito merely matches captured biometric data against multiple sources and does not also authenticate an integrated device by transmitting a code uniquely identifying the integrated device to an agent that "is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed. Saito merely verifies that captured biometric data matches locally stored data and, if the captured biometric data matches locally stored

data, verifies that the captured biometric data matches data in a remote authentication system. Saito, ¶ [0008]. While Saito provides that the local match and remote match of the captured biometric data may be different, only biometric data is matched using the different systems. Saito, ¶ [0008]. There is no disclosure or suggestion in Saito of a code uniquely identifying the integrated device or of a trusted-third party authority including a list of codes identifying legitimate integrated devices. Hence, Saito also fails to disclose "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Thus, claims 3, 13, 14 and 17 are patentably distinct from the cited references, both alone and in combination, and reconsideration and withdrawal of their rejection is respectfully requested.

CONCLUSION

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

Respectfully submitted,
JOHN J. GIOBBI

Dated: January 3, 2011 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

Electronic Acknowledgement Receipt

EFS ID:	9149195
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	03-JAN-2011
Filing Date:	20-DEC-2005
Time Stamp:	12:17:15
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		2090_Amendment_D.pdf	146616 b2581370a566bfe92bf2226fdb137e3e8aa4e323	yes	15

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	15
Warnings:			
Information:			
	Total Files Size (in bytes):	146616	

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/314,199	12/20/2005	

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/03/2011

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

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

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

Legal Instrument Examiner:
/FRANCES Y. FIELDS/

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.

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	4993068		1991-02-12	Piosenka et al.	
	2	5917913		1999-06-29	Wang	
	3	6016476		2000-01-18	Maes et al.	
	4	6038334		2000-03-14	Hamid	
	5	6121544		2000-09-19	Petsinger	
	6	6256737		2001-07-03	Bianco et al.	
	7	7191466		2007-03-13	Hamid et al.	
	8	7529944		2009-05-05	Hamid	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020023032		2002-02-21	Pearson et al.	
	2	20020138767		2002-09-26	Hamid et al.	
	3	20030036425		2003-02-20	Kaminkow et al.	
	4	20030046552		2003-03-06	Hamid	
	5	20030054881		2003-03-20	Hedrick 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]

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1	United States Office Action, U.S. Patent Application No. 11,744,831, September 3, 2010, 27 pages.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

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

Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2010-12-20
Name/Print	Brian G. Brannon	Registration Number	57,219

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 Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Brian Gregory Brannon/Connie Evenich
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	9077397
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	20-DEC-2010
Filing Date:	20-DEC-2005
Time Stamp:	18:37:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	6293
Deposit Account	
Authorized User	

File Listing:

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

1	Transmittal Letter	02090_SIDS.pdf	75991 d183ce74e2bcb543306ed3c2aab17eee55c0502e	no	4
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	02090_SB08a.pdf	612807 671c2db0d9a0086b579cdee2a05e952c98433702	no	5
Warnings:					
Information:					
3	NPL Documents	11744831_Office_Action.pdf	1005357 12d3ee58da20341f54a73f0bda4fb775a56579c4	no	27
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	30033 a8c3e92aac4e1e11ce4970cd97b529e6b7514cf0	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1724188	

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

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

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

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

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 Pacific Time Zone of the United States on the local date shown below:

Dated: December 20, 2010 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☒ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a

notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:

☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;

☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☒ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in

37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 20, 2010

By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	10001-02090	4469

89194 7590 11/22/2010
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
11/22/2010	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
gsueoka@patentlawworks.net
bbrannon@patentlawworks.net

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *07 September 2010*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-10,12-15 and 17-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-10,12-15, and 17-25* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/2/2010;9/3/2010;9/28/2010;9/30/2010;10/13/2010*.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This application is in response to the amendment filed 9/7/2010.

Response to Arguments

Applicant's arguments with respect to claims 1, 10, 15 and 19 have been considered but are moot in view of the new ground(s) of rejection.

Furthermore,

Regarding claim 1, on page 8, Applicant argues that “the cited references do not disclose or suggest persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device, sending the code for authentication to an agent, and responsive to authentication of the code, receiving an access message from the agent to allow user access."

In response, Examiner respectfully disagrees. Examiner respectfully submits that Hsu discloses the fob has a public-private key pair, the public key is registered with each door (C*olumn 6, line 66-column 7, line 11*). The private key (code) is stored in the fob preferably in a form in which it cannot be discerned by inspection or reverse engineering (*corresponding to a code in a tamper-resistant format in a storage element on the integrated device*) (*Column 7, lines 6-9*). The fob's private key is used to encrypt the CRC, and is transmitted to the door for authentication (*corresponding to sending the code for authentication to an agent*) (*Figure 4, step 60*), and when the encrypted CRC is received at the door, the door uses the fob's public key which was registered to decrypt (*authenticate*) the fob’s private key to retrieve the CRC. As disclosed by Hsu, the CRC is only generated if there is a match between the sensed fingerprint image with the

reference image (*Column 5, lines 19-47*). Thus, the generated CRC will match with the stored CRC. Therefore, upon successfully authenticated the fob's private key, access will be granted to user (corresponds to responsive to authentication of the code, allow user access)(*Column 7, lines 25-34*).

Claims 10, 15, and 15 are rejected for the same rationale as claim 1 above.

Claims 2-3, 5-10, 12-14, 17-18, and 20-25, see discussions of the independent claims above.

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 103

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

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), and in view of Stanko (US 2005/0074126-hereinafter Stanko).

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 and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device (*Column 4, lines 15-25; Column 6, lines 66- Column 7, lines 13, 56-57; Figure 3, element 32, column 5, lines 19-29-wherein fob's private key corresponds to a code that uniquely identifies the integrated device*);

responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (*Col 4, lines 40-45, wherein scanned fingerprint is received from the sensor*);

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data (*Column 4, lines 40-45; Column 5, lines 29-31, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob*);

responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority (*Figure 4, step 60; Column 7, lines 20-30, wherein the private key is sent to the door)* and

responsive to authentication of the code, allow user access (*Column 7, lines 25-34-wherein once the fob's private key has been successfully authenticated by the registered public key, the CRC is retrieved, and access is granted*)

Hsu does not explicitly disclose receiving an access message from the agent.

However, Stanko discloses receiving a grant message from a secure server (*[0055]*).

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

Regarding claim 2, Hsu also discloses the code is transmitted to the agent over a network (*Figure 4, step 60; Column 7, lines 24-34*).

Regarding claim 5, Hsu also discloses the code indicates that the biometric verification was successful (*Column 5, lines 42-51*).

Regarding claim 7, Hsu also discloses the biometric data and the scan data are both based on a fingerprint scan by the user (*Col 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person*).

Regarding claim 8, Hsu also discloses establishing a secure communication channel prior to sending the code for authentication (*Col 6, lines 42-67; Col 7, lines 1-*

34, wherein exchanging of keys is performed prior to sending the CRC, which corresponds to establishing a secure communication channel prior to sending the code for authentication).

Regarding claim 9, Hsu also discloses 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 (*Fig. 4, step 60; Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" encrypted with the door's public key and the fob's private key which corresponds to a "code" is transmitted*).

Claim 10 is rejected for the same rationale as claim 1 above.

Claim 12 is rejected for the same rationale as claim 2 above.

Regarding claim 15, Hsu discloses a method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with an agent, wherein the agent is a third-party trusted authority (*Column 6, line 66-column 7, line 6, wherein the fob's public key corresponds to a code*);

requesting authentication of the code by the third-party trusted authority and the authentication determining whether the code is legitimate (*Column 7, lines 17-30, wherein upon receiving CRC which has been encrypted with the fob's private key, the*

door determines whether or not the registered public key is legitimate by using it to decrypt the encrypted CRC);

in response to the authentication result being positive, providing access to an application (*Column 7, lines 27-34--wherein once the registered public key successfully decrypts the encrypted CRC, user is granted access*).

Hsu does not explicitly disclose receiving an access message from the agent ;

However, Stanko discloses receiving a grant message from a secure server (*[0055]*).

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

Regarding claim 18, Hsu also 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, lines 29-34; Col 7, lines 5-6*).

Claim 19 is rejected for the same rationale as claims 1 and 10 above.

Regarding claim 20, Hsu also discloses 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 19-25; 40-44*).

Regarding claim 21, Hsu also discloses if the biometric key cannot verify the scan data as being from the user, it does not send the code (*Column 5, lines 42-47, wherein the no-match signal is generated, no further processing is performed, thus no CRC will be generated, and available to send*).

Regarding claim 22, Hsu also discloses the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition (*Column 4, lines 34-39*).

Regarding claim 23, Hsu also discloses the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file (*Figure 4*).

Claim 24 is rejected for the same rationale as claim 22 above.

Claim 25 is rejected for the same rationale as claim 22 above.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Stanko and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

Regarding claim 3, Hsu does not explicitly disclose registering an age verification for the user in association with the code.

However, Saito discloses registering an age verification for a user in association with a code (*[0082]-[0083][0164], wherein date of birth is registered along with other personal data*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the authentication method of Hsu and Stanko in order to enhance the reliability and security of the authentication.

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

Regarding claim 14, Hsu does not disclose the verification module comprises: an LED to be activated for requesting the biometric scan.

However, Saito discloses the verification module comprises an LED to be activated for requesting the biometric scan (*[0040]-[0056], wherein a LED is used to prompt user for biometric data*).

One or ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature of LED into the system of Hsu to provide a clear indication that a biometric data is required.

Claim 17 is rejected for the same rationale as claim 3 above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

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 Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/314,199	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0074126	04-2005	Stanko, Joseph A.	380/279
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009	06/01/2010	11/08/2010					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	-	-	-					
	5	✓	✓	✓	✓					
	6	✓	-	-	-					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	-	-	-					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	-	-	-					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					
	21	✓	✓	✓	✓					
	22			✓	✓					
	23			✓	✓					
	24			✓	✓					
	25			✓	✓					

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
713	155,159,176	6/1/2010; 11/9/2010	PVU
726	27	6/1/2010; 11/9/2010	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Google Search	6/1/2010; 11/9/2010	PVU
East text search	6/1/2010; 11/9/2010	PVU
Inventor names search for double patenting issues	6/1/2010; 11/9/2010	PVU
PLUS search	6/1/2010	PVU

INTERFERENCE SEARCH

Class	Subclass	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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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
/P.V./	1	6709333		2004-03-23	Bradford et al.	
/P.V./	2	7112138		2006-09-26	Hedrick 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
/P.V./	1	20030186739		2003-10-02	Paulsen et al.	
/P.V./	2	20040127277		2004-07-01	Walker et al.	
/P.V./	3	20040209692		2004-10-21	Schober 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	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	11/08/2010

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	11314199
	Filing Date	2007-05-05
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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
/P.V./	1	7644443		2010-01-05	Matsuyama 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
/P.V./	1	20050229007		2005-10-13	Bolle 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2007-05-05
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	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	11/08/2010

*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
L1	6719	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
L2	561	l1 and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:56
L3	248	(transmit$4 or send$4) near10 (access near5 (grant$4 or permit$4)) and ((authenticat $4) near10 (biometric))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
L4	134	l3 and @ad<"20050201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 15:57
L5	56	713/186.ccls. and l1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:01
L6	68	713/176.ccls. and l1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:06
L7	86	713/155,159.ccls. and l1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
L8	80	l7 NOT l6	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
L9	77	l8 NOT l5	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:11
L10	68	726/27.ccls. and l1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:17
L11	68	(john near5 giobbi).in.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22

L12	0	(john near5 giobbi).in. and biometri	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:22
L13	31	(john near5 giobbi).in. and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 17:23
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21
S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51

S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif $6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif $6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07

S25	5	713/186.ccls. and ((authenticat $4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50
S27	31	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51
S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat $4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S31	562	713/186.ccls. and (authenticat $4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat $4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S33	228	713/186.ccls. and (authenticat $4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat $4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat $4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49
S37	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42

S38	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S39	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S40	71	713/176.ccls. and (biometric $6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S41	0	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S42	52	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S43	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S44	102	S43 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S45	9	S43 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48
S46	15	(john near4 giobbi).inv. and (biometric$4 with authenticat $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S47	7	(john near4 giobbi).inv. and (biometric$4 with authenticat $4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S48	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 10:08
S49	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:30
S50	1	"20060143441".pn. and (palm near4 print)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31

S51	1	"20060143441".pn. and (casino near4 machine)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S52	157	713/155,159.ccls. and (biometric$5) with authenticat $4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:25
S53	121	S52 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:26
S54	192	713/176.ccls. and (biometric $5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:39
S55	154	S54 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S56	20	S55 and (LED)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S57	106	726/27.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S58	75	S57 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S59	9	(giobbi near4 john).in. and ((authenticat$4) and (biometric $6)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:47
S60	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/05 17:51
S61	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/11/08 13:21

11/8/2010 5:26:26 PM
C:\Documents and Settings\pvu3\My Documents\EAST\Workspaces\11314199.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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20090328182		2009-12-31	Malakapalli 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

/P.V./	1	Non-Final Office Action, U.S. Patent Application No. 11/292,330, Dated: September 16, 2010, 23 pages.	☐

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	11/08/2010

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020104006		2002-08-01	Boate 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	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	11/08/2010

*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.

EFS Web 2.1.17

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020144117		2002-10-03	Faigle	

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

FOREIGN PATENT DOCUMENTS Remove

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	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	11/08/2010

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

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

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

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020144117		2002-10-03	Faigle	

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

FOREIGN PATENT DOCUMENTS Remove

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1		☐

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

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ None

SIGNATURE

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

Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2010-10-13
Name/Print	Brian G. Brannon	Registration Number	57,219

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:	8621822
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	13-OCT-2010
Filing Date:	20-DEC-2005
Time Stamp:	20:15:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	02090_SIDS.pdf	75992 7e611427dec14b404714ce0fb37aad99387e38ec	no	4

Warnings:

Information:

2	Information Disclosure Statement (IDS) Filed (SB/08)	02090_SB08a.pdf	612141 d13f7e3f3f4bccffe6c54c098e3b012eaa6d76c1	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	688133		

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

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

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

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

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 Pacific Time Zone of the United States on the local date shown below:

Dated: October 13, 2010 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☒ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☒ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a

notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND
- ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in

37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,
JOHN J. GIOBBI

Dated: October 13, 2010

By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20020104006		2002-08-01	Boate 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1		☐

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

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

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

Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2010-09-30
Name/Print	Brian G. Brannon	Registration Number	57219

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 Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Brian Gregory Brannon/Connie Evenich
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	8536514
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	30-SEP-2010
Filing Date:	20-DEC-2005
Time Stamp:	16:30:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	6319
Deposit Account	
Authorized User	

File Listing:

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

1	Transmittal Letter	02090_IDS.pdf	75596 644ca2419f0ced8b0c9cd345dd978f477048518d	no	4
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	02090_SB08a.pdf	612073 6242e6c45209c262314c54608be7761cebf2eaf9	no	4
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30032 233933fa95a8e89742378b48970d372922e3be43	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	717701	

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

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

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

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

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 30, 2010 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☒ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a

notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND
- ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in

37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,

Dated: September 30, 2010

By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	20090328182		2009-12-31	Malakapalli 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1	Non-Final Office Action, U.S. Patent Application No. 11/292,330, Dated: September 16, 2010, 23 pages.	☐

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ None

SIGNATURE

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

Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2010-09-28
Name/Print	Brian G. Brannon	Registration Number	57,219

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:	8518753
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	28-SEP-2010
Filing Date:	20-DEC-2005
Time Stamp:	21:21:18
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	Transmittal Letter	02090_SIDS.pdf	75627 8a35a6179031b964f19cb10380cc9e7def47b732	no	4

Warnings:

Information:

2	Information Disclosure Statement (IDS) Filed (SB/08)	02090_SB08.pdf	612173 286684973720ada0c0cae392c5d17b7111397ce8	no	4
Warnings:					
Information:					
3	NPL Documents	02090_Non_Final_Office_Action.pdf	18269021 dace99e03317dfd050234f9bbedacf591697827c	no	23
Warnings:					
Information:					
			Total Files Size (in bytes):	18956821	

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

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

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

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

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 28, 2010 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☒ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☒ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a

notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND
- ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in

37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,

Dated: September 28, 2010

By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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.			
Signature:	/Elizabeth D. Ruzich/		
Typed or Printed Name:	Elizabeth D. Ruzich, Reg. 54,416	Dated:	September 7, 2010

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

AMENDMENT C

Sir:

Responsive to the Office Action mailed on June 7, 2010, which sets a shortened statutory period for response that expires on September 7, 2010, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;

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 ~~a~~ the code for authentication to an agent, wherein the agent is a third-party trusted authority~~, the code uniquely identifying the integrated device~~; and

responsive to authentication of the code, receiving an access message from the agent, to allow user access.

2. (Currently Amended) The method of claim 1, wherein the code is transmitted to the ~~third-party trusted authority~~ agent over a network.

3. (Original) The method of claim 1, further comprising:
registering an age verification for the user in association with the code.

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

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.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user and a code in a tamper-resistant format, the persistent storage being written once and being not altered subsequently, wherein the code uniquely identifies the integrated device;

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~~ the code for authentication to an agent, wherein the agent is a third-party trusted authority~~, the code uniquely identifying the integrated device~~;

wherein responsive to authentication of the code, the ~~third-party trusted authority~~ agent transmits an access message that enables user access.

11. (Canceled).

12. (Currently Amended) The integrated device of claim 10, wherein the code is transmitted to the ~~third-party trusted authority~~ agent over a network.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with an agent, wherein the agent is a third-party trusted authority;

requesting authentication of the code by the ~~third-party trusted authority~~ agent and the authentication determining whether the code is legitimate;

receiving an access message from the ~~third-party trusted authority~~ agent; and

in response to the access message being positive, providing access to an application.

16. (Canceled).

17. (Currently Amended) The method of claim 15, further comprising:

registering a date of birth or age with the ~~trusted authority~~ agent.

18. (Original) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:

a biometric key to store biometric data for a user and a code 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~~ the code, the code being associated with the verified user and uniquely identifying the biometric key; and

an authentication module to receive the code and send the code to an ~~third-party trusted authority~~ agent for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority, and responsive to the code

being authenticated, the agent sending an access message to an application to allow the user to access the application.

20. (Original) The system of claim 19, wherein 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.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1, 2, 10, 12, 15, 17 and 19 are amended. Support for the amendments can be found throughout the specification, for example at paragraphs [0044] and [0049] of the published application. Claims 2, 12, and 17 are updated to reflect the changes made to claims 1, 10 and 15 respectively. Claims 1-3, 5, 7-10, 12-15 and 17-25 are pending upon entry of this amendment.

Summary of the Rejections

1. Claim 5 is rejected under 35 U.S.C. § 112, second paragraph, for being indefinite.

2. Claims 1-2, 5, 7-10, 12, 15 and 18-25 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Hsu (USPN 6,041,410).

3. Claims 3, 13-14 and 17 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Hsu in view of Saito (U.S. Pub. No. 20040129787).

These rejections are now traversed.

Response to Rejection under 35 U.S.C. § 112

Claim 5 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite since there is no antecedent basis for the limitation "the biometric verification" used in lines 1-2. **Claim 1 has been amended to recite "a biometric verification"** in order to provide antecedent basis for the limitation in claim 5, which depends on claim 1. Accordingly, Applicant requests that the Examiner withdraw the §112 rejection.

Response to Rejections under 35 U.S.C. § 103(a)

The rejections are addressed by reference to the independent claims.

Independent Claim 1

Amended claim 1 recites, in part:

> **persistently storing biometric data for the user and a code** in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;
>
> . . .responsive to a determination that the scan data matches the biometric data, wirelessly **sending the code for authentication to an agent**, wherein the agent is a third-party trusted authority; and
>
> responsive to authentication of the code, **receiving an access message from the agent,** to allow user access. (emphasis added)

The claimed invention discloses a system and a method for an authentication responsive to biometric verification of a user being authenticated. A user's biometric key persistently stores biometric data uniquely associated with the user (e.g., a fingerprint or a retinal scan) and a code. The code is a device ID that uniquely identifies the biometric key and is provided during the manufacturing process or the enrollment of a user. In order to get authenticated, the user first scans his biometric data. The system then verifies the scanned biometric data by comparing it with the stored biometric data. Upon verification, the system wirelessly sends the code to an agent for a second level of authentication. The agent is a third-party trusted authority that stores a list of all the codes. The agent verifies the received code by comparing it with the stored list and upon successful verification, sends an access message authenticating the user. The claimed

invention thus provides two levels of authentication, without the user having to memorize and input multiple credentials (e.g., passwords and PINs) associated with the electronic key or have a security breach wherein an illegitimate user uses a stolen biometric key.

The cited references do not disclose or suggest, among other things, "persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device," "sending the code for authentication to an agent" and "responsive to authentication of the code, receiving an access message from the agent, to allow user access" as recited by amended claim 1.

Hsu describes a system and a method for verifying the identity of a person seeking access to a protected property.[1] In Hsu, the communications are limited to data transmissions between a user's biometric key and a receiver.[2] On page 2 of the Office Action, the Examiner argues that Hsu discloses a door as the third-party and on page 5 states:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication to a third-party trusted authority, the code uniquely identifying the integrated device (*Fig. 4, step 60; Column 5, lines 57-58; column 6, line 66-column 7, line 34, wherein the generated CRC encrypted with the door's public key and the fob's private key is interpreted as code uniquely identifies the integrated device)* and

At most, Hsu describes the fob sending a code to a receiver of a **door that the user is trying to access**. There is nothing in the cited portions or elsewhere in Hsu that

---

[1] Hsu, column 1, lines 50-53.
[2] Hsu, Figure 1.

discloses or suggests a "**sending the code for authentication to an agent**" as recited by amended claim 1.

In addition, Applicant respectfully points out that, in Hsu, the code is **generated** upon verification of the user's biometric data and is ***not* stored persistently in the fob**.[3] Accordingly, Hsu does not disclose or suggest "**persistently storing** biometric data for the user and **a code** in a tamper-resistant format in a storage element on the integrated device," as recited in amended claim 1.

Furthermore, on page 5 of the Office Action, the Examiner acknowledges that Hsu does not disclose "receiving an access message to allow user access." However, the Examiner argues that it is obvious to one of ordinary skill in the art at the time that the invention was made to include "receiving an access message to allow user access" in order to clearly communicate that access is granted. Claim 1 has been amended to recite "receiving an access message from **the agent**" which is **not disclosed in Hsu and is not obvious to one of ordinary skill in the art** at the time that the invention was made. Applicants have carefully reviewed all of Hsu and find no mention of an agent, let alone "receiving an access message from the agent." As a result, Hsu fails to disclose or suggest the above mentioned features of amended claim 1.

Additionally, Saito fails to remedy the deficiencies of Hsu. Saito discloses a smartcard system for biometric identification.[4] Saito fails to even disclose an agent, let alone "receiving an access message from the agent." As a result, Saito fails to teach or disclose the features of amended claim 1.

---

[3] Hsu, column 5, lines 47-60.
[4] Saito, Abstract.

Accordingly, the cited references whether taken alone or in combination do not disclose or suggest every limitation of Applicant's amended claim 1. Amended claim 1 is therefore patentable over the cited references. Claims 2-3, 5 and 7-9 incorporate the limitations of amended claim 1 and are therefore patentable over the cited references for at least the same reasons as amended claim 1.

Independent Claim 10

Amended claim 10 recites, in part:

> a **persistent storage to store biometric data for a user and a code** in a tamper-resistant format, the persistent storage being written once and being not altered subsequently, wherein the code uniquely identifies the integrated device;
>
> 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 the code for authentication to an agent**, wherein the agent is a third-party trusted authority;
>
> wherein responsive to authentication of the code, the **agent transmits an access message** that enables user access. (emphasis added)

The cited references do not disclose or suggest the above mentioned features of Applicant's amended claim 10 for at least the same reasons as those described for claim 1. Accordingly, claim 10 is patentable over the cited references. Claims 12-14 incorporate the limitations of claim 10, and are therefore patentable over the cited references for at least the same reasons as claim 10.

Independent Claim 15

Amended claim 15 recites, in part:

> receiving a code associated with a biometrically verified user, the code being registered with an **agent**, wherein the agent is a third-party trusted authority;
>
> requesting authentication of the code by the agent and the authentication determining whether the code is legitimate;
>
> **receiving an access message from the agent**; and
>
> in response to the access message being positive, providing access to an application. (emphasis added)

The cited references do not disclose or suggest the above mentioned features of Applicant's amended claim 15 for at least the same reasons as those described for claim 1. Accordingly, claim 15 is patentable over the cited references. Claims 17-18 incorporate the limitations of claim 15, and are therefore patentable over the cited references for at least the same reasons as claim 15.

Independent Claim 19

Amended claim 19 recites, in part:

> a biometric key **to store biometric data for a user and a code** 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 the code, the code being associated with the verified user and uniquely identifying the biometric key; and

> an authentication module to receive the code and **send the code to an agent** for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority, and responsive to the code being authenticated, **the agent sending an access message to an application** to allow the user to access the application. (emphasis added)

The cited references do not disclose or suggest the above mentioned features of Applicant's amended claim 19 for at least the same reasons as those described for claim 1. Accordingly, claim 19 is patentable over the cited references. Claims 20-25 incorporate the limitations of claim 19, and are therefore patentable over the cited references for at least the same reasons as claim 19.

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 7, 2010

/Elizabeth D. Ruzich/

Elizabeth D. Ruzich, Reg. No. 54,416
Attorney for Applicant
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9824
Fax: (801) 355-0160
Email: eruzich@patentlawworks.net

Electronic Acknowledgement Receipt

EFS ID:	8362607
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Elizabeth D. Ruzich
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	07-SEP-2010
Filing Date:	20-DEC-2005
Time Stamp:	15:48:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	02090_Amendment_C.pdf	156909 83620f6f7621ec35a7f896175708541db6c4caf7	no	12

Warnings:

Information:

Total Files Size (in bytes):	156909

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 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/314,199	12/20/2005	

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/07/2010	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/Kim Downing/

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.

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	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	6709333		2004-03-23	Bradford et al.	
	2	7112138		2006-09-26	Hedrick 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	20030186739		2003-10-02	Paulsen et al.	
	2	20040127277		2004-07-01	Walker et al.	
	3	20040209692		2004-10-21	Schober 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button Add								
NON-PATENT LITERATURE DOCUMENTS Remove								
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T[5]
	1							☐
If you wish to add additional non-patent literature document citation information please click the Add button Add								
EXAMINER SIGNATURE								
Examiner Signature						Date Considered		

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2005-12-20
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

☒ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

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

Signature	/Brian G. Brannon/	Date (YYYY-MM-DD)	2010-09-03
Name/Print	Brian G. Brannon	Registration Number	57,219

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 Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Brian Gregory Brannon/Connie Evenich
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	8357604
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Brian Gregory Brannon
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	03-SEP-2010
Filing Date:	20-DEC-2005
Time Stamp:	19:12:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	4687
Deposit Account	
Authorized User	

File Listing:

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

1	Transmittal Letter	02090_SIDS.pdf	75596 df505146da6695f3b8df58a49a991daa6b32695f	no	4
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	02090_PTO_SB08a.pdf	611734 742a528cadd0105764b504d34204763da9ec4441	no	4
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30032 34de983567a6b09fa35c6672f5ef789029de0c33	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	717362	

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

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

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

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

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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 Pacific Time Zone of the United States on the local date shown below:

Dated: September 3, 2010 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☒ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a

notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND
- ☐ Attached hereto is the fee set forth under 37 CFR § 1.17(p) for submission of this Information Disclosure Statement under 37 CFR § 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____, filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in

37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,

Dated: September 3, 2010

By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

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	11314199
	Filing Date	2007-05-05
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

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	7644443		2010-01-05	Matsuyama 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	20050229007		2005-10-13	Bolle 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2007-05-05
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

	1		☐

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

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11314199
	Filing Date	2007-05-05
	First Named Inventor	John J. Giobbi
	Art Unit	2437
	Examiner Name	Phy Anh Tran Vu
	Attorney Docket Number	10001-02090

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☐ None

SIGNATURE

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

Signature	/Elizabeth D. Ruzich/	Date (YYYY-MM-DD)	2010-07-02
Name/Print	Elizabeth D. Ruzich	Registration Number	54,416

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.

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

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: July 2, 2010 /Elizabeth D. Ruzich/
Elizabeth D. Ruzich, Reg. No. 54,416

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☐ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☒ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
  - ☒ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☒ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:
  - ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a

foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;

☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

Respectfully submitted,
JOHN J. GIOBBI

Dated: July 2, 2010

By: /Elizabeth D. Ruzich/

Elizabeth D. Ruzich, Reg. No. 54,416
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9824
Fax: (801) 355-0160
Email: eruzich@patentlawworks.net

Electronic Acknowledgement Receipt

EFS ID:	7951165
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Elizabeth D. Ruzich
Filer Authorized By:	
Attorney Docket Number:	10001-02090
Receipt Date:	02-JUL-2010
Filing Date:	20-DEC-2005
Time Stamp:	20:16:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	02090_PTO_SB08a.pdf	612094 134763e95fbb4cf0d9cb06dbac3af05feb2e8ecd	no	4

Warnings:

Information:

2	Transmittal Letter	02090_SIDS.pdf	66634 9dc5c43380b124bb1ac2f4ae48b861b2903e2f9b	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	678728	

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	10001-02090	4469

89194 7590 06/07/2010
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
06/07/2010	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):

eruzich@patentlawworks.net
docketing@patentlawworks.net
gsueoka@patentlawworks.net

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *25 February 2010*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-10,12-15 and 17-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-10,12-15, and 17-25* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/06/2010 has been entered.

Response to Arguments

Applicant's arguments filed 2/25/2010 have been fully considered but they are not persuasive.

Regarding claim 1, on page 7, Applicant argues that "Amended claim 1 recites a method for verifying a user during authentication where biometric scan data is compared to biometric data and where a code is sent to a **third-party** trusted authority to obtain an **access message** to allow user access. Hsu fails to teach or suggest these features."

In response, Examiner respectfully disagrees. Examiner respectfully submits that Hsu discloses 3 parties which include: a user, fob, and a door. Hsu further discloses the user's fingerprint is scanned and is compared to a reference fingerprint stored in the fob, which the user registered prior (*Column 4, lines 40-46; column 5, lines 18-22*). Only when the comparison results in a match, the fob will generate a CRC and transmits the CRC to the door (third party). Upon receiving the CRC, the door will compare the CRC received with the CRC stored during registration, if there is a match, the door is opened

for the user to access (*Column 5, lines 42-60; Column 6, lines 17-24*). Thus contrasting to Applicant's argument, Hsu and Official Notice as rejected in the amended claim 1 below disclose each and every limitation in the amended claim 1, which recites a method for verifying a user during authentication where biometric scan data is compared to biometric data and where a code is sent to a **third-party** trusted authority to obtain an **access message** to allow user access. "

Regarding claim 2, on pages 8-9, Applicant argues that " At most, Hsu discloses two parties: the user and the institution. There is no third-party authority in this passage. Hsu fails to disclose a network."

In response, Examiner respectfully disagrees. First, with regard to "There is no third- party authority, please see discussion of claim 1 above. Second, network is defined as two or more devices connected via wired/wireless. Hsu, discloses a fob is connected to the door wirelessly to exchange biometric data for authentication (Figure 1). Therefore, contrasting to Applicant's argument, Hsu has a network.

Regarding claims 3, 5, 7-10, 15, and 19, please see discussion of claim 1 above.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 5 recites the limitation "the biometric verification" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 103

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

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

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu).

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 in a storage element on the integrated device that is written once and is not altered subsequently (*Column 4, lines 15-25; Column 7, lines 56-57; Figure 3, element 32, column 5, lines 19-29*);

responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (*Col 4, lines 40-45, wherein scanned fingerprint is received from the sensor*);

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data (*Column 4, lines 40-45; Column 5, lines 29-31, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob*);

responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication to a third-party trusted authority, the code uniquely identifying the integrated device (*Fig. 4, step 60; Column 5, lines 57-58; column 6, line 66-column 7, line 34, wherein the generated CRC encrypted with the door's public key and the fob's private key is interpreted as code uniquely identifies the integrated device)* and

Hsu discloses when there's a match between the CRC (code) received with the one that was stored, then the door is opened for the user (*Column 6, lines 16-24*)

Hsu does not explicitly disclose in response to authentication of the code, receiving an access message to allow user access.

However, it is obvious to one of ordinary skill in the art at the time the invention was made to include in response to authentication of the code, receiving an access message to allow user access in order to clearly communicate that access is granted.

Regarding claim 2, Hsu also discloses the code is transmitted to the third-party trusted authority over a network (*Figure 4, step 60; Column 7, lines 24-34*).

Regarding claim 5, Hsu also discloses the code indicates that the biometric verification was successful (*Column 5, lines 42-51*).

Regarding claim 7, Hsu also discloses the biometric data and the scan data are both based on a fingerprint scan by the user (*Col 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person*).

Regarding claim 8, Hsu also discloses establishing a secure communication channel prior to sending the code for authentication (*Col 6, lines 42-67; Col 7, lines 1-34, wherein exchanging of keys is performed prior to sending the CRC, which corresponds to establishing a secure communication channel prior to sending the code for authentication*).

Regarding claim 9, Hsu also discloses 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 (*Fig. 4, step 60; Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" encrypted with the door's public key and the fob's private key which corresponds to a "code" is transmitted*).

Claim 10 is rejected for the same rationale as claim 1 above.

Claim 12 is rejected for the same rationale as claim 2 above.

Regarding claim 15, Hsu discloses a method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with a third-party trusted authority (*Column 6, lines 2-9; column 7, line 5-37*);

requesting authentication of the code by the third-party trusted authority and the authentication determining whether the code is legitimate (*Column 6, lines 2-9; column 7, line 5-16*);

in response to the authentication result being positive, providing access to an application (*Column 7, lines 30-34*).

Hsu does not explicitly disclose receiving an access message from the third-party trusted authority;

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include this step of receiving an authentication result from the trusted authority to clearly indicate the status of the authentication result to the user.

Regarding claim 18, Hsu also 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, lines 42-67; Col 7, lines 1-34; Fig. 4, step 60; column 5, lines 57-58; column 6, line 66-column 7, line 34*).

Claim 19 is rejected for the same rationale as claim 15 above.

Regarding claim 20, Hsu also discloses 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 19-25; 40-44*).

Regarding claim 21, Hsu also discloses if the biometric key cannot verify the scan data as being from the user, it does not send the code (*Column 5, lines 42-47, wherein the no-match signal is generated, no further processing is performed, thus no CRC will be generated, and available to send*).

Regarding claim 22, Hsu also discloses the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition (*Column 4, lines 34-39*).

Regarding claim 23, Hsu also discloses the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file (*Figure 4*).

Claim 24 is rejected for the same rationale as claim 22 above.

Claim 25 is rejected for the same rationale as claim 22 above.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

Regarding claim 3, Hsu does not explicitly disclose registering an age verification for the user in association with the code.

However, Saito discloses registering an age verification for a user in association with a code (*[0082]-[0083][0164], wherein date of birth is registered along with other personal data*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the authentication method of Hsu in order to enhance the reliability and security of the authentication.

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

Regarding claim 14, Hsu does not disclose the verification module comprises: an LED to be activated for requesting the biometric scan.

However, Saito discloses the verification module comprises an LED to be activated for requesting the biometric scan (*[0040]-[0056], wherein a LED is used to prompt user for biometric data*).

One or ordinary skill in the art at the time the invention was made would have been motivated to incorporate the feature of LED into the system of Hsu to provide a clear indication that a biometric data is required.

Claim 17 is rejected for the same rationale as claim 3 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 Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/314,199	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,041,410	03-2000	Hsu et al.	713/186
*	B	US-2004/0129787	07-2004	Saito et al.	235/492
*	C	US-2007/0220272	09-2007	Campisi et al.	713/186
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009	06/01/2010						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	-	-						
	5	✓	✓	✓						
	6	✓	-	-						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	-	-						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	-	-						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22			✓						
	23			✓						
	24			✓						
	25			✓						

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
713	155,159,176	6/1/2010	PVU
726	27	6/1/2010	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Google Search	6/1/2010	PVU
East text search	6/1/2010	PVU
Inventor names search for double patenting issues	6/1/2010	PVU
PLUS search	6/1/2010	PVU

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21
S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51

S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif $6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif $6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07

S25	5	713/186.ccls. and ((authenticat $4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50
S27	31	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51
S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat $4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S31	562	713/186.ccls. and (authenticat $4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat $4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S33	228	713/186.ccls. and (authenticat $4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat $4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat $4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49
S37	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42

S38	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S39	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
S40	71	713/176.ccls. and (biometric $6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S41	0	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S42	52	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
S43	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S44	102	S43 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
S45	9	S43 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48
S46	15	(john near4 giobbi).inv. and (biometric$4 with authenticat $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S47	7	(john near4 giobbi).inv. and (biometric$4 with authenticat $4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
S48	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 10:08
S49	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:30
S50	1	"20060143441".pn. and (palm near4 print)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31

S51	1	"20060143441".pn. and (casino near4 machine)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/05/27 15:31
S52	157	713/155,159.ccls. and (biometric$5) with authenticat $4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:25
S53	121	S52 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:26
S54	192	713/176.ccls. and (biometric $5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:39
S55	154	S54 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S56	20	S55 and (LED)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:40
S57	106	726/27.ccls. and (biometric$5) with authenticat$4	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S58	75	S57 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:44
S59	9	(giobbi near4 john).in. and ((authenticat$4) and (biometric $6)).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2010/06/01 10:47

6/ 1/ 2010 2:38:14 PM
C:\ Documents and Settings\ pvu3\ My Documents\ EAST\ Workspaces\ 11314199.wsp

PLUS Search Results for S/N 11314199, Searched Tue Jun 01 11:47:56 EDT 2010

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5245329 99
5337043 99
6035398 99
20080310619 99
20090283583 87
5977655 86
5991408 86
6292830 86
6923370 86
7502934 86
7581105 86
20050087597 86
20050132195 86
20050132196 86
20050237150 86
20060278700 86
20070208867 86
20070277042 86
20080022111 86
20080141040 86
20090158423 86
6185316 82
5757916 82
5774551 82
6006328 82
6035403 82
6173400 82
4941173 82
5020105 82
5608387 82
5987232 82
6035406 82
6038315 82
6052468 82
6084967 82
6167517 82
6189096 82
6202151 82
6219793 82
6219793 82
6263446 82
6310966 82
6317834 82
6332193 82
6363485 82
6401206 82
6453416 82
6580815 82
6678821 82
6687375 82

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	25000-11062	4469

89194 7590 03/16/2010
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

RECEIVED
PATENT DOCKETING
Patent Law Works
3/19/2010 9:17:01 AM

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
03/16/2010	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):

eruzich@patentlawworks.net
docketing@patentlawworks.net
gsueoka@patentlawworks.net

PTOL-90A (Rev. 04/07)

NOTICE OF IMPROPER REQUEST FOR CONTINUED EXAMINATION (RCE)	Application No. 11/314,199	Applicant(s) GIOBBI, JOHN J.	
		Art Unit 2400	Date Mailed:

The request for continued examination (RCE) under 37 CFR 1.114 filed on 25 February, 2010 is improper for reason(s) indicated below:

1. ☐ Continued examination under 37 CFR 1.114 does not apply to an application for a design patent. Applicant may wish to consider filing a continuing application under 37 CFR 1.53(b) or a CPA under 37 CFR 1.53(d). An RCE cannot be treated as a CPA.

2. ☐ Continued examination under 37 CFR 1.114 does not apply to an application that was filed before June 8, 1995. Applicant may wish to consider filing a continuing application under 37 CFR 1.53(b).

3. ☐ Continued examination under 37 CFR 1.114 does not apply to an application unless prosecution in the application is closed. If the RCE was accompanied by a reply to a non-final Office action, the reply will be entered and considered under 37 CFR 1.111. If the RCE was not accompanied by a reply, the time period set forth in the last Office action continues to run from the mailing date of that action.

4. ☐ The request was not filed before payment of the issue fee, and no petition under 37 CFR 1.313 was granted. If this application has not yet issued as a patent, applicant may wish to consider filing either a petition under 37 CFR 1.313 to withdraw this application from issue, or a continuing application under 37 CFR 1.53(b).

5. ☐ The request was not filed before abandonment of the application. The application was abandoned, or proceedings terminated on _____. Applicant may wish to consider filing a petition under 37 CFR 1.137 to revive this abandoned application.

6. ☒ The request was not accompanied by the fee set forth in 37 CFR 1.17(e) as required by 37 CFR 1.114. Since the application is not under appeal, the time period set forth in the final Office action or notice of allowance continues to run from the mailing date of that action or notice.

7. ☐ The request was not accompanied by a submission as required by 37 CFR 1.114. Since theapplication is not under appeal, the time period set forth in the final Office action or notice of allowance continues to run from the mailing date of that action or notice.

Note: A continued prosecution application (CPA) under 37 CFR 1.53(d) cannot be filed in a utility or plant application. A CPA filed in a utility or plant application that has a filing date **on or after June 8, 1995** will be treated as an RCE under 37 CFR 1.114. The request for a CPA in the instant application, however, has been treated as an improper RCE for the reason(s) indicated above.

A copy of this Notice MUST be returned with the reply.

Direct any questions concerning this notice to

/AUDRIS SIAS/, Technology Center 2400

Telephone Number: (571)272-1048

Electronic Patent Application Fee Transmittal

Application Number:	11314199
Filing Date:	20-Dec-2005
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Filer:	Elizabeth D. Ruzich/Connie Evenich
Attorney Docket Number:	10001-02090

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**470**

Electronic Acknowledgement Receipt

EFS ID:	7253562
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Elizabeth D. Ruzich/Connie Evenich
Filer Authorized By:	Elizabeth D. Ruzich
Attorney Docket Number:	10001-02090
Receipt Date:	22-MAR-2010
Filing Date:	20-DEC-2005
Time Stamp:	12:52:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$470
RAM confirmation Number	8877
Deposit Account	
Authorized User	

File Listing:

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

1	Examination support document	02090_Notice_of_Improper_Request_for_RCE.pdf	752169 d38e539075a0d6b296015b2615e936e44d0204df	no	2
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	31990 82459f52db152599f1d54dde126456f93c901d8f	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	784159	

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/314,199	12/20/2005	John J. Giobbi	25000-11062	4469

89194 7590 03/16/2010
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
03/16/2010	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):

eruzich@patentlawworks.net
docketing@patentlawworks.net
gsueoka@patentlawworks.net

PTOL-90A (Rev. 04/07)

NOTICE OF IMPROPER REQUEST FOR CONTINUED EXAMINATION (RCE)	Application No. 11/314,199	Applicant(s) GIOBBI, JOHN J.	
		Art Unit 2400	Date Mailed:

The request for continued examination (RCE) under 37 CFR 1.114 filed on 25 February, 2010 is improper for reason(s) indicated below:

1. ☐ Continued examination under 37 CFR 1.114 does not apply to an application for a design patent. Applicant may wish to consider filing a continuing application under 37 CFR 1.53(b) or a CPA under 37 CFR 1.53(d). An RCE cannot be treated as a CPA.

2. ☐ Continued examination under 37 CFR 1.114 does not apply to an application that was filed before June 8, 1995. Applicant may wish to consider filing a continuing application under 37 CFR 1.53(b).

3. ☐ Continued examination under 37 CFR 1.114 does not apply to an application unless prosecution in the application is closed. If the RCE was accompanied by a reply to a non-final Office action, the reply will be entered and considered under 37 CFR 1.111. If the RCE was not accompanied by a reply, the time period set forth in the last Office action continues to run from the mailing date of that action.

4. ☐ The request was not filed before payment of the issue fee, and no petition under 37 CFR 1.313 was granted. If this application has not yet issued as a patent, applicant may wish to consider filing either a petition under 37 CFR 1.313 to withdraw this application from issue, or a continuing application under 37 CFR 1.53(b).

5. ☐ The request was not filed before abandonment of the application. The application was abandoned, or proceedings terminated on _____. Applicant may wish to consider filing a petition under 37 CFR 1.137 to revive this abandoned application.

6. ☒ The request was not accompanied by the fee set forth in 37 CFR 1.17(e) as required by 37 CFR 1.114. Since the application is not under appeal, the time period set forth in the final Office action or notice of allowance continues to run from the mailing date of that action or notice.

7. ☐ The request was not accompanied by a submission as required by 37 CFR 1.114. Since theapplication is not under appeal, the time period set forth in the final Office action or notice of allowance continues to run from the mailing date of that action or notice.

Note: A continued prosecution application (CPA) under 37 CFR 1.53(d) cannot be filed in a utility or plant application. A CPA filed in a utility or plant application that has a filing date **on or after June 8, 1995** will be treated as an RCE under 37 CFR 1.114. The request for a CPA in the instant application, however, has been treated as an improper RCE for the reason(s) indicated above.

A copy of this Notice MUST be returned with the reply.

Direct any questions concerning this notice to

/AUDRIS SIAS/, Technology Center 2400

Telephone Number: (571)272-1048

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/314,199	12/20/2005	John J. Giobbi	25000-11062

CONFIRMATION NO. 4469

89194
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

POA ACCEPTANCE LETTER

OC000000040513220

Date Mailed: 03/11/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/03/2010.

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.

/squreshi/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/314,199	12/20/2005	John J. Giobbi	25000-11062

CONFIRMATION NO. 4469

89194
Patent Law Works/Proxense
165 South Main St
Salt Lake City, UT 84111

POWER OF ATTORNEY NOTICE

OC000000040513206

Date Mailed: 03/11/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/03/2010.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/squreshi/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 89194

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 89194

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

Proxense, LLP
689 NW Stonepine Drive
Bend, OR 97710-6818

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	2/22/10
Name	John Giobbi	Telephone	541-382-5745
Title	Chief Executive Officer		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: John Joseph Giobbi

Application No./Patent No.: 11/314,199 Filed/Issue Date: December 20, 2005

Titled: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

Proxense, LLC (Name of Assignee), a Corporation (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. [X] the assignee of the entire right, title, and interest in;

2. [ ] an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. [ ] the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. [ ] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

B. [X] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: J. Giobbi To: Proxense, LLC

   The document was recorded in the United States Patent and Trademark Office at Reel 017659, Frame 0679, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet(s).

[ ] As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Elizabeth Ruzich/	3/3/2010
Signature	Date
Elizabeth Ruzich, Reg. No. 54,416	Attorney for Applicant
Printed or Typed Name	Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	7135260
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Elizabeth D. Ruzich
Filer Authorized By:	
Attorney Docket Number:	25000-11062
Receipt Date:	03-MAR-2010
Filing Date:	20-DEC-2005
Time Stamp:	17:49:07
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	02090USPowerofAttorney.pdf	1014805 d19ae545af83ee177fab166e3f05eaf890f8db2a	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73(b).	02090US373B.pdf	424385 776d921ec7b37aec600732878b389749a6727f32	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1439190	

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/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	11/314,199	Filing Date	2009-12-20	Docket Number (if applicable)	10001-02090	Art Unit	2437
First Named Inventor	John J. Giobbi			Examiner Name	Phy Anh Tran Vu		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Elizabeth D. Ruzich/	Date (YYYY-MM-DD)	2010-02-25
Name	Elizabeth D. Ruzich	Registration Number	54416

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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.

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
SERIAL NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

CERTIFICATE OF ELECTRONIC (EFS-WEB) TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.8(a)(i)(C) from the Mountain Time Zone of the United States on the local date shown below.

Dated: February 25, 2010 By: /Elizabeth D. Ruzich/

Elizabeth D. Ruzich, Reg. No. 54,416

AMENDMENT B AND RESPONSE

Sir:

This amendment for the patent application identified above is in response to the Office action dated November 25, 2009, which set a shortened statutory period for response that expires on February 25, 2009.

Kindly amend this application as indicated herein.

IN THE CLAIMS:

1. (Currently Amended) 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 in a storage element on the integrated device that is written once and is not altered subsequently;

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 scan data matches the biometric data; ~~and~~

responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication to a third-party ~~that the code is legitimate by a~~ trusted authority, the code uniquely identifying the integrated device; and

responsive to authentication of the code, receiving an access message to allow user access.

2. (Currently Amended) The method of claim 1, wherein the code is transmitted to ~~registered with~~ the third-party trusted authority over a network~~, and the code can be authenticated to a third party by the trusted authority~~.

3. (Original) The method of claim 1, further comprising:
registering an age verification for the user in association with the code.

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

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.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user in a tamper-resistant format~~;~~ , the persistent storage being written once and being not altered subsequently;

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 to a third-party ~~that the code is legitimate by a~~ trusted authority, the code uniquely identifying the integrated device,

wherein responsive to authentication of the code, the third-party trusted authority transmits an access message that enables user access.

11. (Canceled).

12. (Currently Amended) The integrated device of claim 10, wherein the code is transmitted to ~~registered with~~ the third-party trusted authority over a network~~, wherein the code can be authenticated to a third party by the trusted authority~~.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with a third-party trusted authority;

requesting authentication of the code by the third-party trusted authority and the authentication determining whether the code is legitimate;

receiving an ~~authentication result~~ access message from the third-party trusted authority; and

in response to the ~~authentication result~~ access message being positive, providing access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:

registering a date of birth or age with the trusted authority.

18. (Original) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) 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, the code being associated with the verified user;

an authentication module to receive the code and send the code to a third-party trusted authority for authentication to determine whether the code is legitimate, and responsive to the code being authenticated, sending an access message to an application to allow ~~allowing~~ the user to access ~~an~~ the application.

20. (Original) The system of claim 19, wherein 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.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (New) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (New) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (New) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (New) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-21 were pending and presented for examination. In an Office Action dated November 25, 2009, 1-3, 5, 7-10, 12-15 and 17-21 were rejected. Applicant amends claims 1, 2, 10, 12, 15 and 19. Support for the amendment is found throughout the specification, for example, at paragraph 44. Applicant adds claims 22-25. Support for claims 22 and 24-25 can be found throughout the specification, for example, in paragraph 22. Support for claim 23 can be found throughout the specification, for example, at paragraph 37.

Summary of Rejections

The Examiner rejects claims 1, 2, 5, 7-10, 12 and 19-21 under 35 USC § 102(b) as allegedly being anticipated by Hsu (USPN 6,041,410). The Examiner rejects claims 15 and 18 under 35 USC § 103(a) as allegedly being unpatentable in view of Hsu. These rejections are traversed.

The rejections are addressed by reference to the independent claims.

Independent Claim 1

Applicant's amended claim 1 recites, in part:

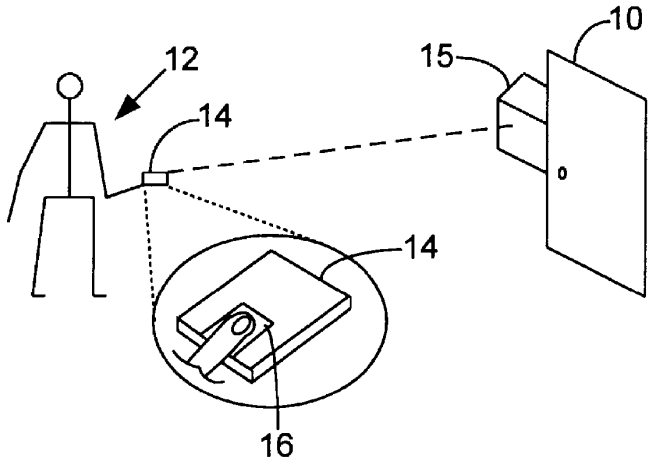
> responsive to receiving a request for biometric verification of the user,
> receiving scan data from a biometric scan;
> comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication to a **third-party trusted authority**, the code uniquely identifying the integrated device; and

responsive to authentication of the code, receiving an **access message** to allow user access.

Amended claim 1 recites a method for verifying a user during authentication where biometric scan data is compared to biometric data and where a code is sent to a **third-party** trusted authority to obtain an **access message** to allow user access.

Hsu fails to teach or suggest these features. Applicant draws the Examiner's attention to Figure 1 of Hsu, which is reproduced below:



In Hsu, the communications are limited to data transmissions between the fob 14 and the receiver 15 to obtain access to the door 10. If someone wanted to tamper with the fob 14 to obtain access to the door 10, there is no safety check.

Claim 1, on the other hand, requires a second level of authentication. The authentication process is not completed until a code associated with the integrated device is transmitted to a third party and the third party transmits back an access message.

With reference to claim 2, the Examiner asserted that Hsu discloses authenticating the code with a third party in column 6, lines 2-9 and column 7, lines 5-16. Applicant strongly disagrees. For the Examiner's convenience, Applicant reproduces column 6, lines 2-9 below:

> 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**.

The above passage actually demonstrates the opposite of what the Examiner asserts. In Hsu, the user must prove to the <u>same</u> institution that authenticates the fingerprint information that the user is who he purports to be. Thus, identifying information for the user is stored **<u>in the door</u>**. At most, Hus discloses two parties: the user and the institution. There is no third-party authority in this passage.

Next, we turn to column 7, lines 5-16:

> the next. The fob public key is registered with each door **10** and it would be impractical to change it for every use. The fob private key is stored (at **36**, FIG. **3**) in the fob **14**, preferably in a form in which it cannot be discerned by inspection or reverse engineering. The key may, for example, be encoded into the silicon structure of the processor module **20** in such a way that it is practically indecipherable by any normal reverse engineering technique. Each door **10** generates a new public-private key pair on every new use of the door. Thus, these keys cannot be determined in advance of the actual message exchange with a fob **14**.

Again, the door and **not** a third-party generates the public-private key pair. At most, the above passage discloses two parties: the user and the door. Thus, there is no third-party trusted authority to provide an additional layer of authentication. Hsu therefore does not disclose or suggest the above-quoted elements of claim 1.

Amended claim 2 recites that the code is transmitted to the third-party trusted authority over a network. Hsu fails to teach or suggest a network. As a result, Hsu cannot anticipate claim 2.

Claims 3, 5 and 7-9 incorporate the limitations of claim 1, and are therefore patentable over the cited references for at least the same reasons as claim 1. Hence, reconsideration and withdrawal of the rejection of claims 2, 3, 5 and 7-9 is respectfully requested.

Independent Claim 10

Applicant's amended claim 10 recites, in part:

> 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 to a **third-party trusted authority**, the code uniquely identifying the integrated device,
>
> wherein responsive to authentication of the code, the **third-party trusted authority** transmits an **access message** that enables user access.

The cited references do not disclose or suggest the above-quoted elements of Applicant's claim 10 for at least the same reasons as those described for claim 1. Accordingly, claim 10 is patentable over the cited references. Claims 12-14 incorporate the limitations of claim 10, and are therefore patentable over the cited references for at least the same reasons as claim 10.

Independent Claim 15

Applicant's amended claim 15 recites, in part:

> receiving a code associated with a biometrically verified user, the code being registered with a **third-party trusted authority**;
>
> requesting authentication of the code by the **third-party** trusted authority and the authentication determining whether the code is legitimate;
>
> receiving an access message from the **third-party** trusted authority; and
>
> in response to the **access message** being positive, providing access to an application.

The cited references do not disclose or suggest the above-quoted elements of Applicant's claim 15 for at least the same reasons as those described for claim 1. Accordingly, claim 15 is patentable over the cited references. Claims 17 and 18 incorporate the limitations of claim 15, and are therefore patentable over the cited references for at least the same reasons as claim 15.

Independent claim 19

Applicant's amended claim 19 recites, in part:

> an authentication module to receive the code and send the code to a **third-party trusted authority** for authentication to determine whether the code is legitimate, and responsive to the code being authenticated, sending an access message to an application to allow the user to access the application.

The cited references do not disclose or suggest the above-quoted elements of Applicant's claim 19 for at least the same reasons as those described for claim 1. Accordingly, claim 1 is patentable over the cited references. Claims 20 and 21 incorporate the limitations of claim 1, and are therefore patentable over the cited references for at least the same reasons as claim 10.

Conclusion

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

Respectfully Submitted,
JOHN GIOBBI

Dated: February 25, 2010

/Elizabeth D. Ruzich/

Elizabeth D. Ruzich, Reg. No. 54,416
Attorney for Applicant
Patent Law Works LLP
165 South Main Street, 2nd Floor
Salt Lake City, UT 84111
Tel: (801) 258-9824
Fax: (801) 258-0160
Email: eruzich@patentlawworks.net

Electronic Acknowledgement Receipt

EFS ID:	7091302
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	89194
Filer:	Elizabeth D. Ruzich/Connie Evenich
Filer Authorized By:	Elizabeth D. Ruzich
Attorney Docket Number:	25000-11062
Receipt Date:	25-FEB-2010
Filing Date:	20-DEC-2005
Time Stamp:	17:35:30
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	Request for Continued Examination (RCE)	02090US-2010-02-25-RequestForExamination.pdf	697841 4c91381ee98e609b9dd5cf4265d6d7617c37176f	no	3

Warnings:

Information:

2	Amendment After Final	02090-US-2010-02-25v1-Amendment-B.pdf	186680 17e25cef97db72d7591558f20a37cbee697bb2df	no	12
Warnings:					
Information:					
			Total Files Size (in bytes):	884521	

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 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
11/314,199	12/20/2005	☐ To be Mailed

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 02/25/2010

	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT

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

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

Legal Instrument Examiner:
/DONNA D. SMALLS LOGAN/

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.
11/314,199	12/20/2005	John J. Giobbi	25000-11062	4469

89194 7590 11/25/2009
Proxense/Fenwick
Silicon Valley Center
801 California Street
Mountain View, CA 94041

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
11/25/2009	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):

ptoc@fenwick.com
gsueoka@fenwick.com
nmorad@fenwick.com

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *27 July 2009*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-10,12-15 and 17-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5, 7-10, 12-15, 17-21* is/are rejected.

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

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

Application Papers

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

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the amendment filed on 7/27/2009.

Response to Arguments

Applicant's arguments with respect to claims 1-2, 10, 12, 15, 17, and 19 have been considered but are moot in view of the new ground(s) of rejection.

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 5, 7-10, 12, 19-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Hsu et al. (US 6,041,410 A1, hereinafter Hsu).

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 in a storage element that is written once and is not altered subsequently (*Col 4, lines 15-25; Col 7, lines 56-67*);

responsive to receiving a request for biometric verification of the user (*i.e: Col 4, lines 26-45)*, receiving scan data from a biometric scan (*i.e: Col 4, lines 40-45, wherein scanned fingerprint is received from the sensor*);

comparing the scan data to the biometric data to determine whether the data match (*i.e: Col 4, lines 40-45, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob)*; and

responsive to a determination that the scan data matches the biometric data *(i.e: Col 4, lines 40-45)*, wirelessly sending a code for authentication that the code is legitimate by a trusted authority, the code uniquely identifying the integrated device (*i.e: Fig. 4, step 60;column 5, lines 57-58; column 6, line 66-column 7, line 34, wherein the generated CRC encrypted with the door's public key and the fob's private key is interpreted as code uniquely identifies the integrated device*).

Regarding claim 2, Hsu also discloses the method of claim 1, wherein the code is registered with the trusted authority, and the code can be authenticated to a third party by the trusted authority (*i.e: column 6, lines 2-9; column 7, line 5-16*).

Regarding claim 5, Hsu also discloses the method of claim 1, wherein the code indicates that the biometric verification was successful (*i.e: Col 7, lines 17-34, wherein when the CRC is compared with the CRC in the database resulting a match, the door will open to allow access, which corresponds to the code indicates that the biometric verification was successful)*.

Regarding claim 7, Hsu also discloses the method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user *(i.e: Col 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person*).

Regarding claim 8, Hsu also discloses the method of claim 1, further comprising: establishing a secure communication channel prior to sending the code for authentication (*i.e: Col 6, lines 42-67; Col 7, lines 1-34, wherein exchanging of keys is performed prior to sending the CRC, which corresponds to establishing a secure communication channel prior to sending the code for authentication*).

Regarding claim 9, Hsu also discloses the method of claim 1, further comprising:

receiving a request for the code without a request for biometric verification (*i.e: Fig. 4, step 60; Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" encrypted with the door's public key and the fob's private key which corresponds to a "code" is transmitted)*; and

responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data *(i.e: Fig. 4, step 60; Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" encrypted with door's public key and fob's private key, which corresponds to a "code" is transmitted)*.

Claim 10 is rejected for the same rationale as claim 1 above.

Claim 12 is rejected for the same rationale as claim 2 above.

Claim 19 is rejected for the same rationale as claim 1 above.

Regarding claim 20, Hsu also discloses the system of claim 19, wherein 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 (*i.e: column 4, lines 19-25; 40-44*).

Regarding claim 21, Hsu also discloses the system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code (i.e: column 5, lines 42-47, *wherein the no-match signal is generated, no further processing is performed, thus no CRC will be generated, and available to send*).

Claim Rejections - 35 USC § 103

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

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

Claims 15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al (US Patent 6,041,410, hereinafter Hsu).

Regarding claim 15, Hsu discloses a method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with a trusted authority (*i.e: column 6, lines 2-9; column 7, line 5-37*);

requesting authentication of the code by the trusted authority and the authentication determining whether the code is legitimate (*i.e: column 6, lines 2-9; column 7, line 5-16*);

in response to the authentication result being positive, providing access to an application (*i.e: column 7, lines 30-34*).

Hsu does not explicitly disclose receiving an authentication result from the trusted authority;

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include this step of receiving an authentication result from the trusted authority to clearly indicate the status of the authentication result to the user.

Regarding claim 18, Hsu also discloses the method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key (i.e: *i.e: Col 6, lines 42-67; Col 7, lines 1-34; Fig. 4, step 60; column 5, lines 57-58; column 6, line 66-column 7, line 34*).

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, and further in view of Saito et al (US 20040129787 A1, hereinafter Saito)

Regarding claim 3, Hsu discloses the method of claim 1.

Hsu does not disclose registering an age verification for the user in association with the code.

However, Saito discloses registering an age verification for a user in association with a code (*i.e: [0082]-[0083] [0164], wherein date of birth is registered along with other personal data)*.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the authentication method of Hsu in order to enhance the reliability and security of the authentication.

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

Regarding claim 14, Hsu discloses the integrated device of claim 10.

Hsu does not disclose wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

However, Saito discloses the verification module comprises an LED to be activated for requesting the biometric scan (*i.e: [0040]-[0056], wherein a LED is used to prompt user for biometric data*).

Claim 17 is rejected for the same rationale as claim 3 above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE7MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

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 Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	181	726/27.ccls. and (biometric$6)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:42
L2	1	726/27.ccls. and (biometric$6) with (authenticat$4 with (device near3 ID))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
L3	34	726/27.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:43
L4	71	713/176.ccls. and (biometric $6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
L5	0	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and@ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
L6	52	713/176.ccls. and (biometric $6) with (authenticat$4 with (device)) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:44
L7	152	"380"/$.ccls. and (biometric$6) with (authenticat$4 with (device))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
L8	102	l7 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:46
L9	9	l7 and 380/286.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:48
L10	15	(john near4 giobbi).inv. and (biometric$4 with authenticat $4)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50
L11	7	(john near4 giobbi).inv. and (biometric$4 with authenticat $4).clm.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 13:50

S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21
S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36
S6	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S7	63	S6 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
S8	2	S6 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S9	2	S6 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
S10	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S11	621	S10 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
S12	90	S11 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
S13	182	S11 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58

S14	199	S11 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S15	17	S14 not S13	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
S16	36	S11 and (portable (device or apparatus or system)) and S14	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01
S17	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S18	2443	S17 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
S19	0	S17 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S20	3168	S17 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
S21	298	S20 and ((authenticat$3 or verif $6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S22	38	S20 and ((authenticat$3 or verif $6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
S23	23	S20 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S24	23	S20 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S25	5	713/186.ccls. and ((authenticat $4) with code with (identif$6) near6 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:23
S26	70	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:50

S27	31	713/186.ccls. and ((authenticat $4) with (card or device) near3 ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 10:51
S28	38	713/186.ccls. and ((verif$7) with (card or device) near3 ID)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S29	30	S28 not S27	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:09
S30	745	713/186.ccls. and (authenticat $4 with (device or apparatus or card))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S31	562	713/186.ccls. and (authenticat $4 with device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S32	445	713/186.ccls. and (authenticat $4 near5 device)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S33	228	713/186.ccls. and (authenticat $4 near5 device) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:17
S34	3	713/186.ccls. and (authenticat $4 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:22
S35	1	713/186.ccls. and (authenticat $4) with (identif$7 near5 device ID) and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:27
S36	3	11/314199	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/11/07 11:49

11/7/2009 1:56:00 PM
C:\ Documents and Settings\ pvu3\ My Documents\ EAST\ Workspaces\ 11314199.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009	11/07/2009							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	-							
	5	✓	✓							
	6	✓	-							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	-							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	-							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
380	23	4/20/2009	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Googlel Search	4/20/2009; 11/9/2009	PVU
East text search	4/20/2009; 11/9/2009	PVU
Inventor names search	4/20/2009	PVU
Class 380/286; 713/176, 186; 726/27	4/20/2009; 11/9/2009	PVU
Spoke to Tod Swan in WQAS regarding 101 issue for claim 15	4/22/2009	PVU
PLUS search	11/9/2009	PVU

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/314,199		2437	

OC000000037299486

Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 89194 on 08/10/2009

- **Correspondence Address**
- **Maintenance Fee Address**
- **Power of Attorney Address**

The address of record for Customer Number 89194 is:

89194
Proxense/Fenwick
Silicon Valley Center
801 California Street
Mountain View, CA 94041

PART 1 - ATTORNEY/APPLICANT COPY

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh TranVu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	25000-11062

CERTIFICATE OF ELECTRONIC (EFS-WEB) TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.8(a)(i)(C) from the Pacific Time Zone of the United States on the local date shown below.

Dated: July 27, 2009 By: /Fengling Li/

Fengling Li, Reg. No. 62,962

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

AMENDMENT A UNDER 37 C.F.R. §1.111

The following amendment and remarks are in response to the Office Action dated April 27, 2009, which set a shortened statutory period for response that expires on July 27, 2009.

AMENDMENTS TO THE SPECIFICATION

On page 1, please amend paragraph [0003] as follows:

--[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 allowing 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~~ user often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.--

On page 7, please amend paragraph [0026] as follows:

--[0026] 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]] 226, 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.--

On page 8, please amend paragraph [0027] as follows:

--[0027] 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]] 220. 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.--

On page 9, please amend paragraph [0029] as follows:

--[0029] 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]] 224 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.--

On page 10, please amend paragraph [0033] as follows:

--[0033] 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]] 230 can be optimized for low-power usage by, for example, using short-range transceivers. RF communication module 230 can actively send out connection requests, or passively detect connection requests.--

On page 11, please amend paragraph [0036] as follows:

--[0036] 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~~ serves 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.--

AMENDMENTS TO THE CLAIMS

Claims 1-2, 10, 12, 15 and 19 are amended herein. Claims 4, 6, 11 and 16 are canceled. All pending claims are produced below.

1. (Currently Amended) 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 in a storage element that is written once and is not altered subsequently;

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 that the code is legitimate by a trusted authority, the code uniquely identifying the integrated device.

2. (Currently Amended) The method of claim 1, wherein the code is registered with [[a]] the trusted authority, and the code can be authenticated to a third party by the trusted authority.

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

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

4. (Canceled)

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled)

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

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.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user in a tamper-resistant format; the persistent storage being written once and being not altered subsequently;

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 that the code is legitimate by a trusted authority, the code uniquely identifying the integrated device.

11. (Canceled)

12. (Currently Amended) The integrated device of claim 10, wherein the code is registered with [[a]] the trusted authority, wherein the code can be authenticated to a third party by the trusted authority.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with a trusted authority;

requesting authentication of the code by the trusted authority and the authentication determining whether the code is legitimate;

receiving an authentication result from the trusted authority; and

in response to the authentication result being positive, providing access to an application.

16. (Canceled)

17. (Currently Amended) The method of claim [[16]] 15, further comprising:

registering a date of birth or age with the trusted authority.

18. (Original) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) 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, the code being associated with the verified user;

an authentication module to receive the code and send the code to a trusted authority for authentication to determine whether the code is legitimate, and responsive to the code being authenticated, allowing the user to access an application.

20. (Original) The system of claim 19, wherein 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.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

REMARKS

The specification was objected to informalities. Applicants have amended the specification to correct the informalities. The Examiner is asked to withdraw the objection of the specification.

Claims 1-21 were presented and stand rejected. Claims 1-2, 10, 12, 15 and 19 are amended herein. Claims 4, 6, 11 and 16 are canceled. No new matter is added in view of the amendments to claims 1-2, 10, 12, 15, 17 and 19.

Claims 1, 10 and 11 were rejected under 35 USC § 112, ¶ 2 as not specifically pointing out and distinctly claiming the subject matter that the Applicant regards as the invention. Claim 11 is canceled. The rejection of claim 11 is now moot. Applicant has amended claims 1 and 10 to recite a persistent storage as being written once and being not altered subsequently. Thus, claims 1 and 10 as amended distinctly claim the subject matter that the Applicant regards as the invention. The Examiner is asked to withdraw the rejection of claims 1 and 10 under 35 USC § 112, ¶ 2.

Claims 15-18 were rejected under 35 USC § 101 as not qualified as a statutory process. Applicant has amended claim 15 to recite a computer processor to execute method steps. Applicant submits that amended claim 15 recites statutory subject matter. Dependent claims 16-18 depend from claim 15. Thus, claims 16-18 also recite statutory subject matter by virtue of their dependency of claim 15.

Claims 1, 4-11, 15 and 18 were rejected under 35 USC § 102(b) as being anticipated by Hsu et al. (U.S. Patent No. 6,041,410) ("Hsu"). Claims 2-3, 12-14, 16-17 and 19-21 were

rejected under 35 USC § 103(a) as being unpatenable by Hsu and further in view of Saito et al. (US 2004/0129787 A1) ("Saito"). These rejections are respectfully traversed.

The claimed invention relates to authentication responsive to biometric verification of a user being authenticated. For example, as amended, claim 1 now recites (with emphasis added):

> A method for verifying a user during authentication of an integrated device, comprising the steps of:
>
> permanently storing biometric data for the user in a tamper-resistant format in a storage element that is written once and is not altered subsequently;
>
> 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 that the code is legitimate by a trusted authority, the code uniquely identifying the integrated device**.

The claimed invention advantageously allows user authentication to be bolstered with highly reliable biometric verification of the user in a single integrated device. The claimed invention further advantageously provides **enhanced security** by authenticating the code by a trusted authority responsive to a determination that the biometric scan data of the user matches the stored biometric data (Specification, ¶¶[0038]-[0039]).

Hsu does not disclose the claimed features. Specifically, Hsu does not disclose "responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication that the code is legitimate by a trusted authority."

Hsu discloses a method for verifying the identity of a person seeking access to a protected property (Abstract) using a portable device. The Examiner acknowledges that Hsu does not disclose authenticating the code by a trusted authority and depends on Saito to disclose the claimed feature. However, Saito does not remedy the deficiencies of Hsu.

Saito discloses a method for biometric verification of identity of a user (Abstract). The Examiner cited paragraphs [0095]-[0098] of Saito as disclosing the claimed feature. These portions of Saito describe that if there is a match between the captured biometric data and the locally stored biometric data, an authentication server uses a challenge character sequence as a Hash code to encrypt the related information (e.g., IP address of the client terminal). The encrypted related information is used as a challenge response. The Examiner equates Saito's Hash code to the claimed code and Saito's authentication server to the claimed trusted authority. Assume, *arguendo*, that this is correct.

Saito's hash code merely references the Saito's challenge character sequence. Saito's hash code does not uniquely identify any integrated device. Therefore, Saito's hash code is not equivalent to the claimed code. Further, Saito's authentication server merely determines whether **the user's identity** has in fact been authenticated using the challenge response (¶[0098]), and such determination does not disclose an authentication that **the hash code** is legitimate. Saito's authentication is neither equivalent to the claimed authentication nor disclosing the claimed authentication. Thus, Saito does not disclose or teach sending a code **for authentication that the code is legitimate by a trusted authority, and the code uniquely identifying the integrated device** as claimed.

Thus, claim 1 is not anticipated by Hsu and is not obvious in view of the art of records. Thus, claim 1 is patentable over the cited references, and claim 1 should be allowed.

Independent claims 10, 15 and 19 are amended to recite similar language as claim 1. Since claim 1 (as amended) is not obvious in view of any combination with art of record, claims 10, 15 and 19 (as amended) are allowable for at least the same reasons. Thus, claims 10, 15 and 19 are in a condition for allowance.

Dependent claims 2-3, 5, 7-9, 12-14, 17-18 and 20-21 depend from claims 1, 10, 15 and 19, shown above to be patentable over the cited references, and contain additional patentably distinguishable limitations. Thus, claims 2-3, 5, 7-9, 12-14, 17-18 and 20-21 are patentably distinguishable over the combination of the cited references for at least the same reasons, as well as the additional patentable limitations they recite. Claims 2-3, 5, 7-9, 12-14, 17-18 and 20-21 are in a condition for allowance.

Applicant respectfully submits that for at least these reasons claims 1-3, 5, 7-10, 12-15 and 17-21 are patentably distinguishable over the cited reference. Therefore, Applicant respectfully requests that Examiner reconsider the rejection, and withdraw it. In addition, Applicant respectfully invites Examiner to contact Applicant's representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully submitted,
JOHN J. GIOBBI

Dated: July 27, 2009 By: /Fengling Li/

Fengling Li, Reg. No. 62,962
Patent Agent
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel. (650) 335-7182
Fax (650) 938-5200

Electronic Acknowledgement Receipt

EFS ID:	5772709
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	00758
Filer:	Fengling Li
Filer Authorized By:	
Attorney Docket Number:	25000-11062
Receipt Date:	27-JUL-2009
Filing Date:	20-DEC-2005
Time Stamp:	15:41:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		11062_Amendment_A.pdf	139241 f357dbc54b1c917fd0e000f7fd27563d70c1d277	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	4
	Claims	5	8
	Applicant Arguments/Remarks Made in an Amendment	9	12
Warnings:			
Information:			
	Total Files Size (in bytes):	139241	

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

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

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

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

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	
11/314,199	12/20/2005	☐ To be Mailed

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			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 07/27/2009	(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 ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 17	Minus	** 21	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

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

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

Legal Instrument Examiner:
/RUTH M. LLOYD/

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.
11/314,199	12/20/2005	John J. Giobbi	25000-11062	4469

758 7590 04/27/2009
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER
VU, PHY ANH TRAN

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
04/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	11/314,199	GIOBBI, JOHN J.	
	Examiner	Art Unit	
	PHY ANH VU	2437	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

1)☒ Responsive to communication(s) filed on *20 December 2005*.

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

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

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

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

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

Application Papers

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

10)☒ The drawing(s) filed on *20 December 2005* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

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

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

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

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

a)☐ All b)☐ Some * c)☐ None of:

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

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

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

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

Attachment(s)

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

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/16/2006,10/30/2006,1/16/2007,5/23/2007,5/23/2007*.

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

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 11/314,199, filed on 12/20/2005 is presented for examination by the examiner.

Examiner Notes

Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Specification

The specification of the disclosure is objected to because of the following reasons:

[0003] recites “a uses often…”, it appears that the word “uses” is misspelled of the word “**user**”.

[0026] recites “persistent storage **240**”, wherein “persistent storage” in the drawing is labeled as “persistent storage **226**”, consistent in labeling is requested.

[0027] recites “…biometric portion **210**”, wherein, it should have recited as “…biometric portion **220**” to be consistent with the drawing.

[0029] recites "...validation module **214**”, wherein, it should have recited as “validation module **224**”.

[0033] recites “…RF communication **220**”, wherein it should have recited as ““…RF communication **230**”

[0036] recites “…authentication module **servers** as…” it appears that the word “servers” here is intended as the word “**serves**”. Appropriate corrections are required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 10, and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 and 10 recite “persistently storing” and “a persistent storage” respective, it is not clear as to what degree of persistent the applicant intends convey about this storage.

Claim 11, recites "the persistent storage permanently stores", it is not clear to the examiner what the applicant intends to claim here.

To expedite the prosecution of the application, examiner will interpret these as storing the biometric data in a storage that can not be erased easily by accident (ie: ROM)

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.

Claim 15 is rejected under 35 U.S.C. 101 the claimed invention is directed to non-statutory subject matter. .

Claim 15 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively

recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

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

Claims 16-18 are rejected under 35 U.S.C. 101 as non-statutory for at least the reason stated above. Claims 16-18 are depended on claim 15; however, they do not add any feature or subject matter that would solve any of the non-statutory deficiencies of claim 15.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1,4-11, 15, 18 are rejected under 35 U.S.C. 102(b) as being anticipated by **Hsu et al. (US 6,041,410 A1, hereinafter Hsu)**.

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 (i.e: ***Col 4, lines 15-25; Col 7, lines 56-67; wherein biometric data of the user is stored in a device that is highly resistant to tampering***);

responsive to receiving a request for biometric verification of the user (***i.e: Col 4, lines 26-45***), receiving scan data from a biometric scan (***i.e: Col 4, lines 40-45, wherein scanned fingerprint is received from the sensor***);

comparing the scan data to the biometric data to determine whether the data match (***i.e: Col 4, lines 40-45, wherein the person's fingerprint is compared with a reference fingerprint image stored in the fob***); and

responsive to a determination that the scan data matches the biometric data (***i.e: Col 4, lines 40-45***), wirelessly sending a code for authentication (***i.e: Col 4, lines 26-56; Col 5, lines 48-67; Col 6, 1-9, wherein a " fingerprint CRC " corresponds to a "code" for authentication is transmitted from the fob to the door wirelessly***).

Regarding claim 4, Hsu discloses the method of claim 1, wherein the code uniquely identifies the integrated device (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; wherein the CRC uniquely identifies the fob, which corresponds to the code uniquely identifies the integrated device***).

Regarding claim 5, Hsu also discloses the method of claim 1, wherein the code indicates that the biometric verification was successful (***i.e: Col 7, lines 17-34, wherein when the CRC is compared with the CRC in the database resulting a match, the***

door will open to allow access, which corresponds to the code indicates that the biometric verification was successful).

Regarding claim 6, Hsu also discloses the method of claim 1, wherein persistently storing biometric data comprises:

Permanently storing biometric data (***i.e: Col 4, lines 15-25; Col 5, lines 20-47; Col 7, lines 56-67; wherein biometric data is stored in a device that is highly resistant to tampering***)

Regarding claim 7, Hsu also discloses the method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user (***i.e: Col 4, lines 15-56, wherein the person's fingerprint and the fingerprint image stored in fob are obtained by the same person***).

Regarding claim 8, Hsu also discloses the method of claim 1, further comprising: establishing a secure communication channel prior to sending the code for authentication (***i.e: Col 6, lines 42-67; Col 7, lines 1-34, wherein exchanging of keys is performed prior to sending the CRC, which corresponds to establishing a secure communication channel prior to sending the code for authentication***).

Regarding claim 9, Hsu also discloses the method of claim 1, further comprising:

receiving a request for the code without a request for biometric verification (***i.e: Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" which corresponds to a "code" is transmitted***); and

responsive to receiving the request for the code without a request for biometric verification (***i.e: Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" which corresponds to a "code" is transmitted***),

sending the code without requesting the scan data(***i.e: Col 5, lines 47-67; Col 6, lines 1-24, wherein only "CRC" which corresponds to a "code" is transmitted)*** .

Claim 10 is rejected for the same rationale as claim 1.

Claim 11 is rejected for the same rationale as claim 6

Regarding claim 15, Hsu discloses a method for authenticating a verified user, comprising:

receiving a code associated with a biometrically verified user (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; Col 7, lines 17-34; wherein CRC of the authenticated fingerprint is received***);

requesting authentication of the code (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; Col 7, lines 17-34***);

receiving an authentication result (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; Col 7, lines 17-34)***; and

in response to the authentication result being positive, providing access to an application (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; Col 7, lines 17-34; wherein when the CRC matched with the CRC in the database, the door opens and allows access, which corresponds to in response to the authentication result being positive, providing access to an application***).

Regarding claim 18, Hsu discloses the method of claim 15, further comprising:

establishing a secure communications channel with a biometric key (***i.e: Col 6, 35-49, wherein key exchanged is performed in communication between the door and the fob, which corresponds to establishing a secure communications channel with a biometric key***), wherein the code associated with the biometrically verified user is received from the biometric key (***i.e: Col 5, lines 57-67; Col 6, lines 1-9; Col 7, lines 17-34, wherein CRC is transmitted from the fob, which corresponds to the code associated with the biometrically verified user is received from the biometric key***).

Claim Rejections - 35 USC § 103

Claims 2, 3, 12- 14, 16-17, 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu as applied to claim 1 above, and further in view of Saito et al (US 20040129787 A1, hereinafter Saito)

Regarding claim 2, Hsu discloses the method of claim1.

Hsu does not disclose the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.

However, **Saito discloses** the code is registered with a trusted authority (***i.e: [0095]-[0098], wherein "Hash code" corresponds to the "code" is forwarded to "authentication server", which corresponds to a "trusted authority"***), and the code can be authenticated to a third party by the trusted authority (***[0095]-[0101]***).

Regarding claim 3, Hsu discloses the method of claim 1.

Hsu does not disclose registering an age verification for the user in association with the code.

However, **Saito discloses** registering an age verification for the user in association with the code. (***i.e: [0082]-[0083] [0164], wherein date of birth is registered along with other personal data***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase the reliability and security of authentication.

Regarding claim 12, Hsu discloses the integrated device of claim10.

Hsu does not disclose the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.

However, **Saito discloses** the code is registered with a trusted authority (***i.e: [0095]-[0098], wherein "Hash code" corresponds to the "code" is forwarded to "authentication server", which corresponds to a "trusted authority"***), and the code can be authenticated to a third party by the trusted authority (***[0095]-[0101]***).

Regarding claim 13, Hsu discloses the integrated device of claim 12. Hsu does not disclose registering an age verification for the user in association with the code.

However, **Saito discloses** registering an age verification for the user in association with the code. (***i.e: [0082]-[0083] [0164], wherein date of birth is registered along with other personal data***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase the reliability and security of authentication.

Regarding claim 14, Hsu discloses the integrated device of claim 10.

Hsu does not disclose wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

However, **Saito discloses** the verification module comprises an LED to be activated for requesting the biometric scan (***i.e: [0040]-[0056], wherein a LED is used to prompt user for biometric data***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase reliability and security of authentication

Regarding claim 16, Hsu discloses the method of claim 15.

Hsu does not disclose further comprising:

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.

However, **Saito discloses** further comprising:

registering the code with a trusted authority (***i.e: [0095]-[0098], wherein "Hash code" corresponds to the "code" is forwarded to "Web Interface of authentication server" , which corresponds to a "trusted authority"***), wherein requesting authentication of the code comprises providing the code to the trusted authority (***i.e: [0095]-[0098]***) and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority (***i.e: [0095]-[0101]***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase the reliability and security of authentication and authorization by providing a trusted entity that can confirm the user and device are authentic.

Regarding claim 17, Hsu discloses the method of claim 16.

Hsu does not disclose registering a date of birth or age with the trusted authority.

However, **Saito discloses** registering a date of birth or age with the trusted authority (***i.e: [0082]-[0083] [0164], wherein date of birth is registered along with other personal data***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase the reliability and security of authentication.

Regarding claim 19, A system, comprising:

Hsu discloses a biometric key to store biometric data for a user in a tamper resistant format (***i.e: Col 4, lines 15-26; Col 7, lines 56-67; wherein the "fob" corresponds to a "biometric key" stores biometric data, of the person seeking access in a highly resistant tampering environment***), and if scan data can be verified as being from the user by comparing the scan data to the biometric data (***i.e:***

Col 4, lines 40-46, wherein when the fingerprint matches with the fingerprint image stored in the fob, which corresponds verified as being from the user by comparing the scan data to the biometric data), wirelessly sending a code (***i.e: Col 5, lines 48-67; Col 6, lines 1-9; Col 7, lines 17-37, wherein "CRC" which corresponds to a "code" is sent wirelessly to the door***).

an authentication module to authenticate the user for access to an application (***i.e: Col 7, lines 17-34, wherein when the "CRC" matches with the "CRC" stored in the database, then access is granted***)

Hsu does not disclose sending the code to a trusted authority for authentication.

However, **Saito discloses** sending the code to a trusted authority for authentication and responsive to the code being authenticated (***i.e: [0095]-[0101], wherein "Hash code" corresponds to "code", and "authentication server" corresponds to a "trusted authority"***), allowing the user to access an application (***i.e: [0095]-[0101]***).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Saito into the system of Hsu in order to increase the reliability and security of authentication and authorization by providing a trusted entity that can confirm the user and device are authentic.

Regarding claim 20, Hsu in view of Saito discloses the system of claim 19, wherein the biometric key receives an authentication request from the authentication

module (***i.e: Col 5, lines 57-67; Col 6, lines 1-49; Col 7, lines 17-34***; ***wherein the "door" corresponds to the "authentication module" request authentication from the "fob" which corresponds to the "biometric key"***), and in response, requests a biometric scan from the user to generate the scan data ***(i.e: Col 4, lines 14-46, wherein the user's fingerprint is used to generate the scan data***).

Regarding claim 21, Hsu in view of Saito discloses the system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code (***i.e: Saito Col. 5, lines 1-47, wherein when the comparison of images result in no match, which corresponds to biometric key cannot verify the scan data as being from the user, the CRC generator will not be activated to generate CRC, therefore, no CRC will be generated, and available to send***).

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 Mon-Thr 7:30-5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. 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 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Notice of References Cited	Application/Control No. 11/314,199	Applicant(s)/Patent Under Reexamination GIOBBI, JOHN J.	
	Examiner PHY ANH VU	Art Unit 2437	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,041,410	03-2000	Hsu et al.	713/186
*	B	US-2004/0129787	07-2004	Saito et al.	235/492
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

✓	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	04/13/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11314199	GIOBBI, JOHN J.
	Examiner	**Art Unit**
	PHY ANH VU	2437

SEARCHED

Class	Subclass	Date	Examiner
380	23	4/20/2009	PVU

SEARCH NOTES

Search Notes	Date	Examiner
Googlel Search	4/20/2009	PVU
East text search	4/20/2009	PVU
Inventor names search	4/20/2009	PVU
Class 235/380, 492; 713/176; 726/27	4/20/2009	PVU
Spoke to Tod Swan in WQAS regarding 101 issue for claim 15	4/22/2009	PVU

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1167	713/155.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
L2	63	l1 and (portable (device or system apparatus))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:48
L3	2	l1 and fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
L4	2	l1 and fob	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:50
L5	1070	fob and biometric	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
L6	621	l5 and @ad<"20051201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:51
L7	90	l6 and (portable (device or apparatus or system))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:52
L8	182	l6 and (age or date of birth)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:58
L9	199	l6 and (age or date of birth or birth date)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
L10	17	l9 not l8	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 09:59
L11	36	l6 and (portable (device or apparatus or system)) and l9	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:01

L12	6175	biometric and (birth date or age)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
L13	2443	l12 and @ad<"20040101"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:02
L14	0	l12 and @ad<"2001201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
L15	3168	l12 and @ad<"20041201"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:03
L16	298	l15 and ((authenticat$3 or verif$6) with (age or birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
L17	38	l15 and ((authenticat$3 or verif$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:05
L18	23	l15 and ((compar$6) with (birth date))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
L19	23	l15 and ((compar$6) with (birth date or date of birth))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/13 10:07
S1	2	"20060143441".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 08:34
S2	2	"6041410".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:40
S3	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/08 13:42
S4	2	"20040129787".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/09 10:21

S5	2	"20060140405".pn.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT	ADJ	ON	2009/04/10 11:36

4/13/2009 11:32:23 AM
C:\Documents and Settings\pvu3\My Documents\EAST\Workspaces\11314199.wsp

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. 4469

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/314,199	12/20/2005 **RULE**	713	2437	25000-11062

APPLICANTS
John J. Giobbi, Bend, OR;

**** CONTINUING DATA ***************************
This appln claims benefit of 60/637,538 12/20/2004
and claims benefit of 60/652,765 02/14/2005

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/03/2006

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		OR	6	21	4
Verified and Acknowledged	/PHY ANH TRAN VU/ Examiner's Signature	Initials				

ADDRESS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041
UNITED STATES

TITLE
Biometric personal data key (pdk) authentication

FILING FEE RECEIVED		
690	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).

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

OIPE JAN 16 2007 PATENT & TRADEMARK OFFICE

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	~~2137~~ 2437
Examiner Name	~~Emmanuel Lionel Moise~~ Phy Anh Vu
Attorney Docket Number	25000-11062

Sheet	1	of	2

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document No. Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		US-		

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
/P.V./	C1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.smartcardalliance.org/pages/publications-identity>	
	C2	"Applying Biometrics to Door Access," Security Magazine, September 26, 2002 [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.securitymagazine.com/CDA/Articles/Technologies/3ae610eaa34d8010VgnVCM100000f932a8c0____>	
	C3	"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.biopay.com/faqs-lowes.asp>	
	C4	MCIVER, R. et al., "Identification and Verification Working Together," Bioscrypt™, August 27, 2004, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>	
	C5	NILSSON, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, April 2004, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>	
/P.V./	C6	NORDIN, B., "Match-On-Card Technology," Precise™ Biometrics, White Paper, April 2004, [online] [Retrieved on January 7, 2007] Retrieved from the	

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1686538.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	~~2137~~ 2437
				Examiner Name	~~Emmanuel Lionel Moise~~ Phy Anh Vu
Sheet	2	of	2	Attorney Docket Number	25000-11062

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
/P.V./		Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf>	
	C7	"SAFModule™: A Look Into Strong Authentication," saflink Corporation, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>	
	C8	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>	
/P.V./	C9	WADE, W., "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, April 21, 2003, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>	

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1686538.1

OIPE IAP29
MAR 16 2006
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	~~2131~~ 2437
Examiner Name	~~Not Yet Known~~ Phy Anh Vu
Attorney Docket Number	25000-11062

Sheet	1	of	4

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document No. Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
/P.V./	A1	US-6,950,941	09-27-2005	Lee et al.
	A2	US-6,806,887	10-19-2004	Chernock et al.
	A3	US-6,804,825	10-12-2004	White et al.
	A4	US-6,775,655	08-10-2004	Peinado et al.
	A5	US-6,711,464	03-23-2004	Yap et al.
	A6	US-6,683,954	01-27-2004	Searle
	A7	US-6,667,684	12-23-2003	Waggamon et al.
	A8	US-6,647,417	11-11-2003	Hunter et al.
	A9	US-6,632,992	10-14-2003	Hasegawa
	A10	US-6,628,302	09-30-2003	White et al.
	A11	US-6,564,380	05-13-2003	Murphy
	A12	US-6,563,805	05-13-2003	Ma et al.
	A13	US-6,546,418	04-08-2003	Schena et al.
	A14	US-6,529,949	03-04-2003	Getsin et al.
	A15	US-6,510,350	01-21-2003	Steen et al.
	A16	US-6,490,443	12-03-2002	Freeny, Jr.
	A17	US-6,480,188	11-12-2002	Horsley
	A18	US-6,446,130	09-03-2002	Grapes
	A19	US-6,434,535	08-13-2002	Kupka et al.
	A20	US-6,425,084	07-23-2002	Rallis et al.
	A21	US-6,424,715	07-23-2002	Saito
	A22	US-6,411,307	06-25-2002	Rosin et al.
	A23	US-6,401,059	06-04-2002	Shen et al.
	A24	US-6,397,387	05-28-2002	Rosin et al.
	A25	US-6,392,664	05-21-2002	White et al.
	A26	US-6,385,596	05-07-2002	Wiser et al.
/P.V./	A27	US-6,381,747	04-30-2002	Wonfor et al.

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application No.	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	~~2131~~ 2437
				Examiner Name	~~Not Yet Known~~ Phy Anh Vu
Sheet	2	of	4	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
/P.V./	A28	US-6,367,019	04-02-2002	Ansell et al.
	A29	US-2002/0015494 A1	02-07-2002	Nagai et al.
	A30	US-6,336,142	01-01-2002	Kato et al.
	A31	US-2002/0007456 A1	01-17-2002	Peinado et al.
	A32	US-6,336,121	01-01-2002	Lyson et al.
	A33	US-6,295,057	09-25-2001	Rosin et al.
	A34	US-6,266,415	07-24-2002	Campinos et al.
	A35	US-6,247,130	06-12-2001	Fritsch
	A36	US-6,219,109	04-17-2001	Raynesford et al.
	A37	US-6,209,089	03-27-2001	Selitrennikoff et al.
	A38	US-6,161,179	12-12-2000	Seidel
	A39	US-6,148,142	11-14-2000	Anderson
	A40	US-6,104,334	08-15-2000	Allport
	A41	US-6,088,730	07-11-2000	Kato et al.
	A42	US-6,055,314	04-25-2000	Spies et al.
	A43	US-6,035,329	03-07-2000	Mages et al.
	A44	US-6,035,038	03-07-2000	Campinos et al.
	A45	US-5,991,399	11-23-1999	Graunke et al.
	A46	US-5,928,327	07-27-1999	Wang et al.
	A47	US-5,898,880	04-27-1999	Ryu
	A48	US-5,892,825	04-06-1999	Mages et al.
	A49	US-5,857,020	01-05-1999	Peterson, Jr.
	A50	US-5,825,876	10-20-1998	Peterson, Jr.
	A51	US-5,784,464	07-21-1998	Akiyama et al.
	A52	US-5,666,412	09-09-1997	Handelman et al.
	A53	US-5,644,354	07-01-1997	Thompson et al.
/P.V./	A54	US-5,629,980	05-13-1997	Stefik et al.

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	~~2131~~ 2437
Examiner Name	~~Not Yet Known~~ PhyPhy Anh Vu
Attorney Docket Number	25000-11062

Sheet 3 of 4

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document No. Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
/P.V./	A55	US-5,619,251	04-08-1997	Kuroiwa et al.
	A56	US-5,450,489	09-12-1995	Ostrover et al.
	A57	US-5,422,632	06-06-1995	Bucholtz et al.
	A58	US-5,392,433	02-21-1995	Hammersley et al.
	A59	US-5,296,641	03-22-1994	Stelzl
	A60	US-5,187,352	02-16-1993	Blair et al.
/P.V./	A64	US-4,759,060	07-19-1988	Hayashi et al.

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]
/P.V./	B1	WO 05/086802 A2	09-22-2005	Margent Development, LLC	
	B2	WO 05/050450 A1	06-02-2005	Margent Development, LLC	
	B3	WO 01/77790 A1	10-18-2001	Thomson Multimedia	
	B4	WO 01/75876 A1	10-11-2001	Thomson Multimedia	
	B5	WO 01/22724 A1	03-29-2001	Thomson Multimedia	
/P.V./	B6	WO 00/62505 A1	10-19-2000	Thomson Multimedia	

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
/P.V./	C1	ANTONOFF, Michael, "Visiting Video Valley," Sound & Vision, Pages 116 and 118-119, Nov. 2001.	
	C2	Article, "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, July 25, 2000.	
	C3	Article, "Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, August 14, 2000.	
	C4	BLUM, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, (October 2000), 24-27.	
/P.V./	C5	DEBOW, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p10, November, 1989.	

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application No.	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	~~2131~~ 2437
				Examiner Name	~~Not Yet Known~~ Phy Anh Vu
Sheet	4	of	4	Attorney Docket Number	25000-11062

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
/P.V./	C6	DENNIS, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, December 2, 1999, 2 pages.	
	C7	FASCA, Chad, "The Circuit," Electronic News, 45(45) (November 8, 1999), 20.	
	C8	Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, January 18, 1996.	
	C9	LAKE, Matt, "Downloading for Dollars," Sound & Vision, (November 2000), 137-138.	
	C10	LEWIS, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, November 16, 1995.	
	C11	Notification of the International Search Report and Written Opinion, PCT/US04/38124, April 7, 2005, 10 pages.	
	C12	PAGET, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, (Dec. 1999), 4 pgs.	
	C13	Press Release, "Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, January 8, 2002.	
	C14	Press Release, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002.	
	C15	Press Release, "Thompson Bets on Smart Cards For Video Encryption," www.informationweek.com, June 7, 2001.	
	C16	Press Release, "Thompson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001.	
	C17	"Say Hello to Bluetooth," Bluetooth Web site, 4 pages.	
	C18	SAPSFORD, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, (August 14, 2000), B1	
	C19	VAN WINKLE, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, (January 2000), 148-153.	
	C20	WALLACE, Bob, "The Internet Unplugged," InformationWeek, 765(22), (December 13, 1999), 22-24.	
/P.V./	C21	WEBER, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, (July 24, 2000), B1.	

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Emmanuel Lionel Moise
GROUP ART UNIT:	2137
ATTY. DKT. NO.:	25000-11062

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☒ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last

occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:

- ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
- ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;

☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any

individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☒ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

☒ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,
JOHN J. GIOBBI

Dated: May 23, 2007

By: /Greg T. Sueoka/

Greg T. Sueoka, Reg. No.: 33,800
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7194
Fax.: (650) 938-5200

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	~~2137~~ 2437
				Examiner Name	~~Emmanuel Lionel Moise~~ Phy Anh Vu
Sheet	1	of	1	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
/P.V./	A1	US-2004/0129787 A1	07-08-2004	Saito et al.
/P.V./	A2	US-2002/0109580 A1	08-15-2002	Shreve et al.
/P.V./	A3	US-2002/0073042 A1	06-13-2002	Maritzen et al.
/P.V./	A4	US-6,041,410	03-21-2000	Hsu et al.
/P.V./	A5	US-5,991,749	11-23-1999	Morril Jr.

/P.V./ FOREIGN PATENT DOCUMENTS					
		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
/P.V./	C1	PCT International Search Report and Written Opinion, PCT/US05/43447, February 22, 2007, 7 pages.	
/P.V./	C2	PCT International Search Report and Written Opinion, PCT/US05/46843, March 1, 2007, 10 pages.	

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1724469.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	~~2131~~ 2437
				Examiner Name	~~Not Yet Known~~ Phy Anh Vu
Sheet	1	of	1	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
/P.V./	A1	US-2002/0013772 A1	01-31-2002	Peinado
	A2	US-2002/0108049	08-08-2002	Xu et al.
	A3	US-6,463,534 B1	10-08-2002	Geiger et al.
	A4	US-6,550,011 B1	04-15-2003	Sims III
	A5	US-6,697,944 B1	02-24-2004	Jones et al.
	A6	US-6,975,202 B1	12-13-2005	Rodriguez et al.
/P.V./	A7	US-7,012,503 B2	03-14-2006	Nielsen

FOREIGN PATENT DOCUMENTS					
		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]

Examiner Signature	/Phy Anh Vu/	Date Considered	04/13/2009

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1657343.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Emmanuel Lionel Moise
GROUP ART UNIT:	2137
ATTY. DKT. NO.:	25000-11062

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☒ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last

occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:

- ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
- ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;

☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any

individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☒ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

☒ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,
JOHN J. GIOBBI

Dated: May 23, 2007

By: /Greg T. Sueoka/

Greg T. Sueoka, Reg. No.: 33,800
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7194
Fax.: (650) 938-5200

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	2137
				Examiner Name	Emmanuel Lionel Moise
Sheet	1	of	1	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A1	US-2004/0129787 A1	07-08-2004	Saito et al.
	A2	US-2002/0109580 A1	08-15-2002	Shreve et al.
	A3	US-2002/0073042 A1	06-13-2002	Maritzen et al.
	A4	US-6,041,410	03-21-2000	Hsu et al.
	A5	US-5,991,749	11-23-1999	Morril Jr.

FOREIGN PATENT DOCUMENTS					
		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
	C1	PCT International Search Report and Written Opinion, PCT/US05/43447, February 22, 2007, 7 pages.	
	C2	PCT International Search Report and Written Opinion, PCT/US05/46843, March 1, 2007, 10 pages.	

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1724469.1

Electronic Acknowledgement Receipt

EFS ID:	1803133
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	758
Filer:	Greg T. Sueoka
Filer Authorized By:	
Attorney Docket Number:	25000-11062
Receipt Date:	23-MAY-2007
Filing Date:	20-DEC-2005
Time Stamp:	13:31:21
Application Type:	Utility

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	11062IDS.pdf	81025	no	3
Warnings:					

Information:					
This is not an USPTO supplied IDS fillable form					
2	Information Disclosure Statement (IDS) Filed	11062PTO8A.pdf	111065	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	NPL Documents	11062PCTISRWO.pdf	627297	no	10
Warnings:					
Information:					
4	NPL Documents	11163PCTISRWO.pdf	428923	no	7
Warnings:					
Information:					
		Total Files Size (in bytes):	1248310		

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.

OIPE IAP100
JAN 16 2007
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Emmanuel Lionel Moise
GROUP ART UNIT:	2137
ATTY. DKT. NO.:	25000-11062

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: 01/09/07 By: [signature]
Wasif H. Qureshi, Reg. No.: 51,048

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☒ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;

25000/11062/DOCS/1686539.1

- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:
  - ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
    - ☐ no item of information contained in this 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 this

certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☒ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☒ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

☒ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,
JOHN J. GIOBBI

Dated: 01/09/07

By: WHQuresh

Wasif H. Qureshi, Reg. No. 51,048
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7121
Fax.: (650) 938-5200

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

JAN 16 2007 PATENT & TRADEMARK OFFICE

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	2137
Examiner Name	Emmanuel Lionel Moise
Attorney Docket Number	25000-11062

Sheet	1	of	2

U.S. PATENT DOCUMENTS

		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
		US-		

FOREIGN PATENT DOCUMENTS

		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
	C1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.smartcardalliance.org/pages/publications-identity>	
	C2	"Applying Biometrics to Door Access," Security Magazine, September 26, 2002 [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.securitymagazine.com/CDA/Articles/Technologies/3ae610eaa34d8010VgnVCM100000f932a8c0 >	
	C3	"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.biopay.com/faqs-lowes.asp>	
	C4	MCIVER, R. et al., "Identification and Verification Working Together," Bioscrypt™, August 27, 2004, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>	
	C5	NILSSON, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, April 2004, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>	
	C6	NORDIN, B., "Match-On-Card Technology," Precise™ Biometrics, White Paper, April 2004, [online] [Retrieved on January 7, 2007] Retrieved from the	

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1686538.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	2137
				Examiner Name	Emmanuel Lionel Moise
Sheet	2	of	2	Attorney Docket Number	25000-11062

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
		Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf>	
	C7	"SAFModule™: A Look Into Strong Authentication," saflink Corporation, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>	
	C8	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>	
	C9	WADE, W., "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, April 21, 2003, [online] [Retrieved on January 7, 2007] Retrieved from the Internet<URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>	

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1686538.1

OIPE IAP100
JAN 16 2007
PATENT & TRADEMARK OFFICE

DFW

+

TRANSMITTAL FORM (to be used for all correspondence during pendency of filed application)			
		Application Number	11/314,199
		Filing Date	December 20, 2005
		First Named Inventor	John J. Giobbi
		Group Art Unit Number	2137
		Examiner Name	Emmanuel Lionel Moise
Total Number of Pages in This Submission	6*	Attorney Docket Number	25000-11062

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form (in duplicate)
  - ☐ Check Enclosed
- ☒ Return Receipt Postcard
- ☐ Response to Notice to File Missing Parts
- ☐ Assignment & Recordation Cover Sheet
- ☐ Declaration
- ☐ Power of Attorney
- ☐ Application Data Sheet
- ☒ Information Disclosure Statement & PTO/SB/08A
  - ☒ Copies of IDS Cited References
- ☐ Request for Corrected Filing Receipt
- ☐ Request for Correction of Recorded Assignment
- ☐ Amendment/Response: [ ] Page(s)
  - ☐ After Final
- ☐ Status Request
- ☐ Revocation and Substitute Power of Attorney
- ☐ Issue Fee Transmittal
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawing(s):
  [ ] Sheet(s) of Figure(s) [ ]
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Certified Copy of Priority Document(s)
- ☐ After Allowance Communication to Group
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

REMARKS: *Page count does not include cited references.

SIGNATURE OF ATTORNEY OR AGENT

Signature:	WKureshi		
Attorney/Reg. No.:	**Wasif H. Qureshi, Reg. No. 51,048**	Dated:	01/09/07

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.

Signature:	WKureshi		
Typed or Printed Name:	**Wasif H. Qureshi**	Dated:	01/09/07
Express Mail Mailing Number (*optional*):			

25000/11062/DOCS/1686540.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2131
ATTY. DKT. NO.:	25000-11062

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☒ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;
- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a

final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:

- ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
- ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;

☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:

- ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
  - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
  - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any

individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☐ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

☒ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,
JOHN J. GIOBBI

Dated: October 30, 2006

By: /Wasif H. Qureshi/

Wasif H. Qureshi, Reg. No. 51,048
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7121
Fax.: (650) 938-5200

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	2131
				Examiner Name	Not Yet Known
Sheet	1	of	1	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A1	US-2002/0013772 A1	01-31-2002	Peinado
	A2	US-2002/0108049	08-08-2002	Xu et al.
	A3	US-6,463,534 B1	10-08-2002	Geiger et al.
	A4	US-6,550,011 B1	04-15-2003	Sims III
	A5	US-6,697,944 B1	02-24-2004	Jones et al.
	A6	US-6,975,202 B1	12-13-2005	Rodriguez et al.
	A7	US-7,012,503 B2	03-14-2006	Nielsen

FOREIGN PATENT DOCUMENTS					
		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/11062/DOCS/1657343.1

Electronic Acknowledgement Receipt

EFS ID:	1282508
Application Number:	11314199
International Application Number:	
Confirmation Number:	4469
Title of Invention:	Biometric personal data key (pdk) authentication
First Named Inventor/Applicant Name:	John J. Giobbi
Customer Number:	758
Filer:	Wasif H. Qureshi
Filer Authorized By:	
Attorney Docket Number:	25000-11062
Receipt Date:	30-OCT-2006
Filing Date:	20-DEC-2005
Time Stamp:	18:58:04
Application Type:	Utility

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed	11062_IDS.pdf	236700	no	4
Warnings:					

Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	236700

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.

OIPE
MAR 16 2006
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence during pendency of filed application)

Application Number	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Group Art Unit Number	2131
Examiner Name	Not Yet Known
Total Number of Pages in This Submission	8*
Attorney Docket Number	25000-11062

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form (in duplicate)
  - ☐ Check Enclosed
- ☒ Return Receipt Postcard
- ☐ Response to Notice to File Missing Parts
- ☐ Assignment & Recordation Cover Sheet
- ☐ Declaration
- ☐ Power of Attorney
- ☐ Application Data Sheet
- ☒ Information Disclosure Statement & PTO/SB/08A
  - ☒ Copies of IDS Cited Non-Patent References
- ☐ Request for Corrected Filing Receipt
- ☐ Request for Correction of Recorded Assignment
- ☐ Amendment/Response: [ ] Page(s)
  - ☐ After Final
- ☐ Status Request
- ☐ Revocation and Substitute Power of Attorney
- ☐ Issue Fee Transmittal
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawing(s): [ ] Sheet(s) of Figure(s) [ ]
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Certified Copy of Priority Document(s)
- ☐ After Allowance Communication to Group
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

REMARKS: *Page count does not include cited references.

SIGNATURE OF ATTORNEY OR AGENT

Signature:	Dorian Cartwright		
Attorney/Reg. No.:	**Dorian Cartwright, Reg. No. 53,853**	Dated:	3/13/06

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.

Signature:	Dorian Cartwright		
Typed or Printed Name:	**Dorian Cartwright**	Dated:	3/13/06
Express Mail Mailing Number (*optional*):			

25000/01000/DOCS/1605593.1

OIPE
MAR 16 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2131
ATTY. DKT. NO.:	25000-11062

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: 3/13/06 By: Dorian Cartwright

Dorian Cartwright, Reg. No.: 53,853

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

INFORMATION DISCLOSURE STATEMENT
Under 37 CFR §§ 1.56 and 1.97-98

SIR:

Pursuant to the provisions of 37 CFR §§ 1.56 and 1.97-98, enclosed herewith is modified form PTO/SB/08A listing references for consideration by the Examiner.

The filing of this Information Disclosure Statement shall not be construed as a representation regarding the completeness of the list of references, or that inclusion of a reference in this list is an admission that it is prior art or is pertinent to this application, or that a search has been made, or as an admission that the information listed is, or may be considered to be, material to patentability, or that no other material information exists, and shall not be construed as an admission against interest in any manner.

This Information Disclosure Statement is being filed:

- ☒ within three months of the filing date of the application, or date of entry into the national stage of an international application, or before the mailing date of a first office action on the merits, whichever event last occurred;
- ☐ before the mailing of a first official action after the filing of a request for continued examination (RCE) under 37 CFR § 1.114;

- ☐ after three months of the filing date of this national application or the date of entry of the national stage in an international application, or after the mailing date of the first official action on the merits, whichever event last occurred, but before the mailing date of the first to occur of either: (1) a final action under 37 CFR §1.113; or (2) an action that otherwise closes prosecution in the application, and:
  - ☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(c); OR
  - ☐ Applicant certifies pursuant to 37 CFR § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement; OR
    - ☐ no item of information contained in this 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 this certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement;
- ☐ on or before the payment of the issue fee but after the mailing date of the first to occur of either: (1) a final action under 37 CFR § 1.113; (2) a notice of allowance under 37 CFR § 1.311; or (3) an action that otherwise closes prosecution in the application, and:
  - ☐ Applicant certifies pursuant to 37 CFR. § 1.97(e) that:
    - ☐ each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Statement;
    - ☐ no item of information contained in this 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 this

certification after making reasonable inquiry, no item of information contained in this Statement was known to any individual designated under 37 CFR § 1.56(c) more than three months prior to the filing of this Statement; AND

☐ attached hereto is the fee set forth under 37 CFR §1.17(p) for submission of this Information Disclosure Statement under 37 CFR.§ 1.97(d); OR

☐ after the payment of the issue fee. Applicant requests that the information contained in this Information Disclosure Statement be placed in the file according to 37 CFR § 1.97(i), although the information may not be considered by the USPTO.

☐ Enclosed is a copy of each listed reference that may be material to the examination of this application, and for which there may be a duty to disclose.

☐ This application relies, under 35 U.S.C. § 120, on the earlier filing date of prior application No. _____ , filed on _____ , and the references cited therein are hereby referenced, but are not required to be provided in this application under 37 CFR § 1.98(d).

☒ Copies of any foreign patent documents and non-patent literature cited herein are enclosed.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not received by any individual designated in 37 CFR § 1.56(c) more than thirty days prior to the filing of this Information Disclosure Statement. 37 CFR § 1.704(d).

☒ Applicant submits that no fee is required for the consideration of this Information Disclosure Statement.

Consideration of the listed references and favorable action are solicited.

Respectfully submitted,
JOHN J. GIOBBI

Dated: 3/13/06

By: Dorian Cartwright

Dorian Cartwright, Reg. No.: 53,853
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-
Fax.: (650) 938-5200

OIPE IAP29
MAR 16 2006
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	2131
Examiner Name	Not Yet Known
Attorney Docket Number	25000-11062

Sheet	1	of	4

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document No. Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A1	US-6,950,941	09-27-2005	Lee et al.
	A2	US-6,806,887	10-19-2004	Chernock et al.
	A3	US-6,804,825	10-12-2004	White et al.
	A4	US-6,775,655	08-10-2004	Peinado et al.
	A5	US-6,711,464	03-23-2004	Yap et al.
	A6	US-6,683,954	01-27-2004	Searle
	A7	US-6,667,684	12-23-2003	Waggamon et al.
	A8	US-6,647,417	11-11-2003	Hunter et al.
	A9	US-6,632,992	10-14-2003	Hasegawa
	A10	US-6,628,302	09-30-2003	White et al.
	A11	US-6,564,380	05-13-2003	Murphy
	A12	US-6,563,805	05-13-2003	Ma et al.
	A13	US-6,546,418	04-08-2003	Schena et al.
	A14	US-6,529,949	03-04-2003	Getsin et al.
	A15	US-6,510,350	01-21-2003	Steen et al.
	A16	US-6,490,443	12-03-2002	Freeny, Jr.
	A17	US-6,480,188	11-12-2002	Horsley
	A18	US-6,446,130	09-03-2002	Grapes
	A19	US-6,434,535	08-13-2002	Kupka et al.
	A20	US-6,425,084	07-23-2002	Rallis et al.
	A21	US-6,424,715	07-23-2002	Saito
	A22	US-6,411,307	06-25-2002	Rosin et al.
	A23	US-6,401,059	06-04-2002	Shen et al.
	A24	US-6,397,387	05-28-2002	Rosin et al.
	A25	US-6,392,664	05-21-2002	White et al.
	A26	US-6,385,596	05-07-2002	Wiser et al.
	A27	US-6,381,747	04-30-2002	Wonfor et al.

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	2131
				Examiner Name	Not Yet Known
Sheet	2	of	4	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A28	US-6,367,019	04-02-2002	Ansell et al.
	A29	US-2002/0015494 A1	02-07-2002	Nagai et al.
	A30	US-6,336,142	01-01-2002	Kato et al.
	A31	US-2002/0007456 A1	01-17-2002	Peinado et al.
	A32	US-6,336,121	01-01-2002	Lyson et al.
	A33	US-6,295,057	09-25-2001	Rosin et al.
	A34	US-6,266,415	07-24-2002	Campinos et al.
	A35	US-6,247,130	06-12-2001	Fritsch
	A36	US-6,219,109	04-17-2001	Raynesford et al.
	A37	US-6,209,089	03-27-2001	Selitrennikoff et al.
	A38	US-6,161,179	12-12-2000	Seidel
	A39	US-6,148,142	11-14-2000	Anderson
	A40	US-6,104,334	08-15-2000	Allport
	A41	US-6,088,730	07-11-2000	Kato et al.
	A42	US-6,055,314	04-25-2000	Spies et al.
	A43	US-6,035,329	03-07-2000	Mages et al.
	A44	US-6,035,038	03-07-2000	Campinos et al.
	A45	US-5,991,399	11-23-1999	Graunke et al.
	A46	US-5,928,327	07-27-1999	Wang et al.
	A47	US-5,898,880	04-27-1999	Ryu
	A48	US-5,892,825	04-06-1999	Mages et al.
	A49	US-5,857,020	01-05-1999	Peterson, Jr.
	A50	US-5,825,876	10-20-1998	Peterson, Jr.
	A51	US-5,784,464	07-21-1998	Akiyama et al.
	A52	US-5,666,412	09-09-1997	Handelman et al.
	A53	US-5,644,354	07-01-1997	Thompson et al.
	A54	US-5,629,980	05-13-1997	Stefik et al.

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				**Application No.**	11/314,199
				Filing Date	December 20, 2005
				First Named Inventor	John J. Giobbi
				Art Unit	2131
				Examiner Name	Not Yet Known
Sheet	3	of	4	Attorney Docket Number	25000-11062

U.S. PATENT DOCUMENTS				
		Document No.		
Examiner Initials*	Cite No.[1]	Number – Kind Code[2] (if known)	Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	A55	US-5,619,251	04-08-1997	Kuroiwa et al.
	A56	US-5,450,489	09-12-1995	Ostrover et al.
	A57	US-5,422,632	06-06-1995	Bucholtz et al.
	A58	US-5,392,433	02-21-1995	Hammersley et al.
	A59	US-5,296,641	03-22-1994	Stelzl
	A60	US-5,187,352	02-16-1993	Blair et al.
	A64	US-4,759,060	07-19-1988	Hayashi et al.

FOREIGN PATENT DOCUMENTS					
		Foreign Patent Document			
Examiner Initials*	Cite No.[1]	Country Code[3] – Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	T[6]
	B1	WO 05/086802 A2	09-22-2005	Margent Development, LLC	
	B2	WO 05/050450 A1	06-02-2005	Margent Development, LLC	
	B3	WO 01/77790 A1	10-18-2001	Thomson Multimedia	
	B4	WO 01/75876 A1	10-11-2001	Thomson Multimedia	
	B5	WO 01/22724 A1	03-29-2001	Thomson Multimedia	
	B6	WO 00/62505 A1	10-19-2000	Thomson Multimedia	

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
	C1	ANTONOFF, Michael, "Visiting Video Valley," Sound & Vision, Pages 116 and 118-119, Nov. 2001.	
	C2	Article, "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, July 25, 2000.	
	C3	Article, "Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, August 14, 2000.	
	C4	BLUM, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, (October 2000), 24-27.	
	C5	DEBOW, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p10, November, 1989.	

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known	
Application No.	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John J. Giobbi
Art Unit	2131
Examiner Name	Not Yet Known
Attorney Docket Number	25000-11062

Sheet	4	of	4

OTHER REFERENCES – NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[6]
	C6	DENNIS, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, December 2, 1999, 2 pages.	
	C7	FASCA, Chad, "The Circuit," Electronic News, 45(45) (November 8, 1999), 20.	
	C8	Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, January 18, 1996.	
	C9	LAKE, Matt, "Downloading for Dollars," Sound & Vision, (November 2000), 137-138.	
	C10	LEWIS, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, November 16, 1995.	
	C11	Notification of the International Search Report and Written Opinion, PCT/US04/38124, April 7, 2005, 10 pages.	
	C12	PAGET, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, (Dec. 1999), 4 pgs.	
	C13	Press Release, "Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, January 8, 2002.	
	C14	Press Release, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002.	
	C15	Press Release, "Thompson Bets on Smart Cards For Video Encryption," www.informationweek.com, June 7, 2001.	
	C16	Press Release, "Thompson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001.	
	C17	"Say Hello to Bluetooth," Bluetooth Web site, 4 pages.	
	C18	SAPSFORD, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, (August 14, 2000), B1	
	C19	VAN WINKLE, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, (January 2000), 148-153.	
	C20	WALLACE, Bob, "The Internet Unplugged," InformationWeek, 765(22), (December 13, 1999), 22-24.	
	C21	WEBER, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, (July 24, 2000), B1.	

Examiner Signature		Date Considered	

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

[1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

25000/01000/DOCS/1605583.1

(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).

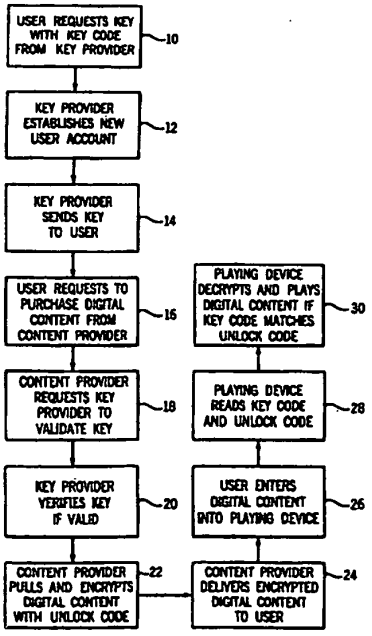
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

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.

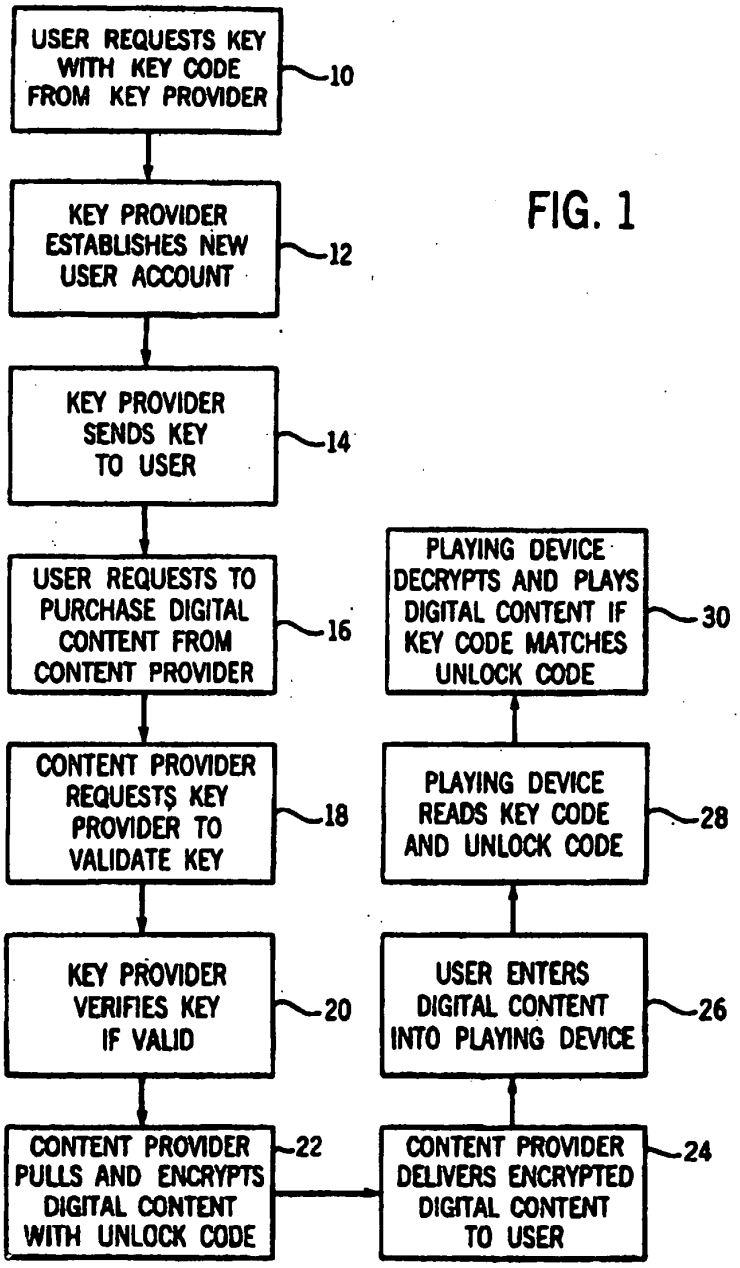

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT 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

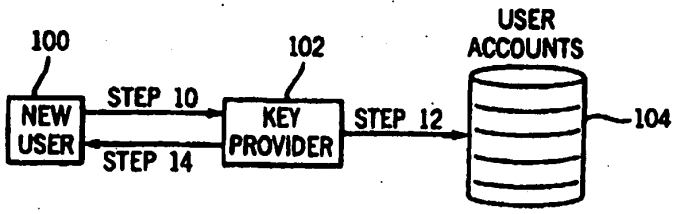


FIG. 2

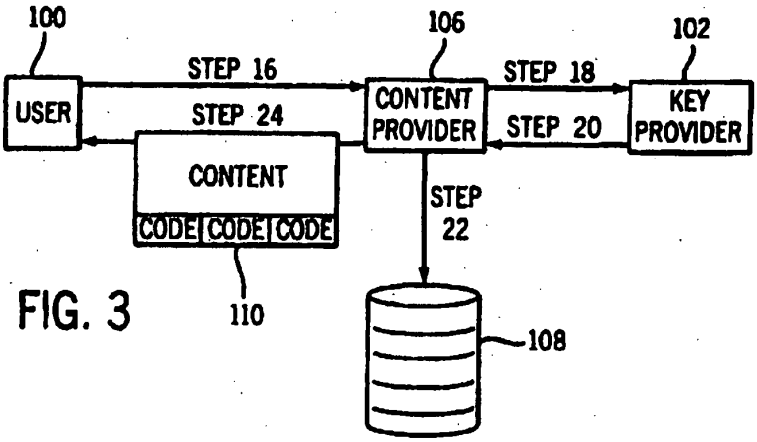


FIG. 3

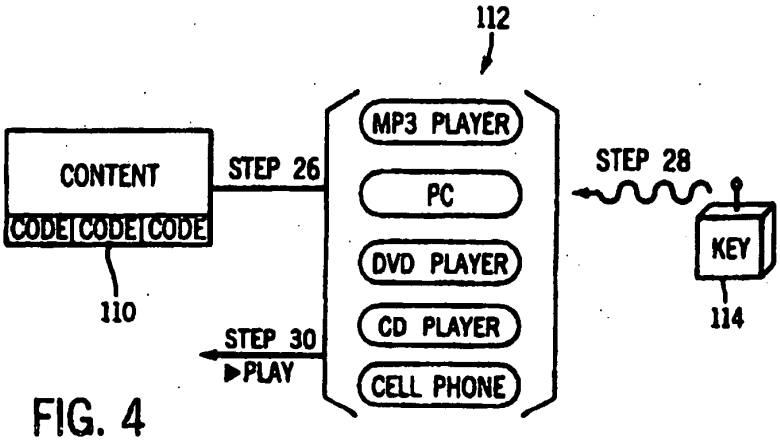


FIG. 4

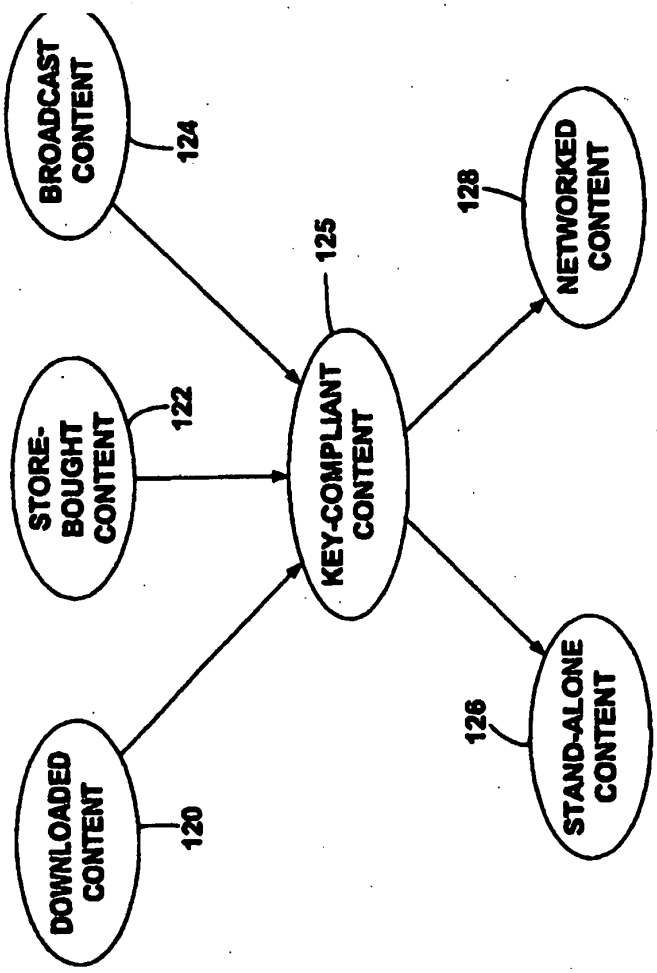

DOWNLOADED CONTENT
120
STORE-BOUGHT CONTENT
122
BROADCAST CONTENT
124
KEY-COMPLIANT CONTENT
125
STAND-ALONE CONTENT
126
NETWORKED CONTENT
128

FIG. 5

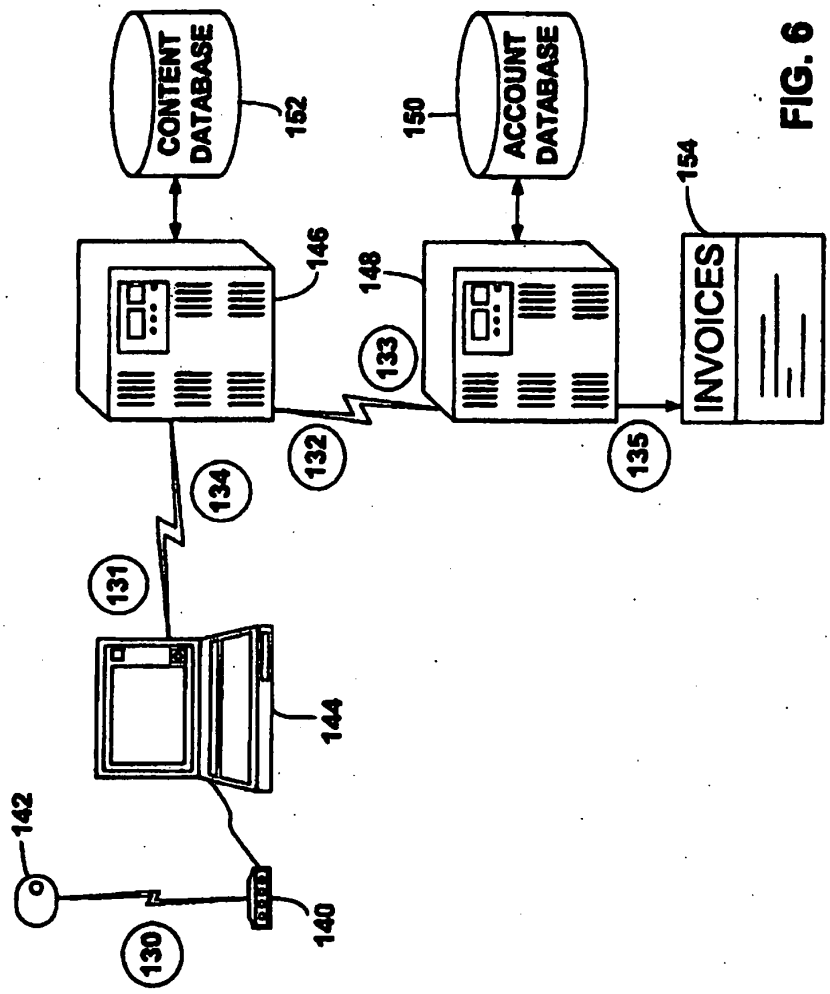

CONTENT DATABASE
152
146
150
ACCOUNT DATABASE
148
154
INVOICES
133
132
134
135
131
144
142
140
130

FIG. 6

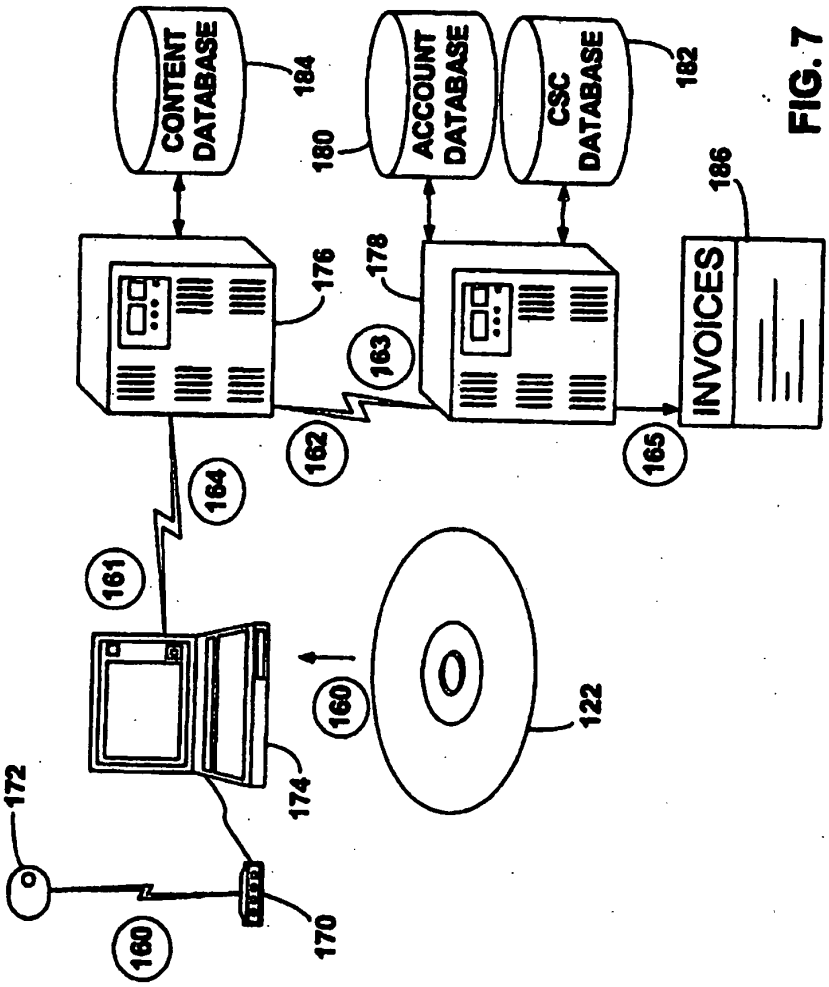

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
176
178
163
162
164
161
INVOICES
186
165
160
122
174
172
170
160

FIG. 7

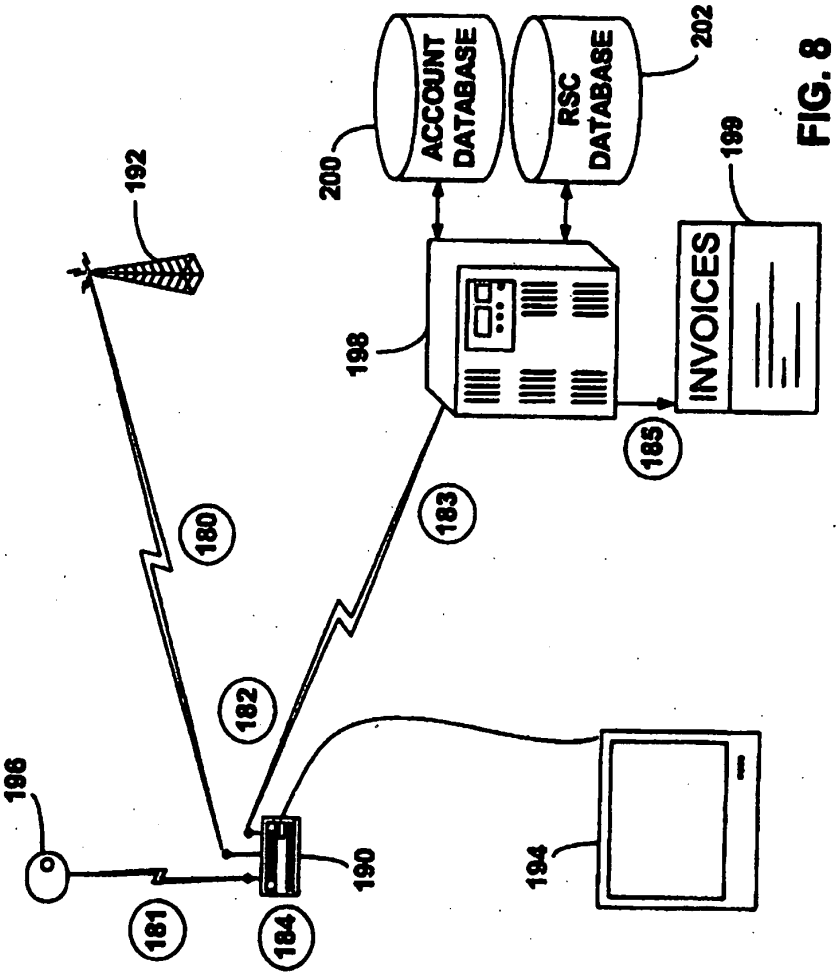

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
198
192
180
183
182
185
196
181
184
190
194

FIG. 8

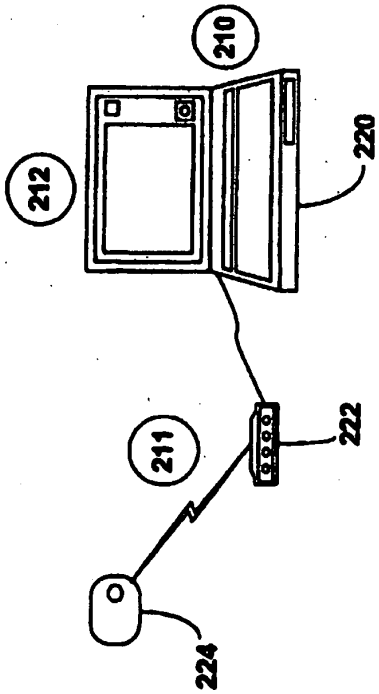


FIG. 9a

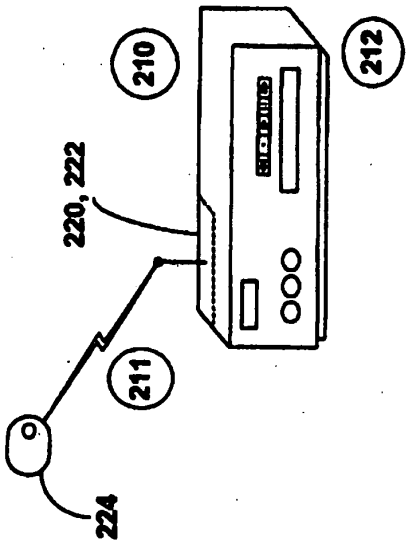


FIG. 9b

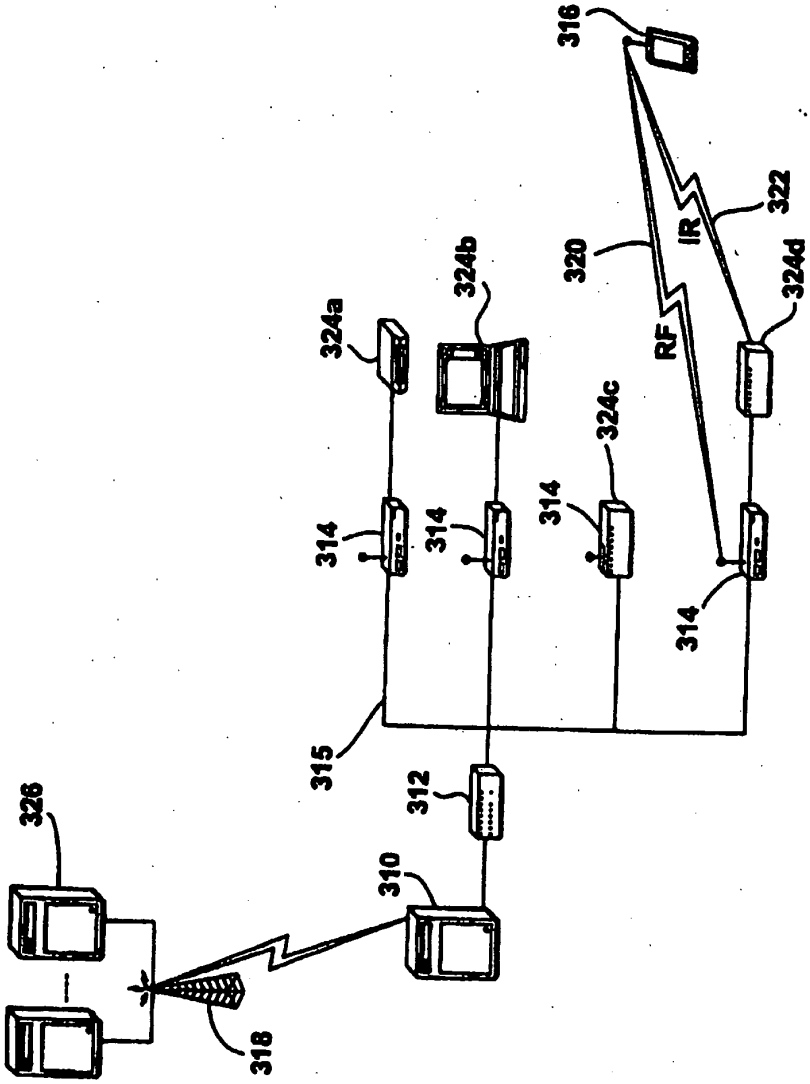

316
322
IR
320
RF
324d
324b
324a
324c
314
314
314
314
315
312
310
326
318

FIG. 10

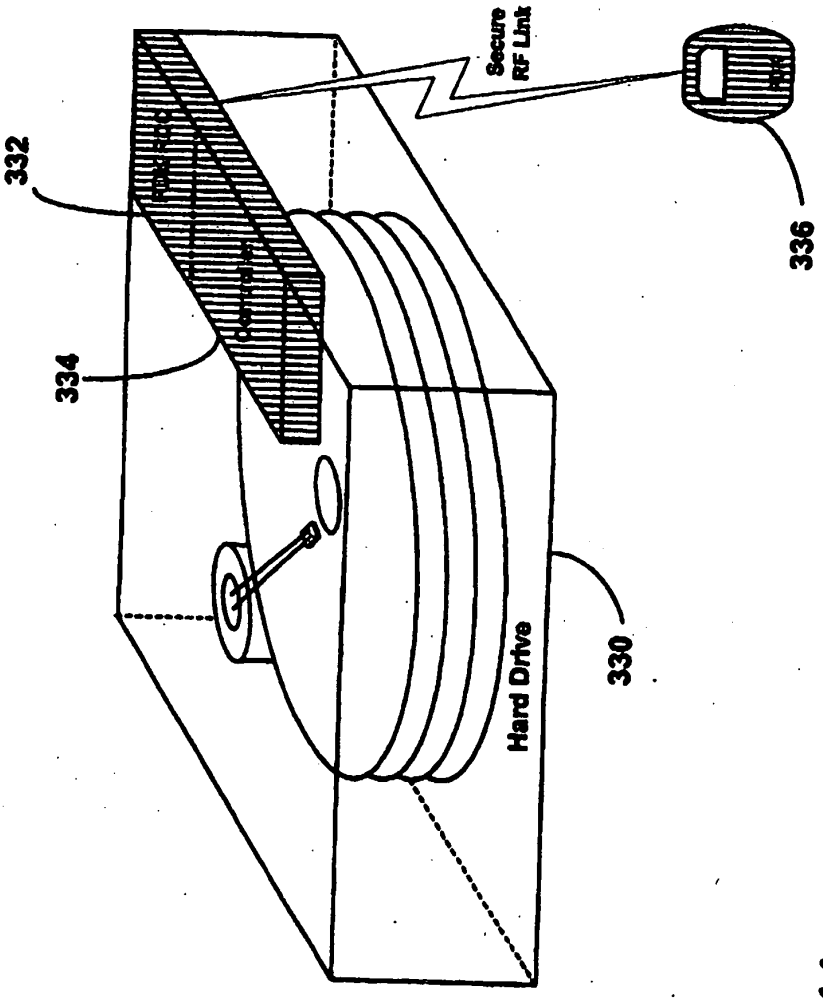


FIG. 11

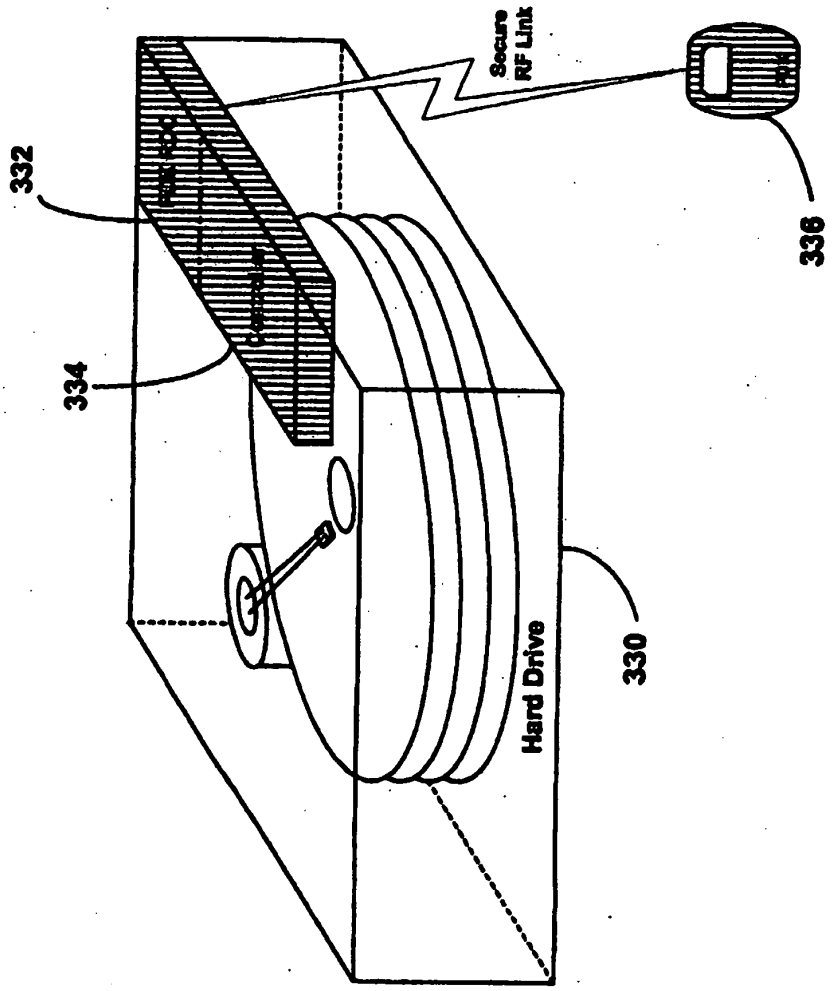


FIG. 12

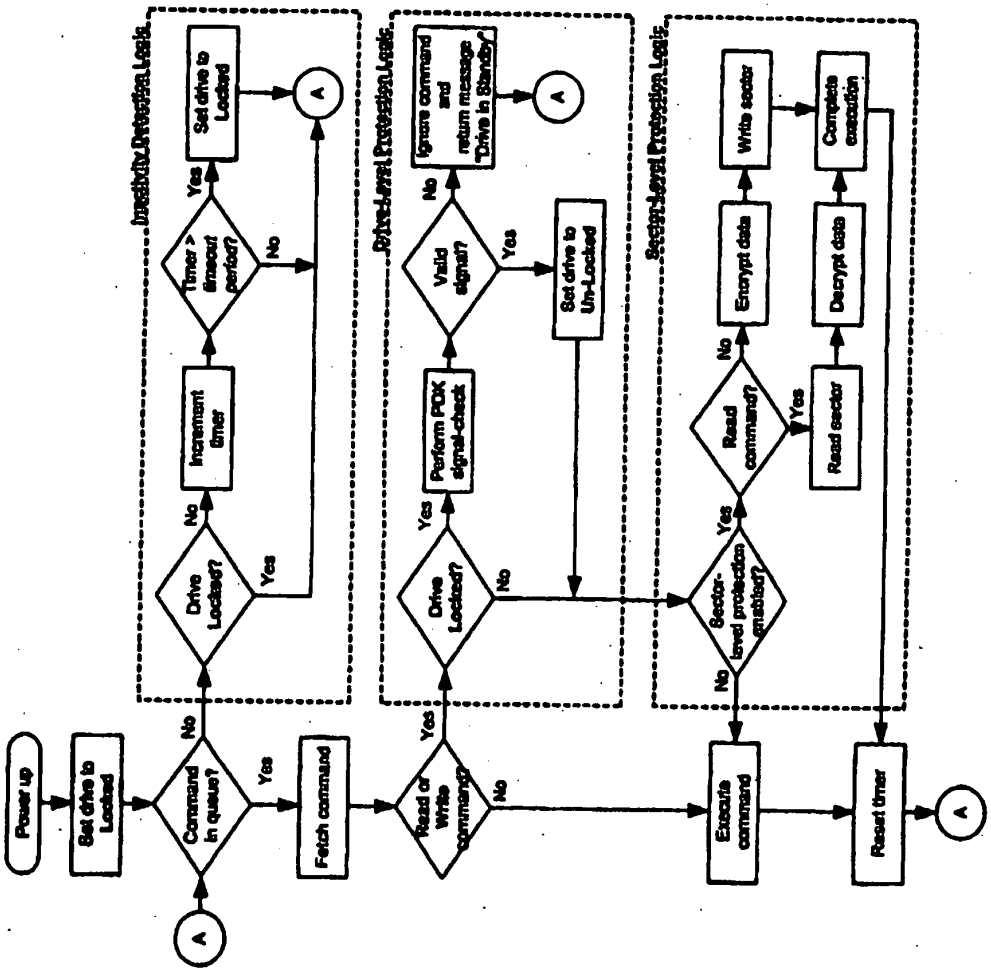

Power up
Set drive to Locked
Command in queue?
No
Yes
A
Fetch command
Read or Write command?
Yes
No
Inactivity Protection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
A
Drive-Level Protection Logic
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
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

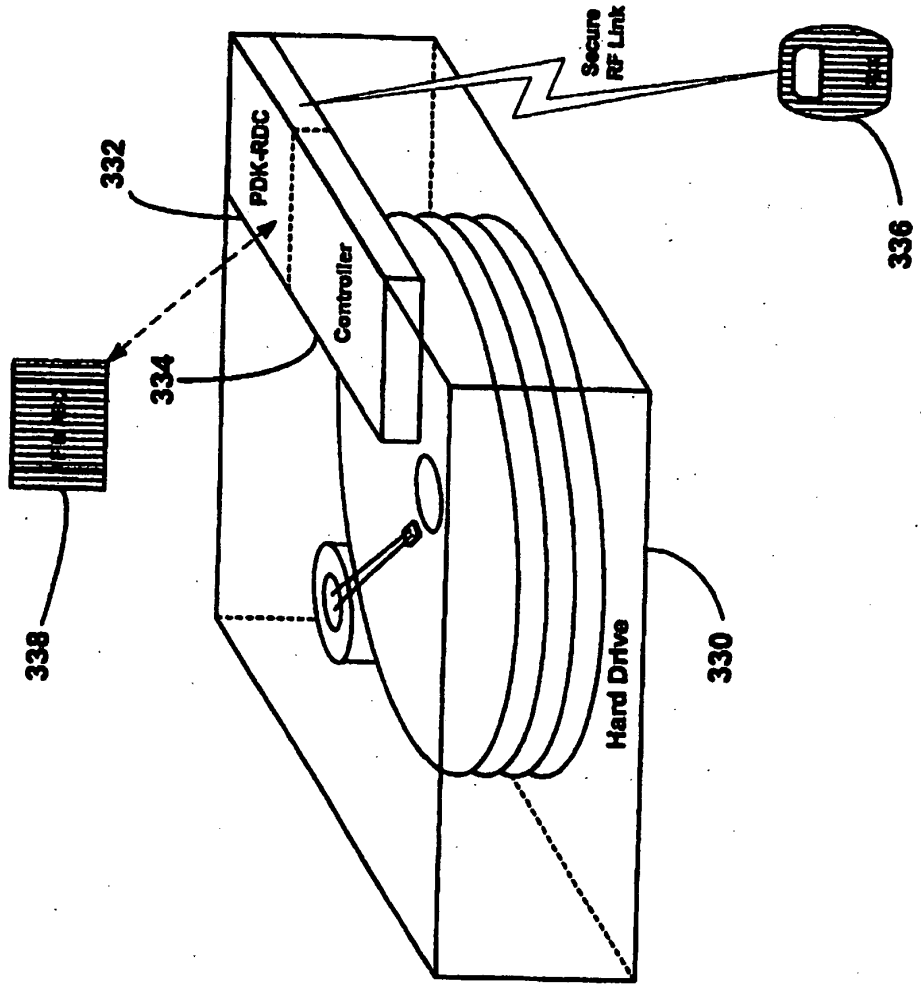

Secure
RF Link
PDK-RDC
Controller
Hard Drive
332
334
336
338
330

FIG. 14

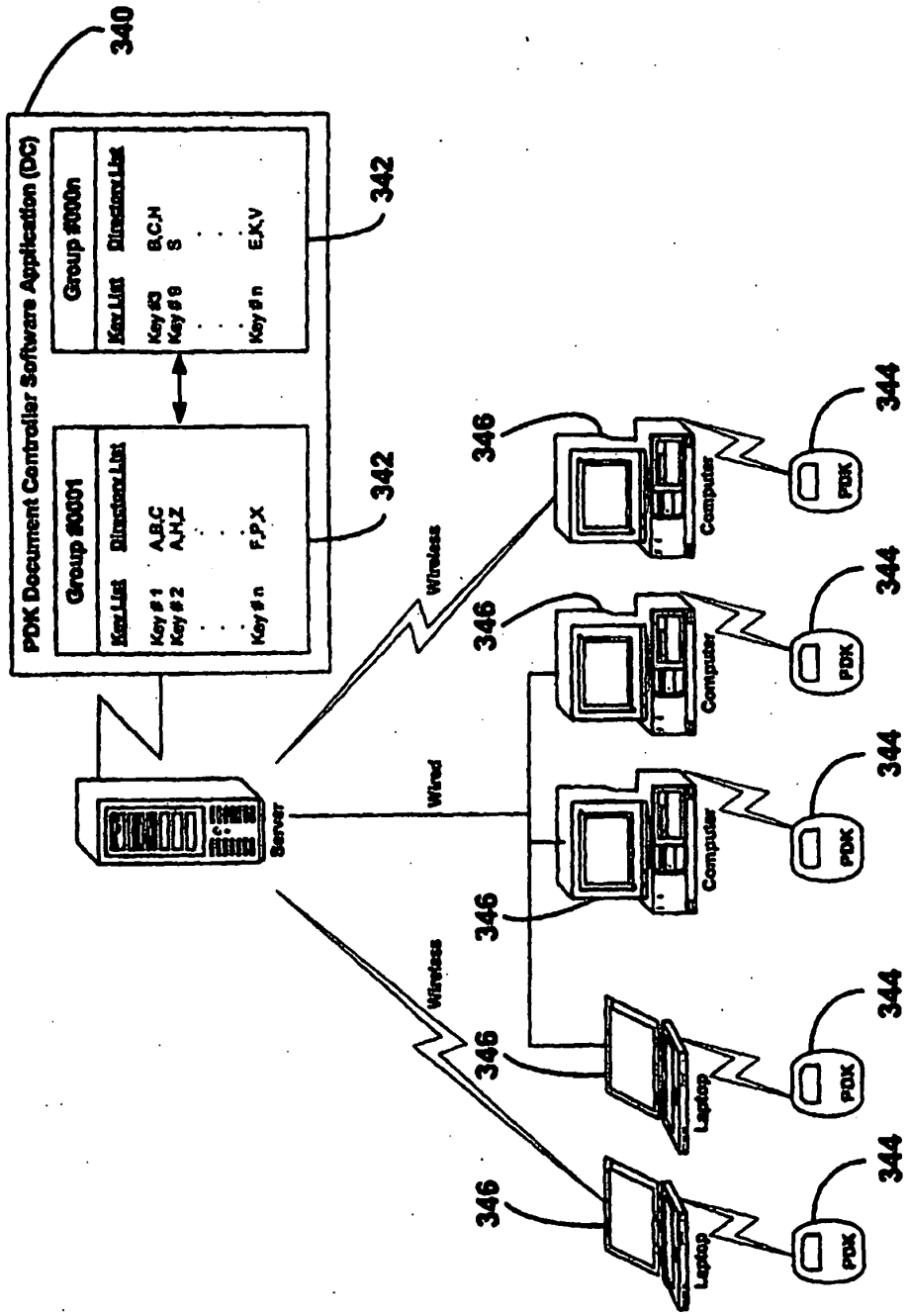

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key #1 A,B,C
Key #2 A,H,Z
Key #n F,P,X
Group #000n
Key List
Directory List
Key #3 B,C,H
Key #6 S
Key #n E,K,V
342
342
Server
Wireless
Wired
Wireless
346
346
346
346
Computer
Computer
Laptop
Laptop
PDK
PDK
PDK
PDK
344
344
344
344

FIG. 15

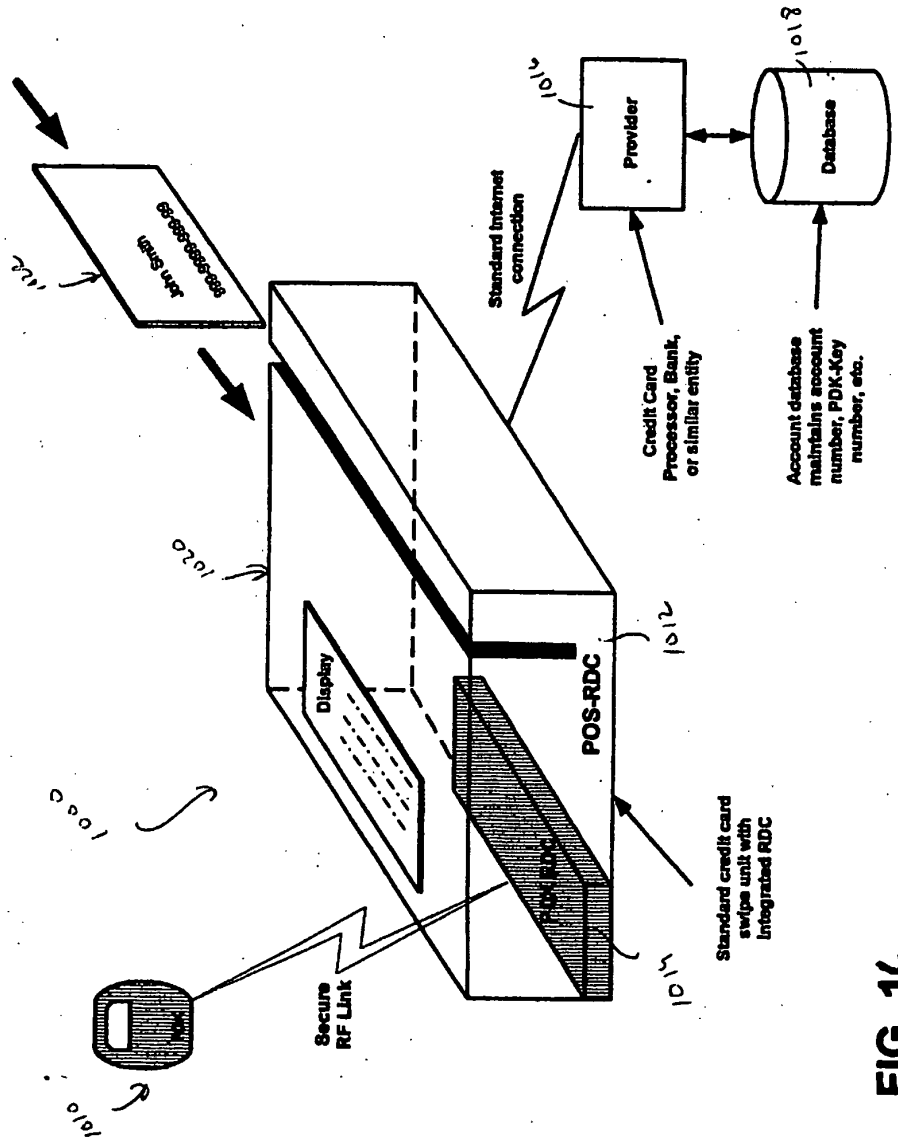

John Smith
Display
POS-RDC
PDK-RDC
Secure RF Link
Standard credit card swipe unit with integrated RDC
Standard Internet connection
Provider
Database
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
1000
1010
1012
1014
1016
1018
1020
1022

FIG. 16

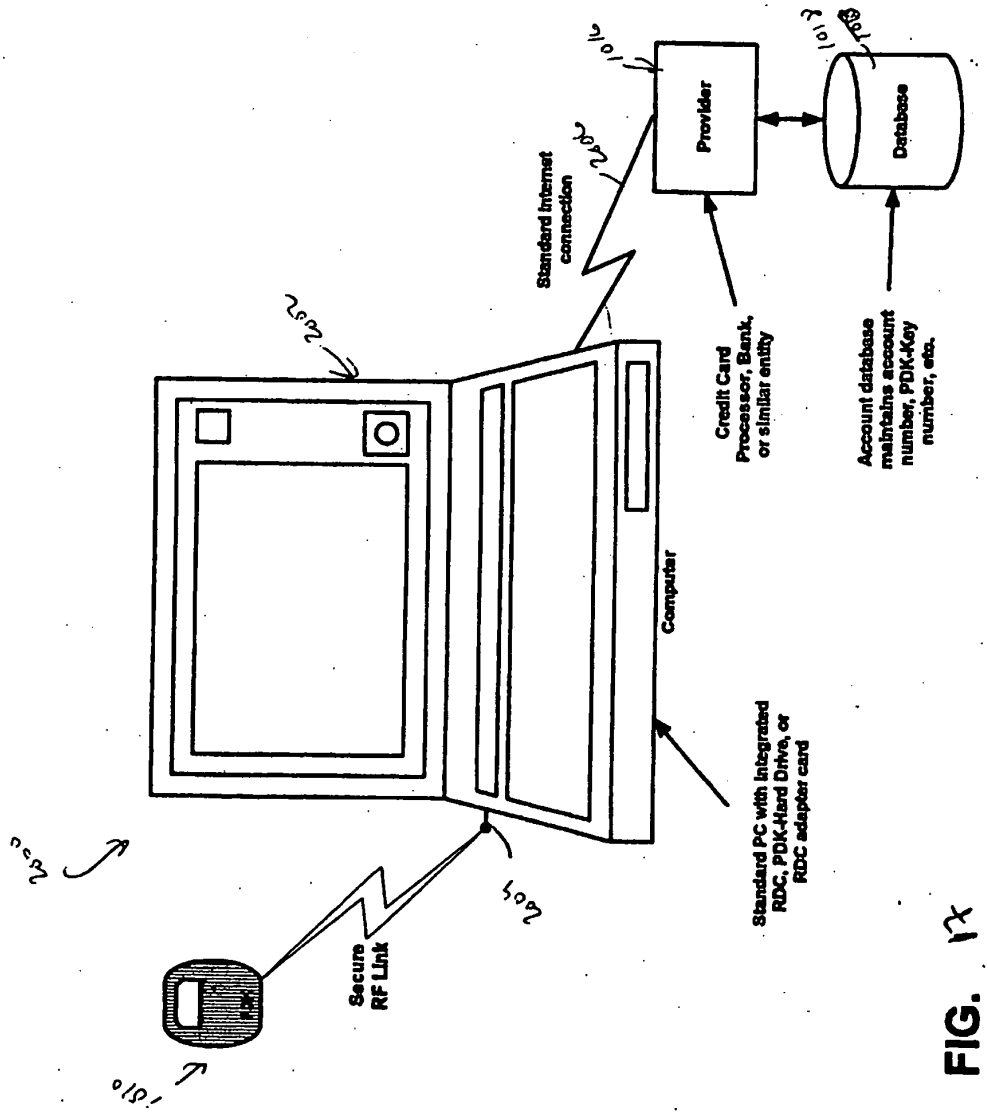

Provider
Database
Standard Internet connection
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
Computer
Standard PC with Integrated RDC, PDK-Hard Drive, or RDC adapter card
Secure RF Link

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).

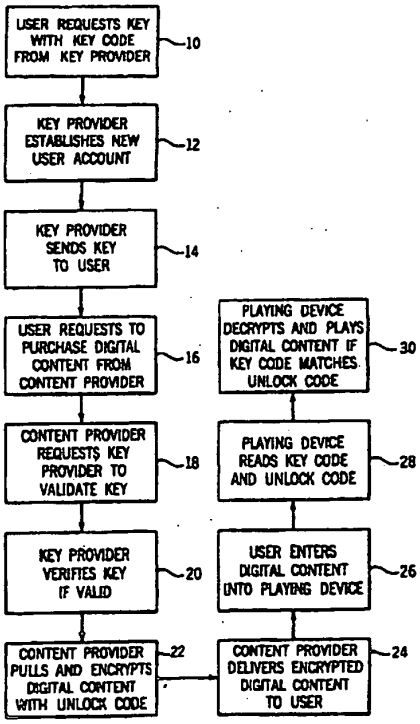
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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
07 October 2005 (07.10.2005)

Date of mailing of the international search report
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
D. Wilbermuth for
James Trammel

Telephone No. 571-272-3600

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

(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).

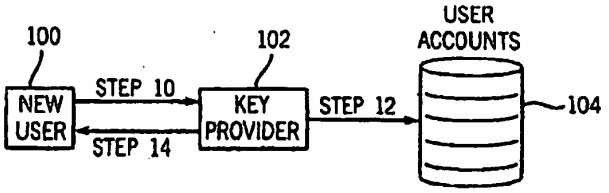
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, 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.

1/13

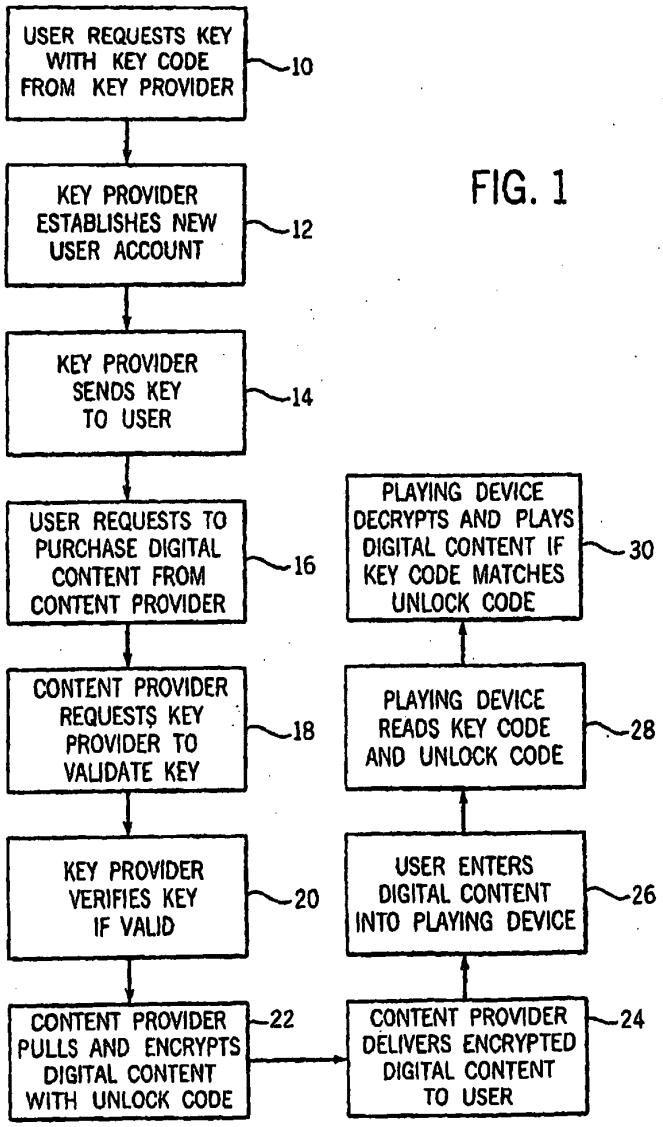

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT 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

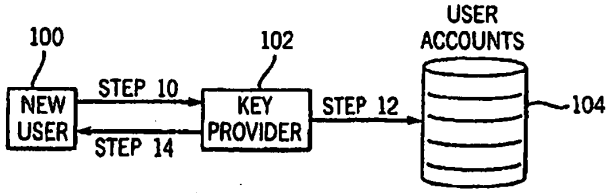


FIG. 2

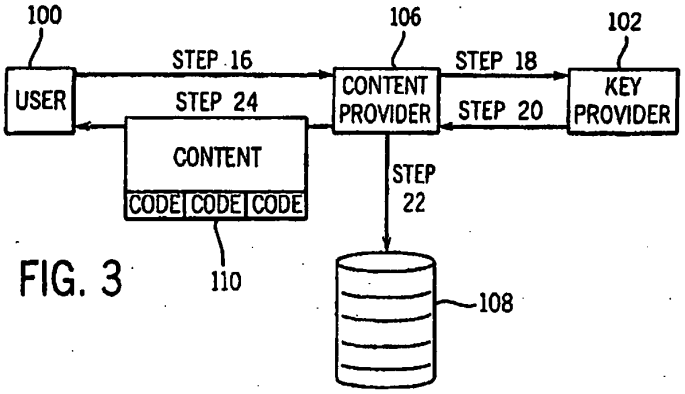


FIG. 3

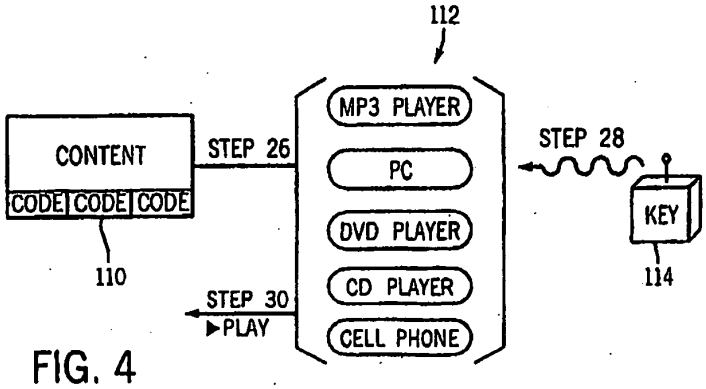


FIG. 4

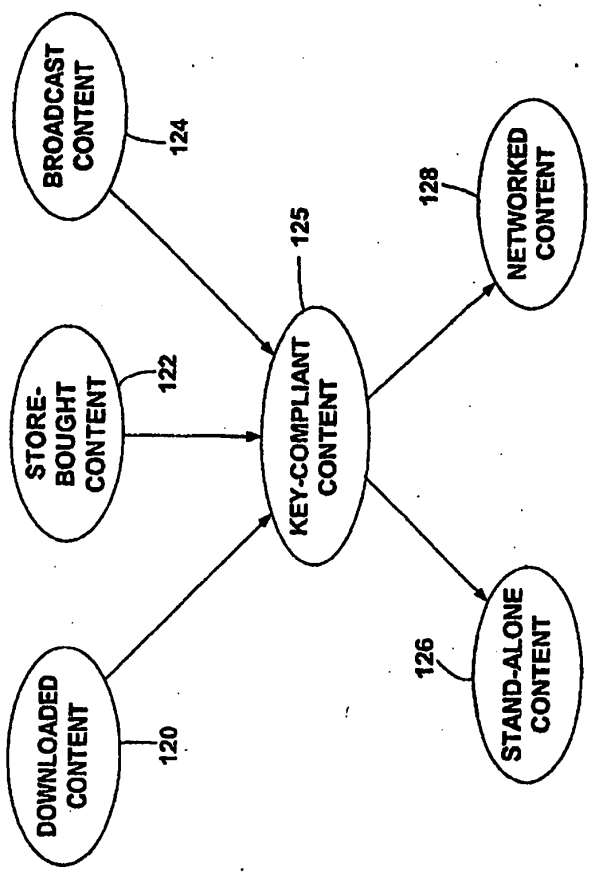

DOWNLOADED CONTENT
120
STORE-BOUGHT CONTENT
122
BROADCAST CONTENT
124
KEY-COMPLIANT CONTENT
125
STAND-ALONE CONTENT
126
NETWORKED CONTENT
128

FIG. 5

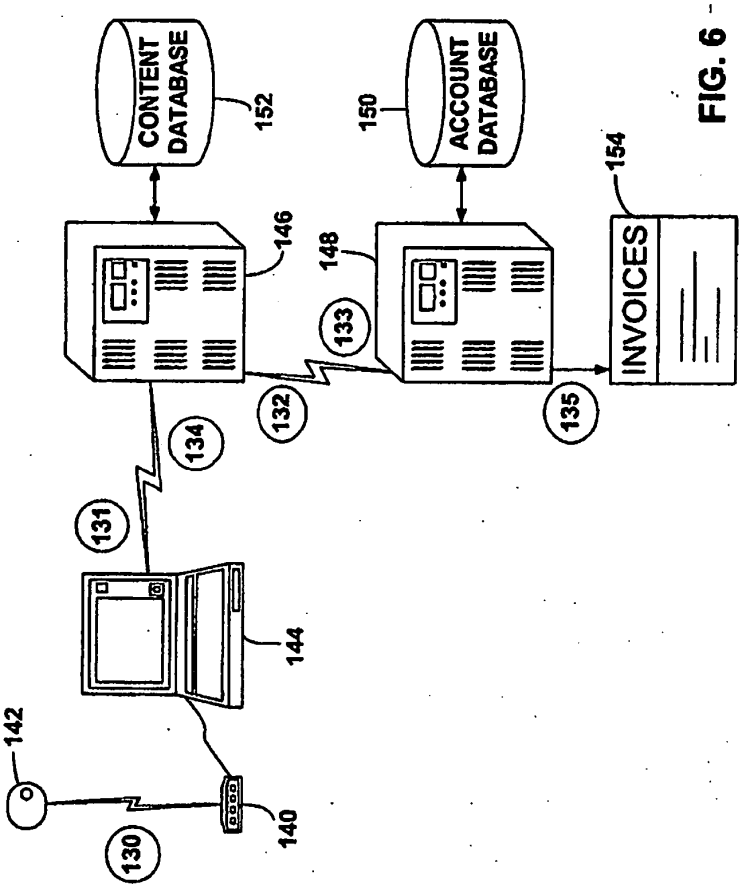

CONTENT DATABASE
152
ACCOUNT DATABASE
150
146
148
154
INVOICES
133
132
135
134
131
144
142
140
130

FIG. 6

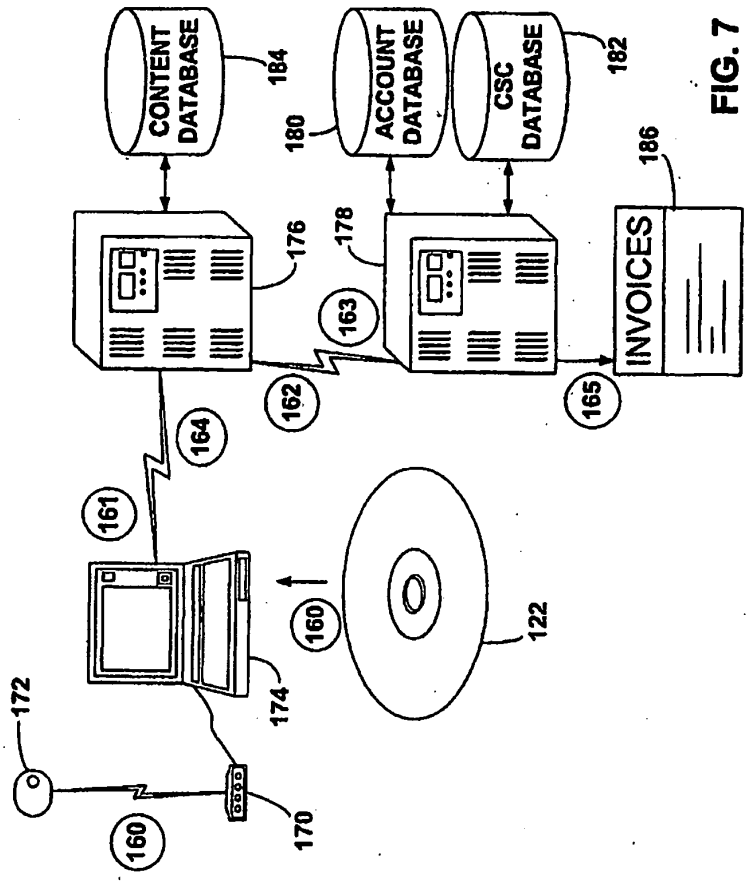

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
INVOICES
186
176
178
163
162
165
164
161
160
122
174
172
170
160

FIG. 7

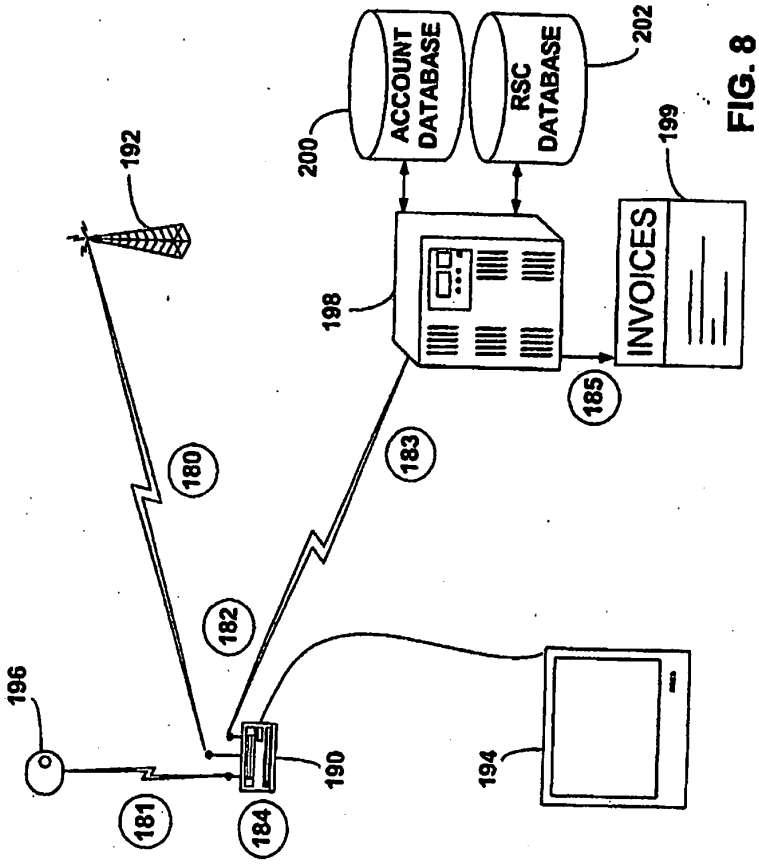

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
198
192
196
180
181
182
183
184
185
190
194

FIG. 8

FIG. 9a

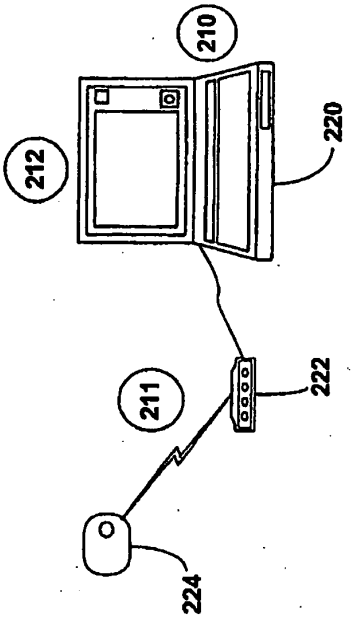
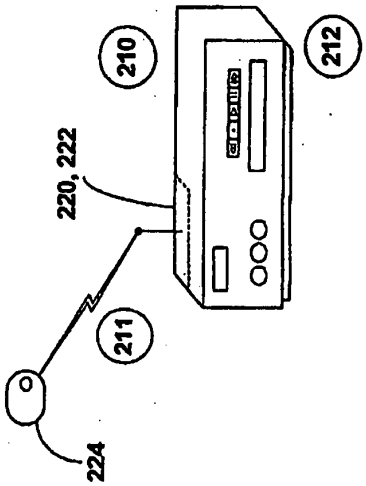


FIG. 9b



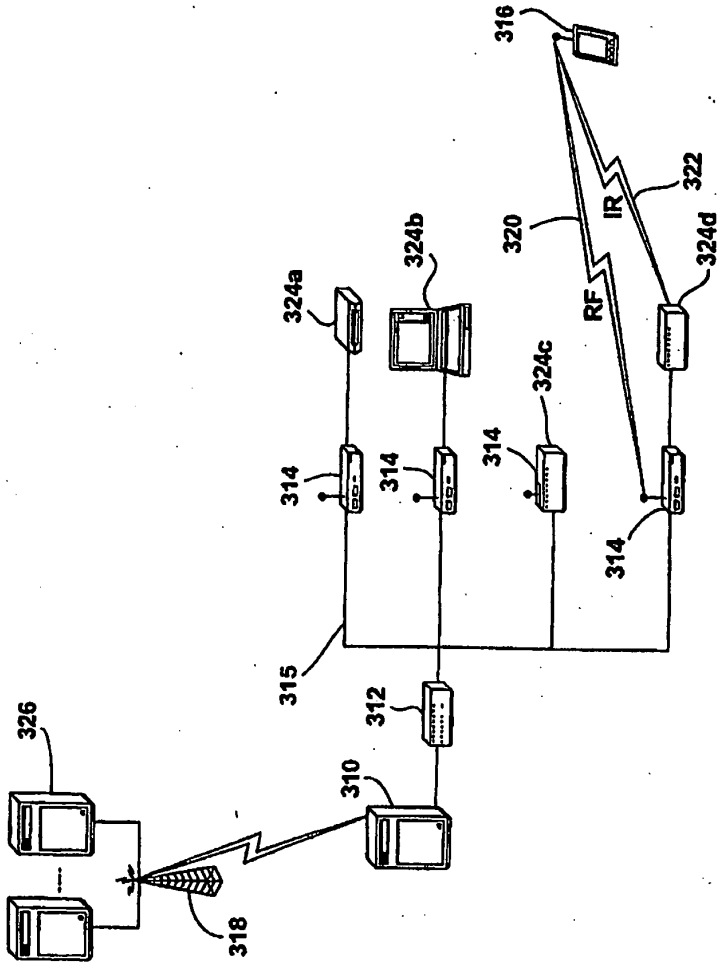

316
322
IR
320
RF
324d
324a
324b
324c
314
314
314
314
315
312
310
326
318

FIG. 10

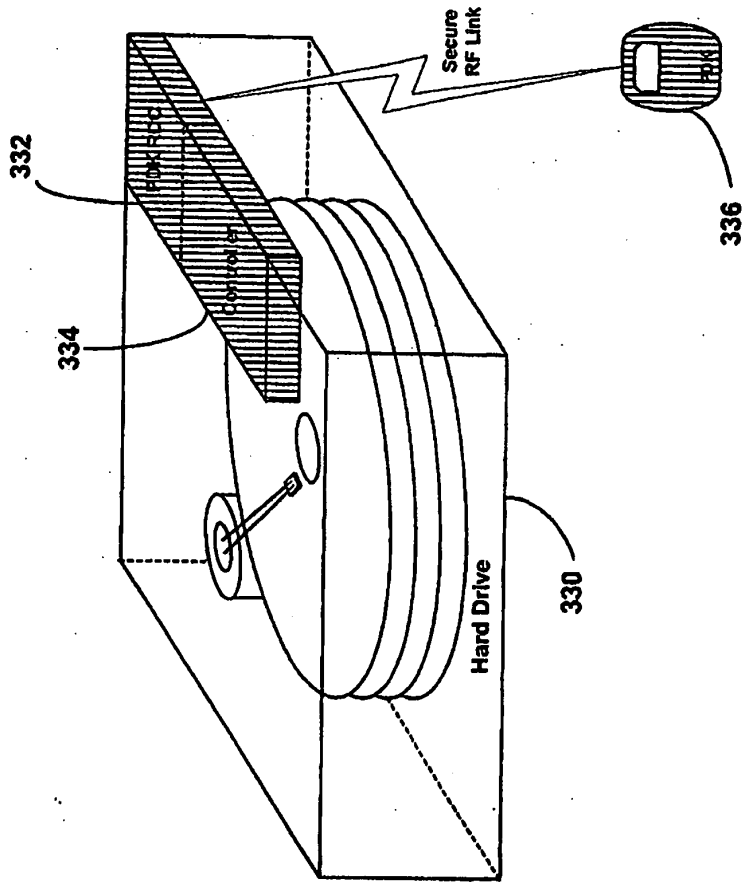


FIG. 11

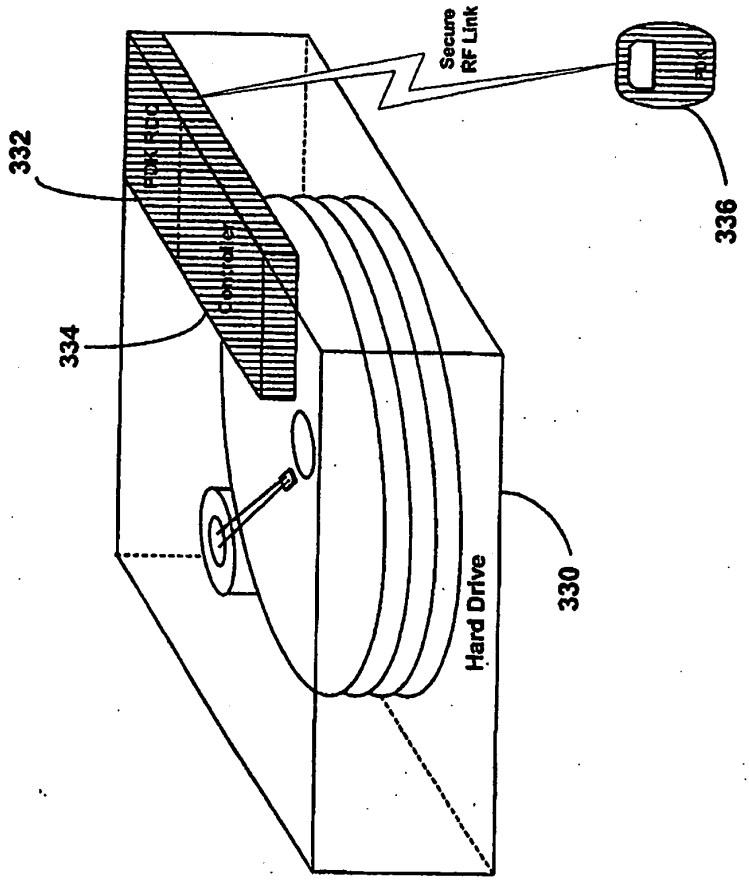


FIG. 12

11/13

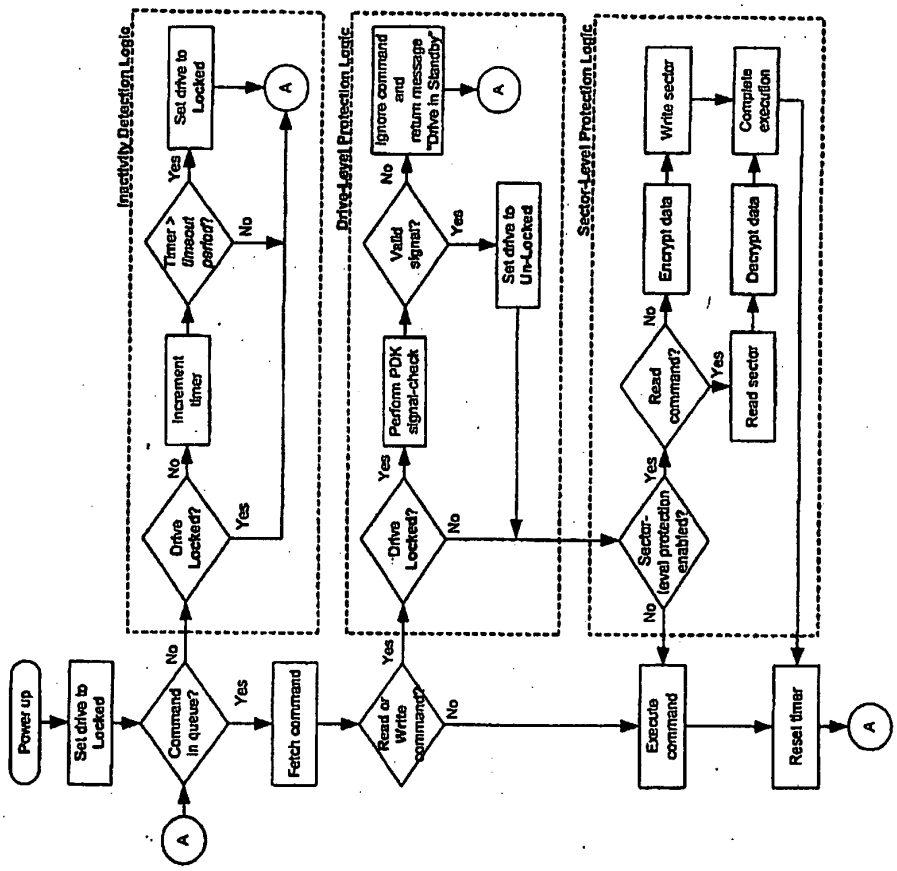

Power up
Set drive to Locked
Command in queue?
No
Yes
A
Fetch command
Inactivity Detection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
A
Drive-Level Protection Logic
Read or Write command?
Yes
No
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
A
Set drive to Un-Locked
Sector-Level Protection Logic
Execute command
Sector-level protection enabled?
Yes
No
Read command?
No
Yes
Encrypt data
Write sector
Read sector
Decrypt data
Complete execution
Reset timer
A

FIG. 13

12/13

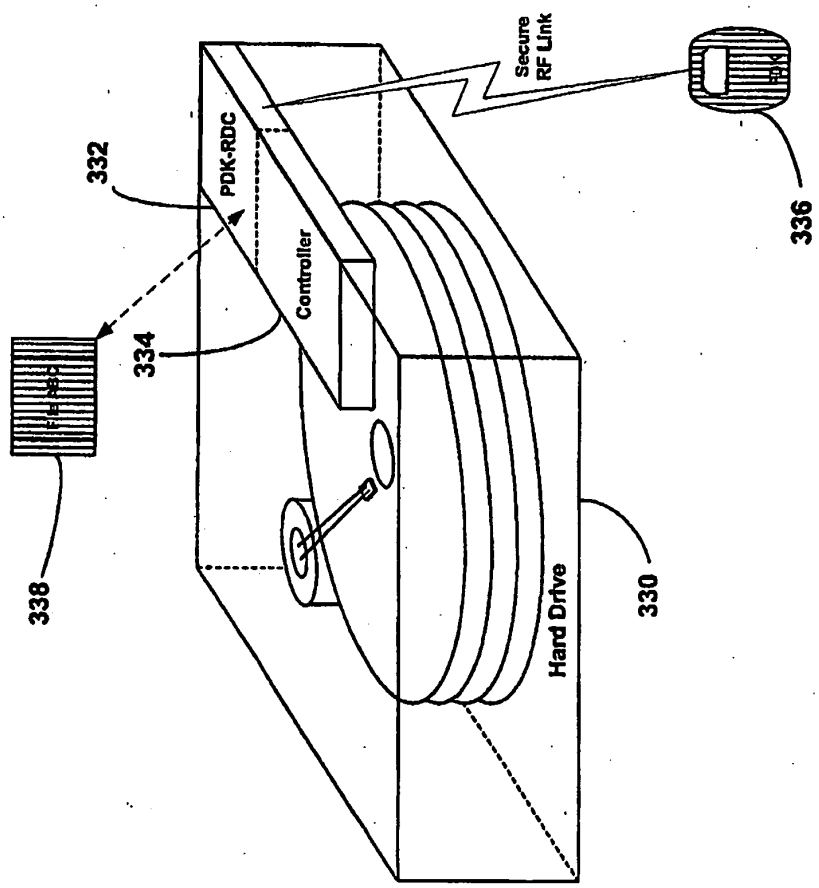

Secure
RF Link
PDK-RDC
Controller
Hard Drive
332
334
336
338
330

FIG. 14

13/13

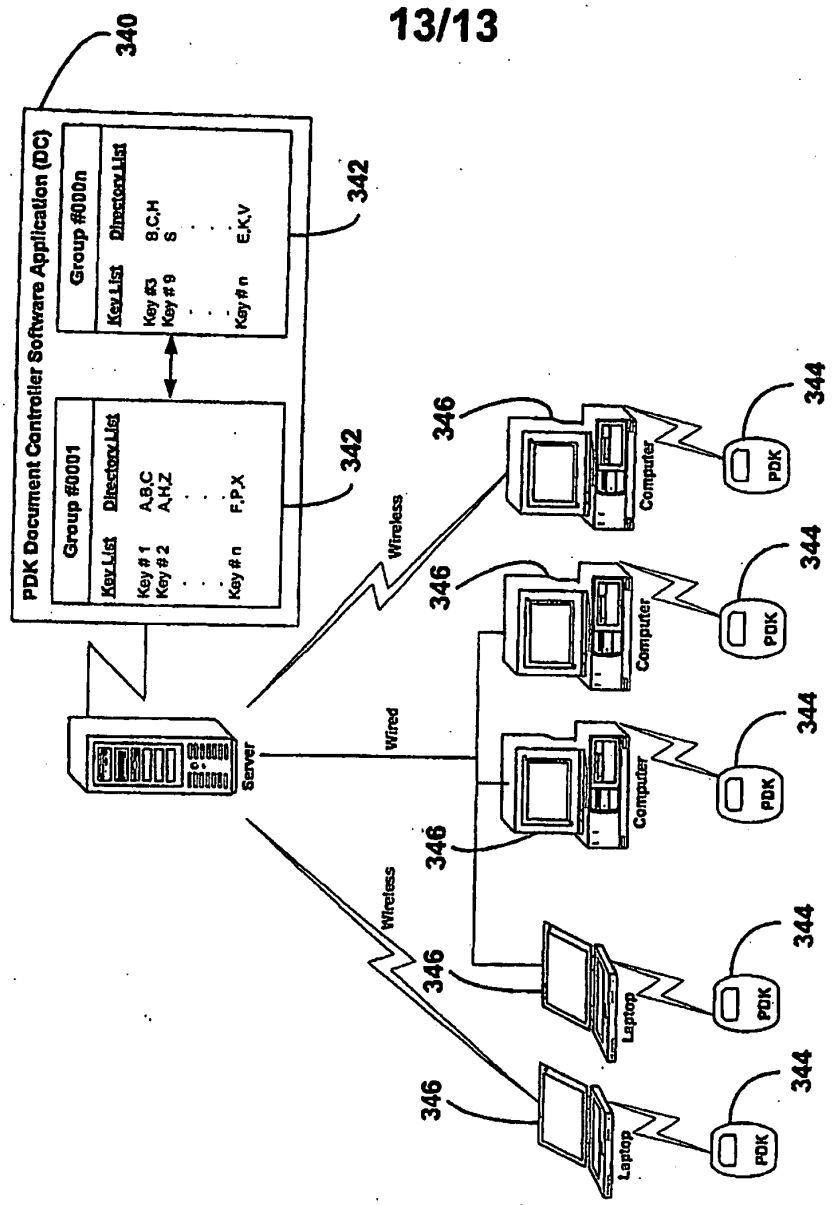

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key # 1
Key # 2
Key # n
A,B,C
A,H,Z
F,P,X
Group #000n
Key List
Directory List
Key #3
Key # 9
Key # n
B,C,H
S
E,K,V
342
342
Server
Wireless
Wired
Wireless
346
346
346
346
346
Computer
Computer
Computer
Laptop
Laptop
PDK
PDK
PDK
PDK
PDK
344
344
344
344
344

FIG. 15

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	Date of mailing of the international search report
17 March 2005 (17.03.2005)	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)

(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).

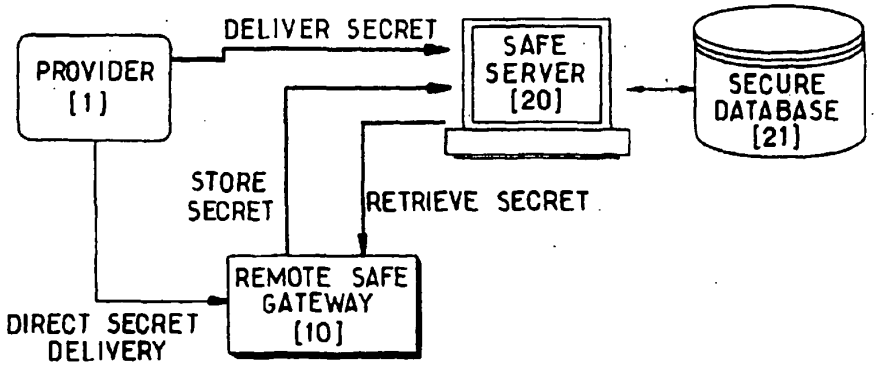
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, 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 :

- InflDuser_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, InflDuser_i for the information to be stored. InflDuser_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 InflDuser_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.

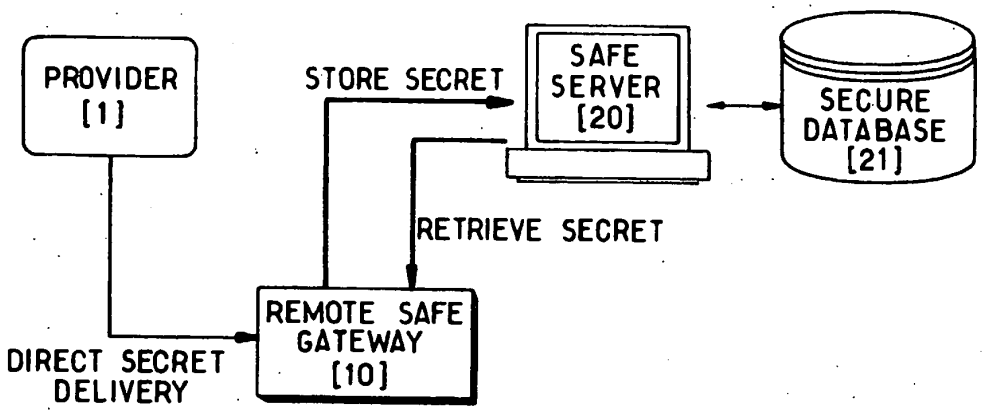

PROVIDER
[1]
STORE SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.1

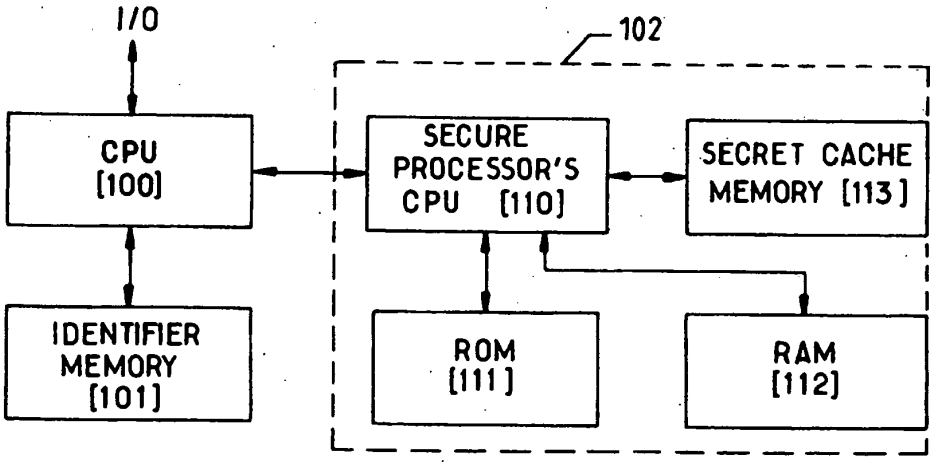

I/O
102
CPU
[100]
SECURE
PROCESSOR'S
CPU [110]
SECRET CACHE
MEMORY [113]
IDENTIFIER
MEMORY
[101]
ROM
[111]
RAM
[112]

FIG.2

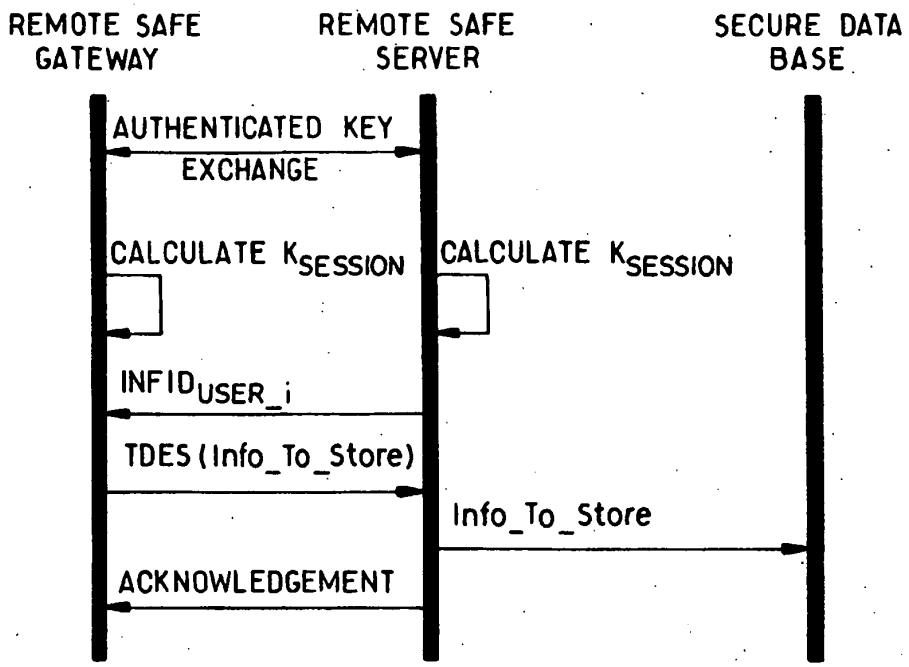

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
TDES(Info_To_Store)
Info_To_Store
ACKNOWLEDGEMENT

FIG.3

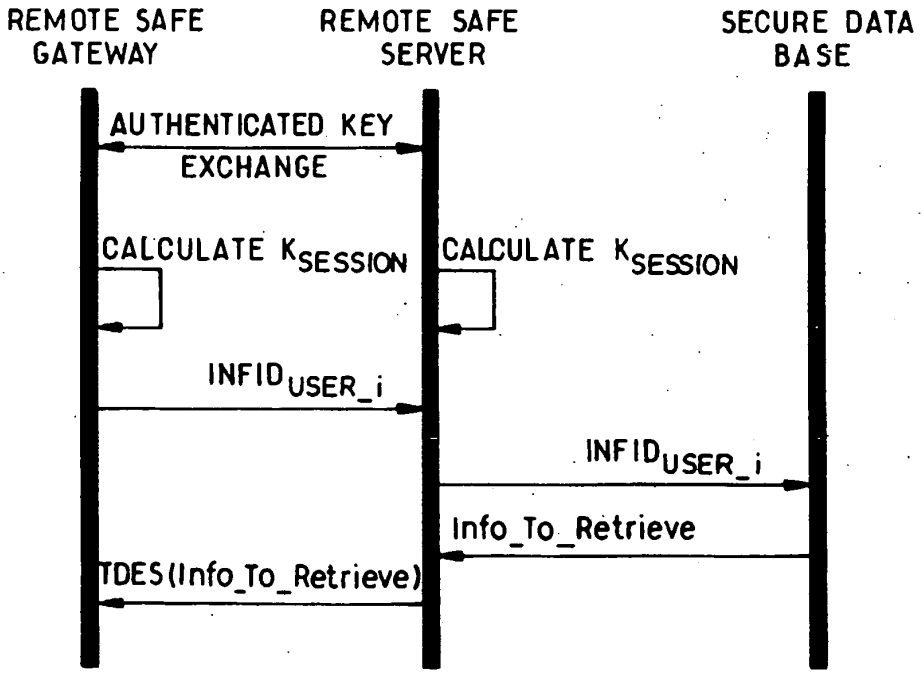

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
$INFID_{USER\_i}$
Info_To_Retrieve
TDES(Info_To_Retrieve)

FIG.4

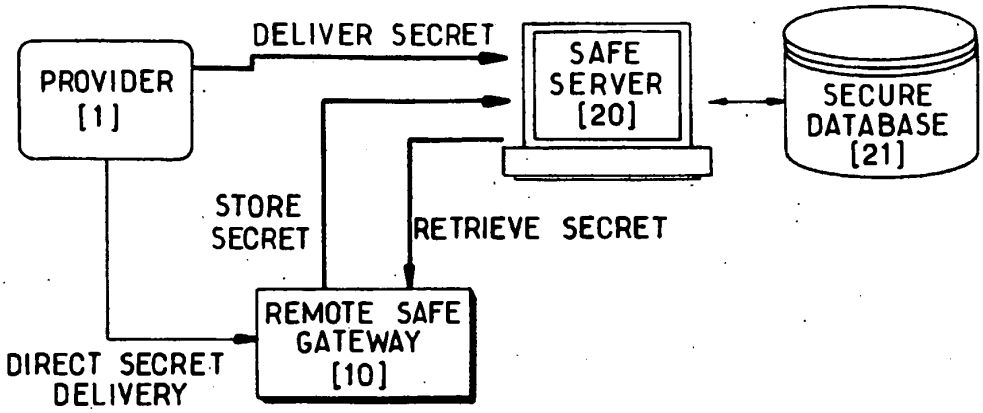

PROVIDER
[1]
DELIVER SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
STORE
SECRET
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.5

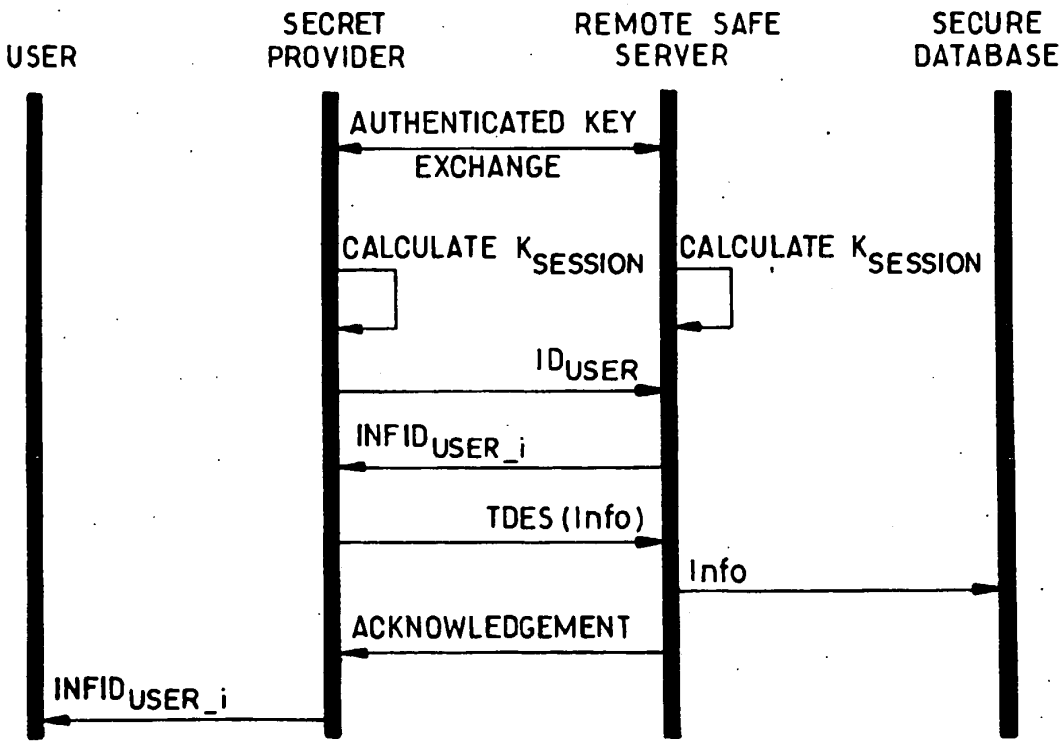

USER
SECRET
PROVIDER
REMOTE SAFE
SERVER
SECURE
DATABASE
AUTHENTICATED KEY
EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
ID_{USER}
$INFID_{USER\_i}$
TDES (Info)
Info
ACKNOWLEDGEMENT
$INFID_{USER\_i}$

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) 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).

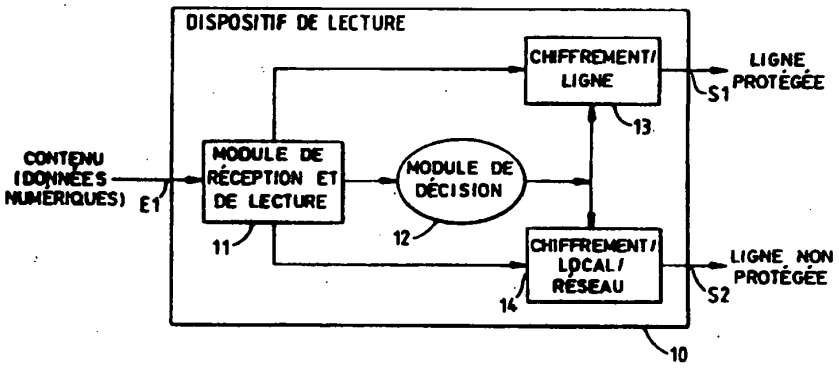
(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **DIEHL, Eric** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **ANDREAUX, Jean-Pierre** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **FURON, Teddy** [FR/FR]; Thomson 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.

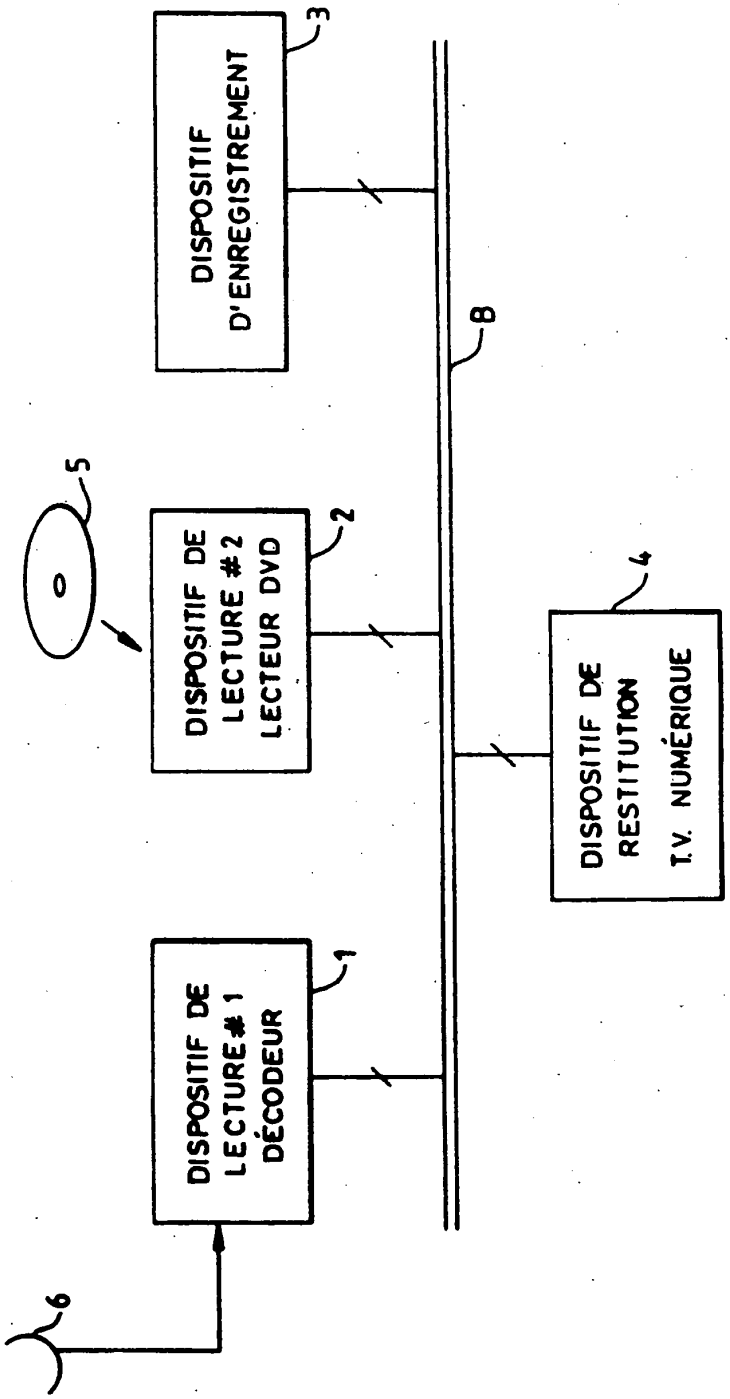

DISPOSITIF D'ENREGISTREMENT
3
8
5
DISPOSITIF DE LECTURE #2 LECTEUR DVD
2
4
DISPOSITIF DE RESTITUTION T.V. NUMÉRIQUE
DISPOSITIF DE LECTURE # 1 DÉCODEUR
1
6

FIG.1

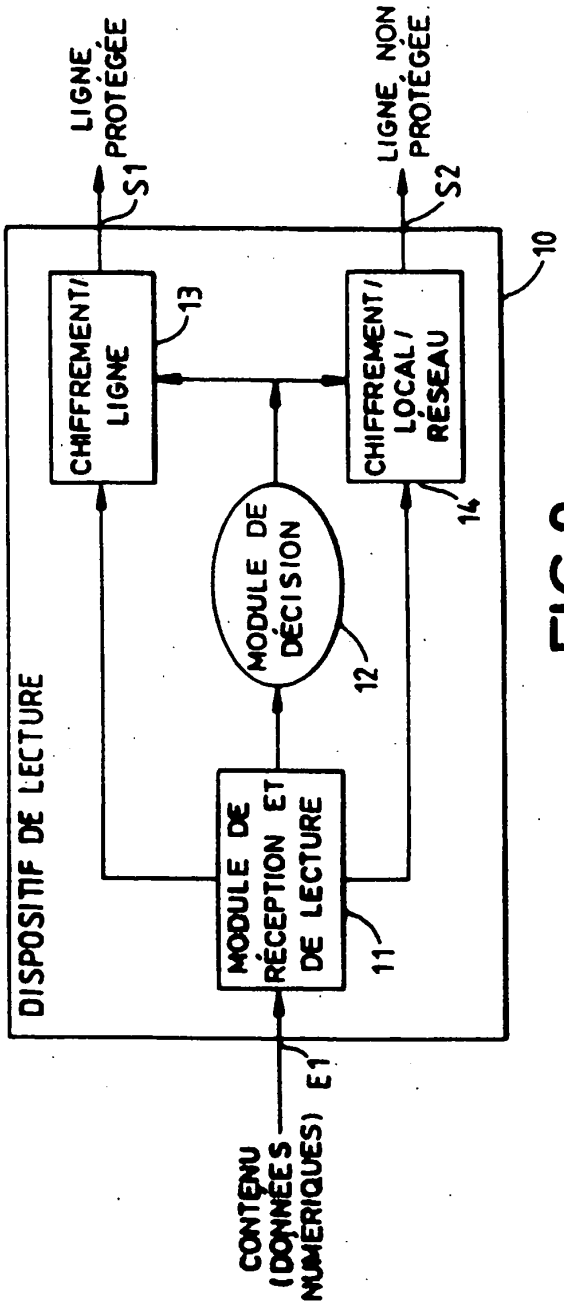

CONTENU (DONNÉES NUMÉRIQUES)
E1
DISPOSITIF DE LECTURE
MODULE DE RÉCEPTION ET DE LECTURE
11
MODULE DE DÉCISION
12
CHIFFREMENT/ LIGNE
13
CHIFFREMENT/ LOCAL/ RÉSEAU
14
10
LIGNE PROTÉGÉE
S1
LIGNE NON PROTÉGÉE
S2

FIG.2

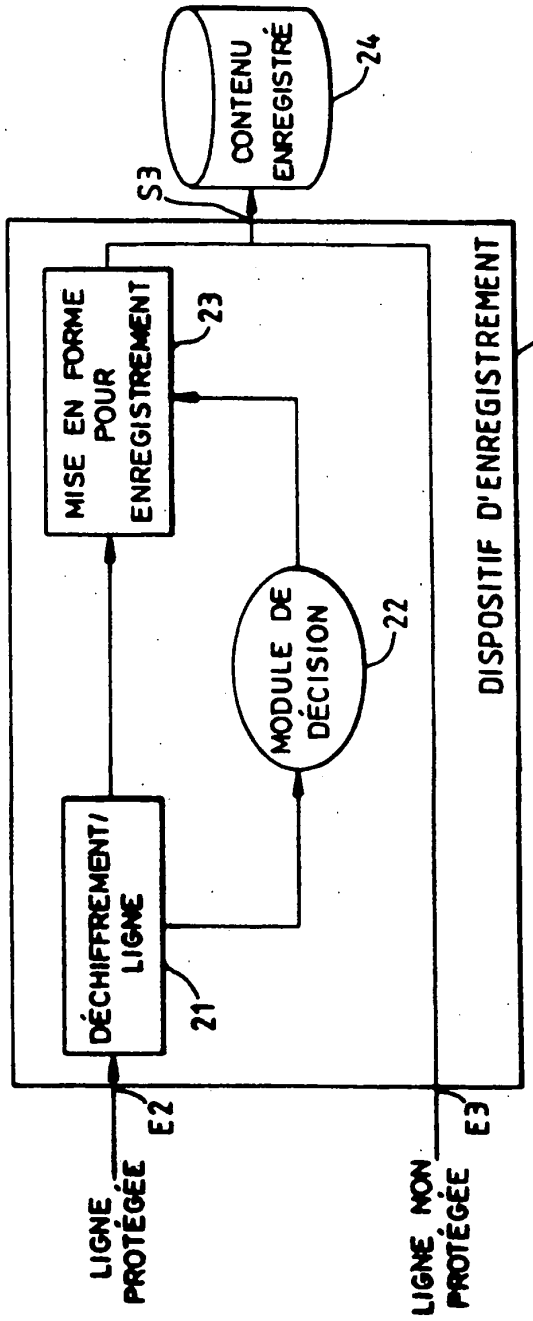

LIGNE PROTÉGÉE
E2
DÉCHIFFREMENT/ LIGNE
21
MISE EN FORME POUR ENREGISTREMENT
23
S3
CONTENU ENREGISTRÉ
24
MODULE DE DÉCISION
22
LIGNE NON PROTÉGÉE
E3
DISPOSITIF D'ENREGISTREMENT
20

FIG.3

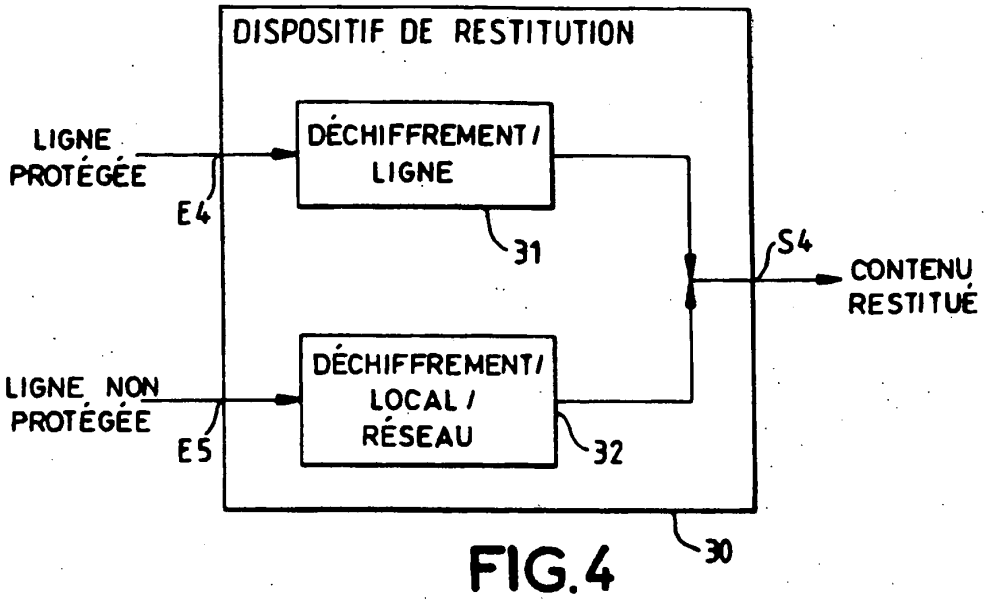

DISPOSITIF DE RESTITUTION
LIGNE PROTÉGÉE
E4
DÉCHIFFREMENT / LIGNE
31
S4
CONTENU RESTITUÉ
LIGNE NON PROTÉGÉE
E5
DÉCHIFFREMENT / LOCAL / RÉSEAU
32
30

FIG.4

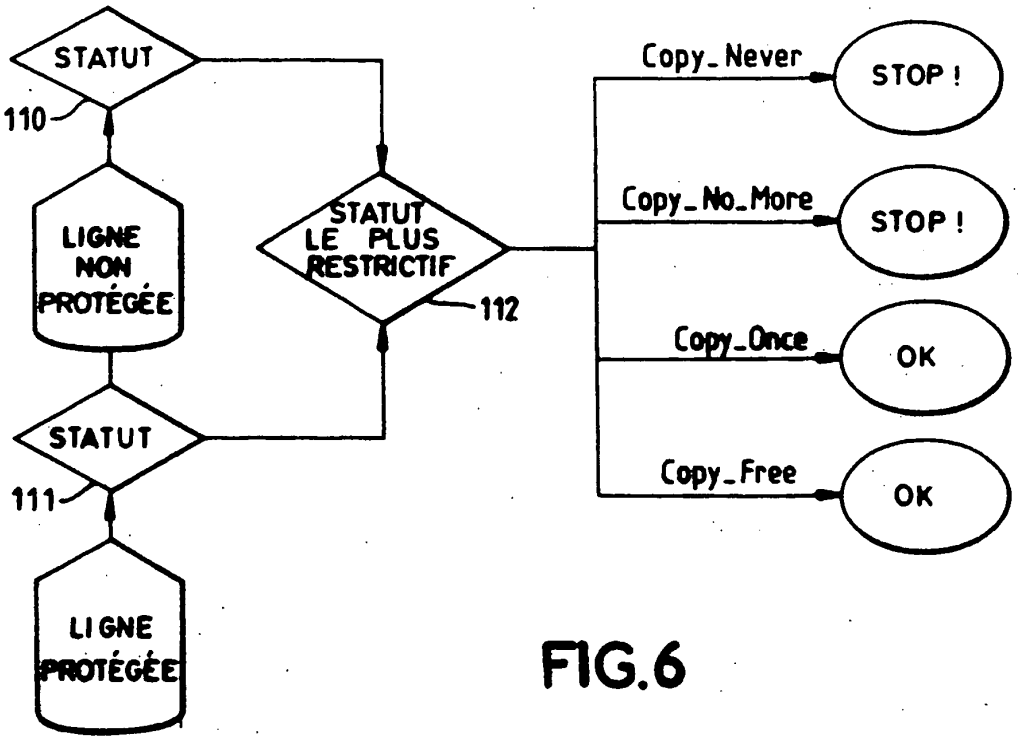

STATUT
110
LIGNE NON PROTÉGÉE
STATUT
111
LIGNE PROTÉGÉE
STATUT LE PLUS RESTRICTIF
112
Copy_Never
STOP !
Copy_No_More
STOP !
Copy_Once
OK
Copy_Free
OK

FIG.6

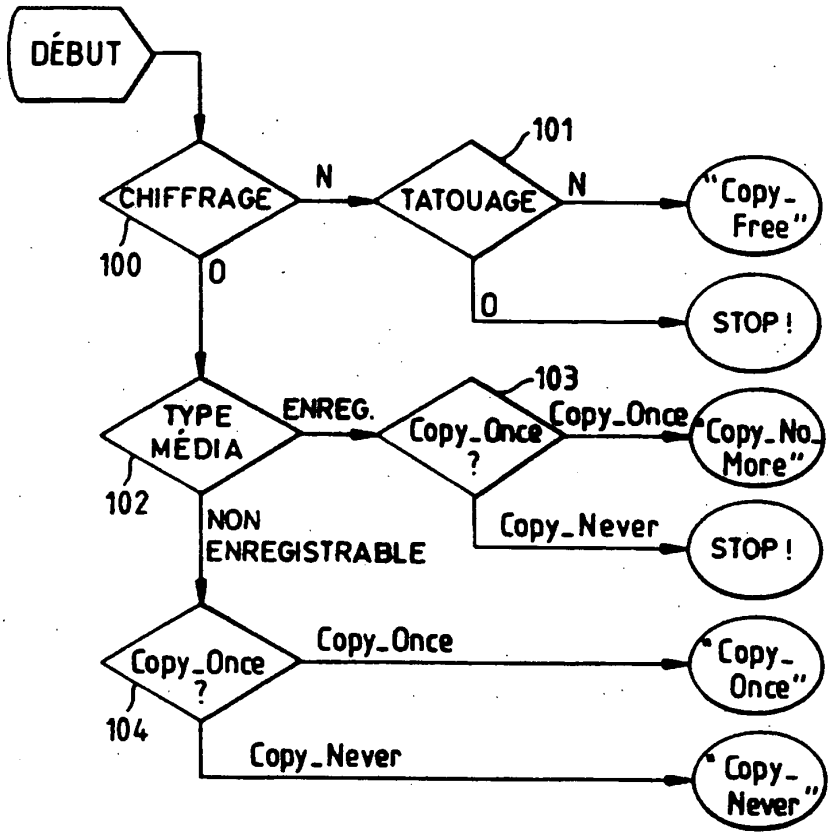

DÉBUT
CHIFFRAGE
100
N
0
TATOUAGE
101
N
0
"Copy_Free"
STOP !
TYPE MÉDIA
102
ENREG.
NON ENREGISTRABLE
Copy_Once ?
103
Copy_Once
Copy_Never
"Copy_No_More"
STOP !
Copy_Once ?
104
Copy_Once
Copy_Never
"Copy_Once"
"Copy_Never"

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

Inforn ɹn on patent family members

Internationa' olication 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' ıtionale No
PCT/FR u1/00572

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 Tél. (+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 membres de familles de brevets

Demande Internationale 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
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).

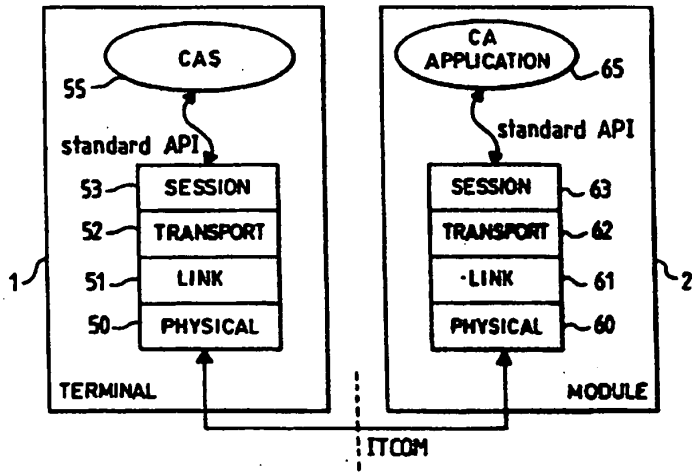
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, 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()").

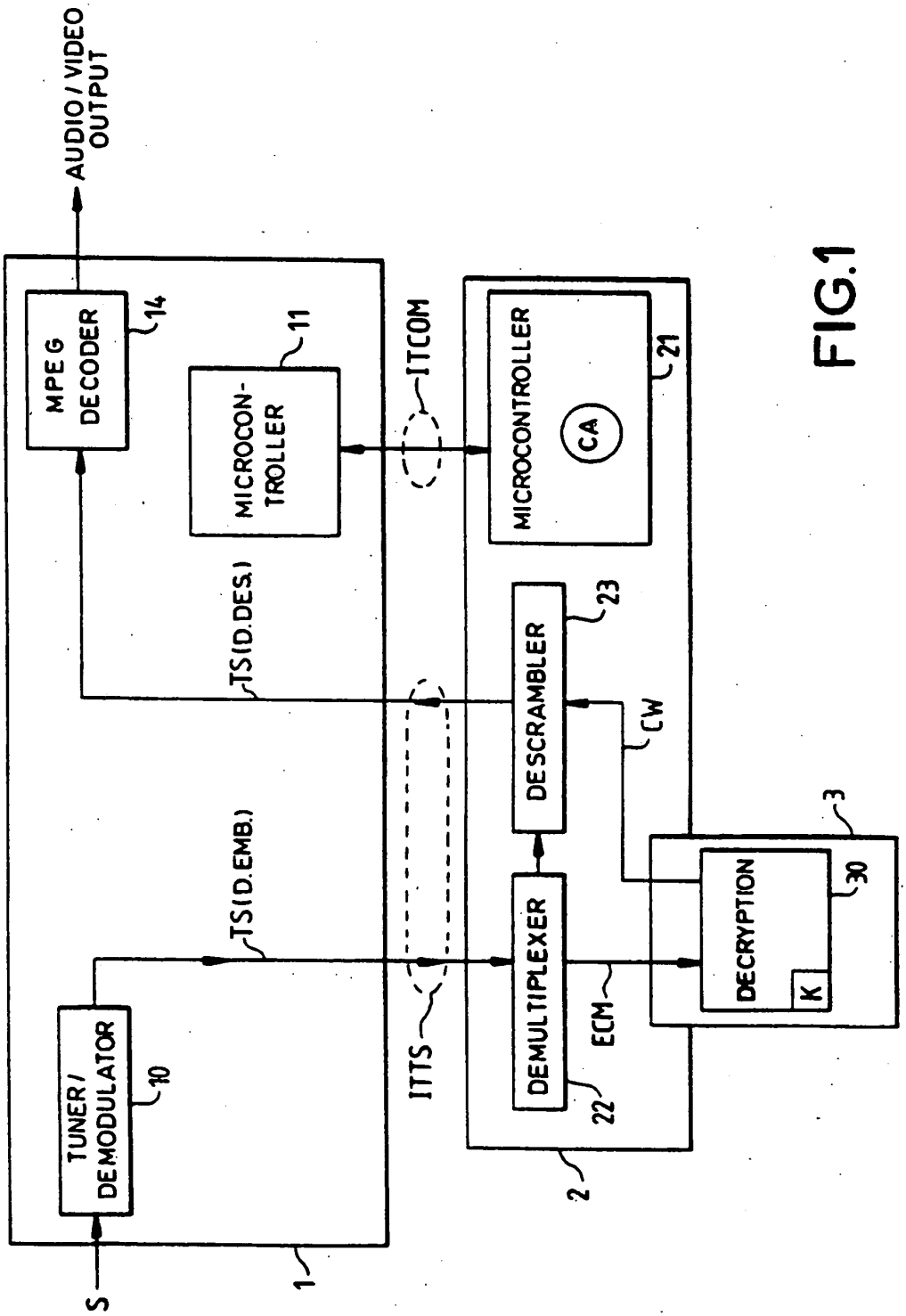

AUDIO / VIDEO OUTPUT
MPEG DECODER
14
MICROCON-TROLLER
11
ITCOM
MICROCONTROLLER
CA
21
TS(D.DES.)
DESCRAMBLER
23
CW
TS(D.EMB.)
DEMULTIPLEXER
22
ECM
DECRYPTION
K
30
3
ITTS
TUNER / DEMODULATOR
10
S
1
2

FIG.1

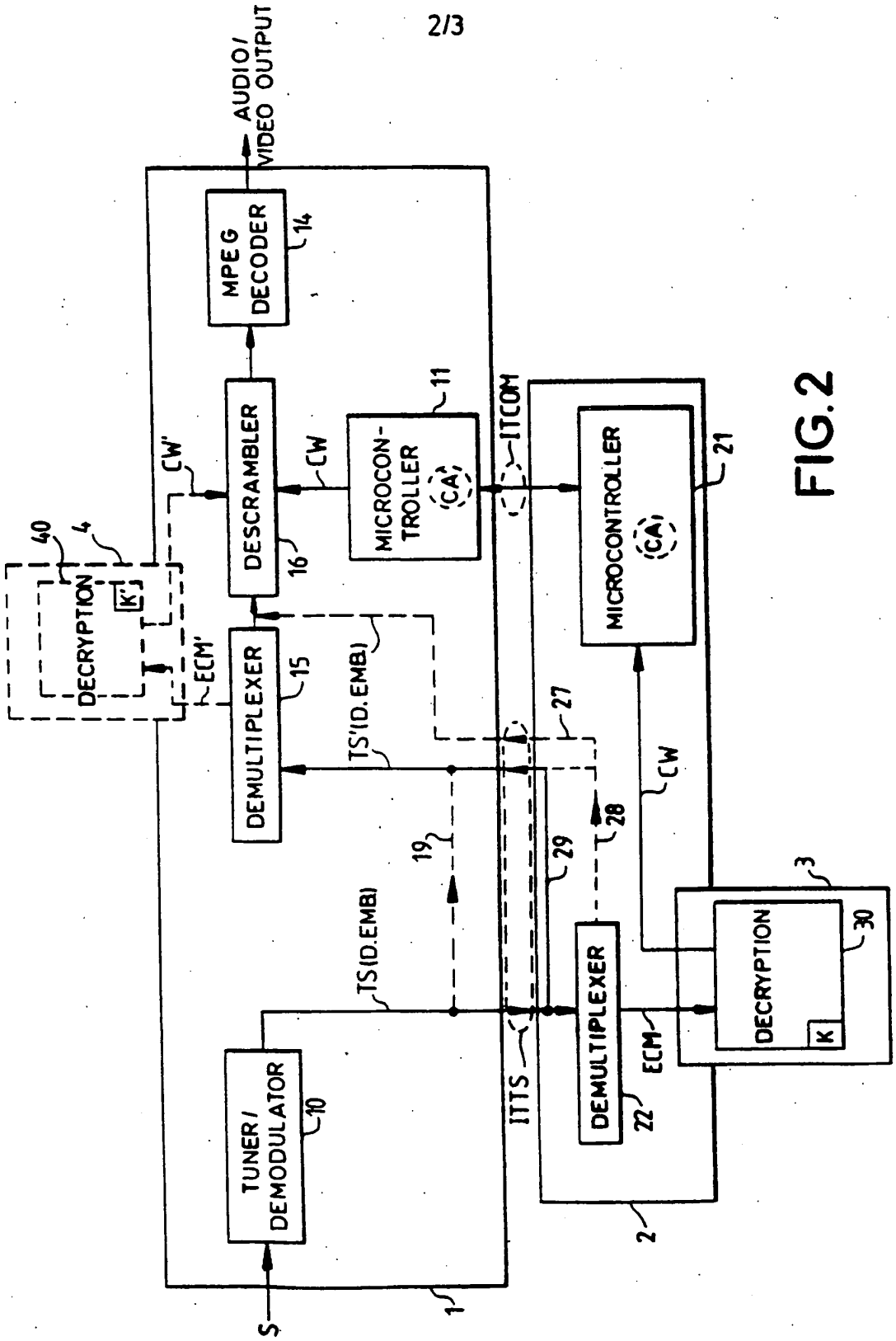

AUDIO/
VIDEO OUTPUT
MPEG
DECODER
14
DESCRAMBLER
16
CW'
CW
MICROCON-
TROLLER
(CA)
11
ITCOM
MICROCONTROLLER
(CA)
21
DECRYPTION
K'
40
4
ECM'
DEMULTIPLEXER
15
TS'(D.EMB)
27
CW
28
29
19
TS(D.EMB)
3
DECRYPTION
K
30
DEMULTIPLEXER
22
ECM
ITTS
TUNER/
DEMODULATOR
10
2
S
1

FIG.2

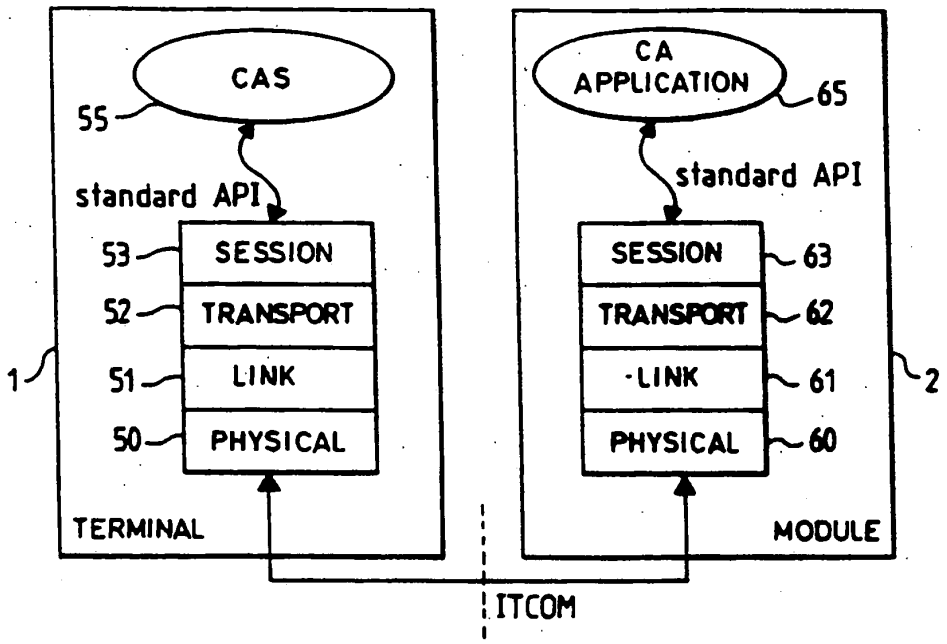

CAS
55
standard API
53
SESSION
52
TRANSPORT
1
51
LINK
50
PHYSICAL
TERMINAL
CA APPLICATION
65
standard API
SESSION
63
TRANSPORT
62
LINK
61
2
PHYSICAL
60
MODULE
ITCOM

FIG.3

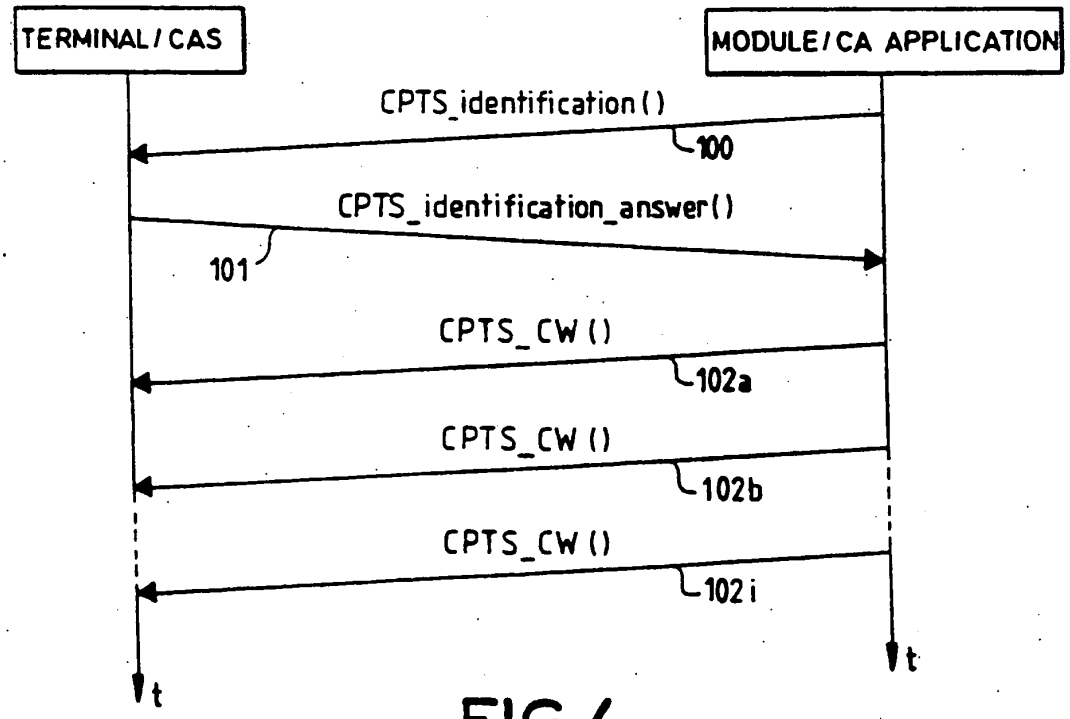

TERMINAL / CAS
MODULE / CA APPLICATION
CPTS_identification()
100
CPTS_identification_answer()
101
CPTS_CW()
102a
CPTS_CW()
102b
CPTS_CW()
102i
t
t

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 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	Authorized officer Van der Zaal, R

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. .ıal 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)

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).

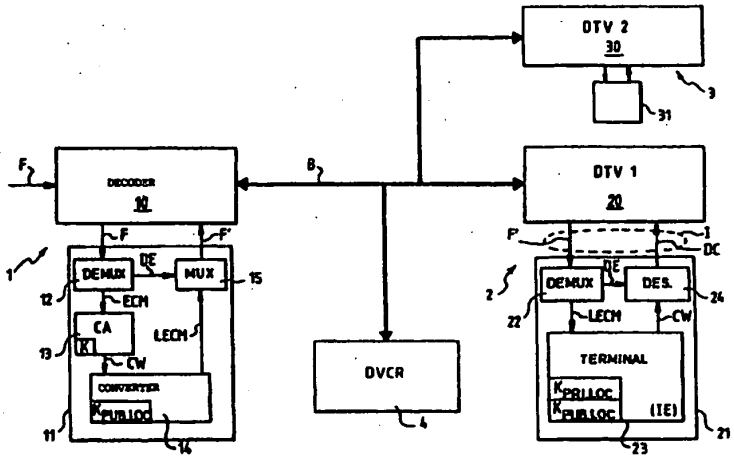
(72) Inventors; and
(75) Inventors/Applicants (*for US only*): QUES, Florence [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR). ANDREAUX, Jean-Pierre [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR). FURON, Teddy [FR/FR]; Thomson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

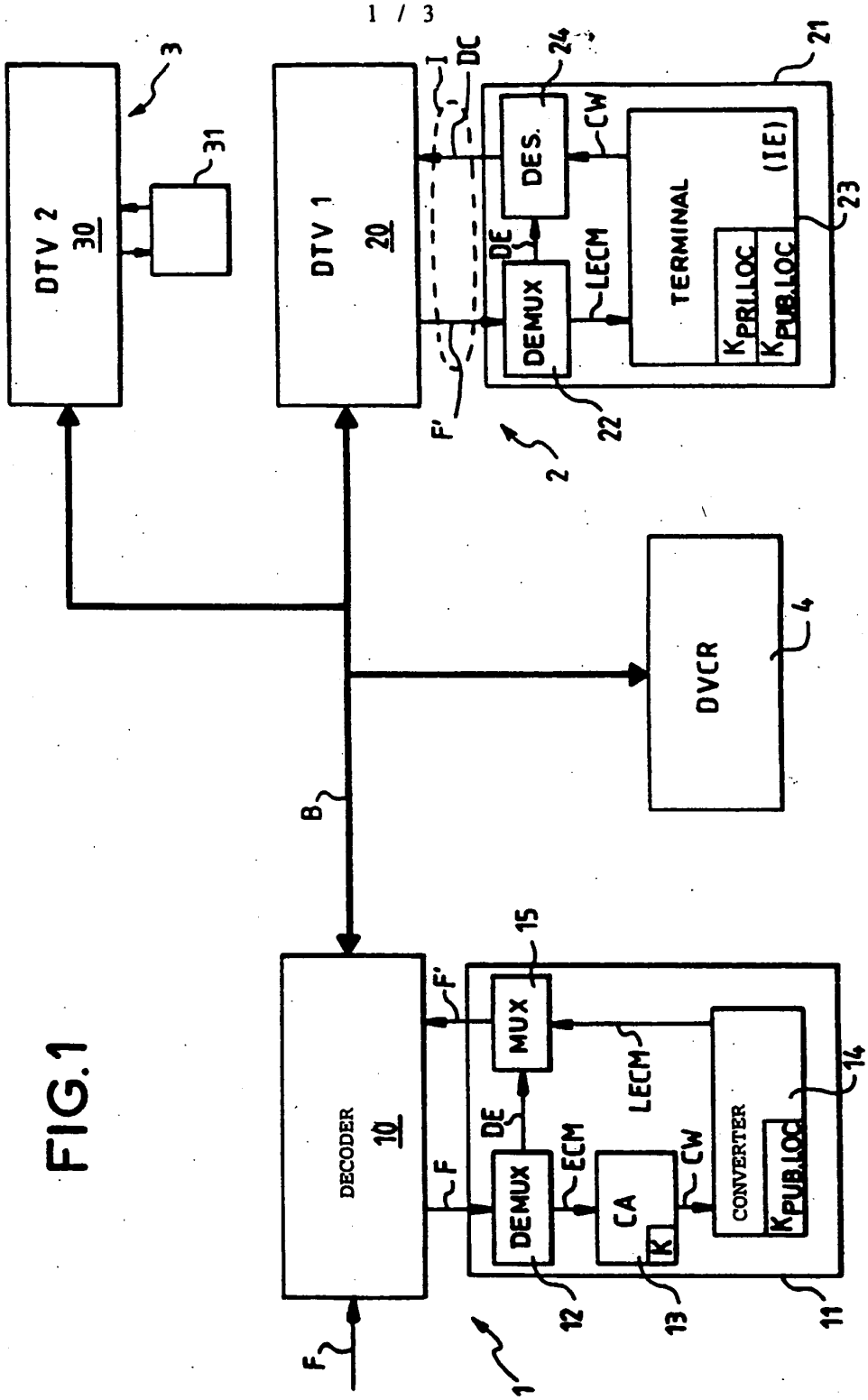

DTV 2
30
31
3
DTV 1
20
I
DC
DES.
24
CW
21
DE
DEMUX
LECM
TERMINAL
(IE)
23
$K_{PRI.LOC}$
$K_{PUB.LOC}$
22
F'
2
DVCR
4
B
DECODER
10
F
F'
MUX
15
DE
DEMUX
ECM
CA
K
CW
LECM
CONVERTER
$K_{PUB.LOC}$
14
12
13
11
1

FIG.1

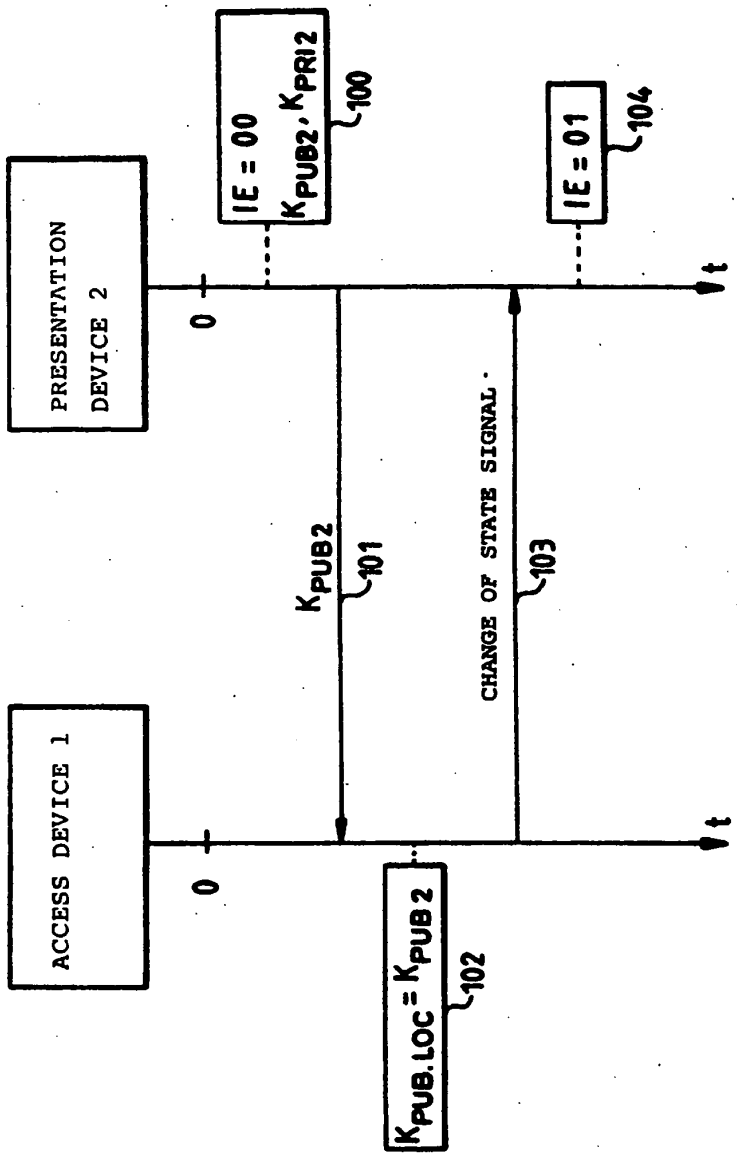

PRESENTATION DEVICE 2
ACCESS DEVICE 1
0
0
IE = 00
K_{PUB2}, K_{PRI2}
100
IE = 01
104
K_{PUB2}
101
CHANGE OF STATE SIGNAL
103
$K_{PUB.LOC} = K_{PUB2}$
102
t
t

FIG. 2

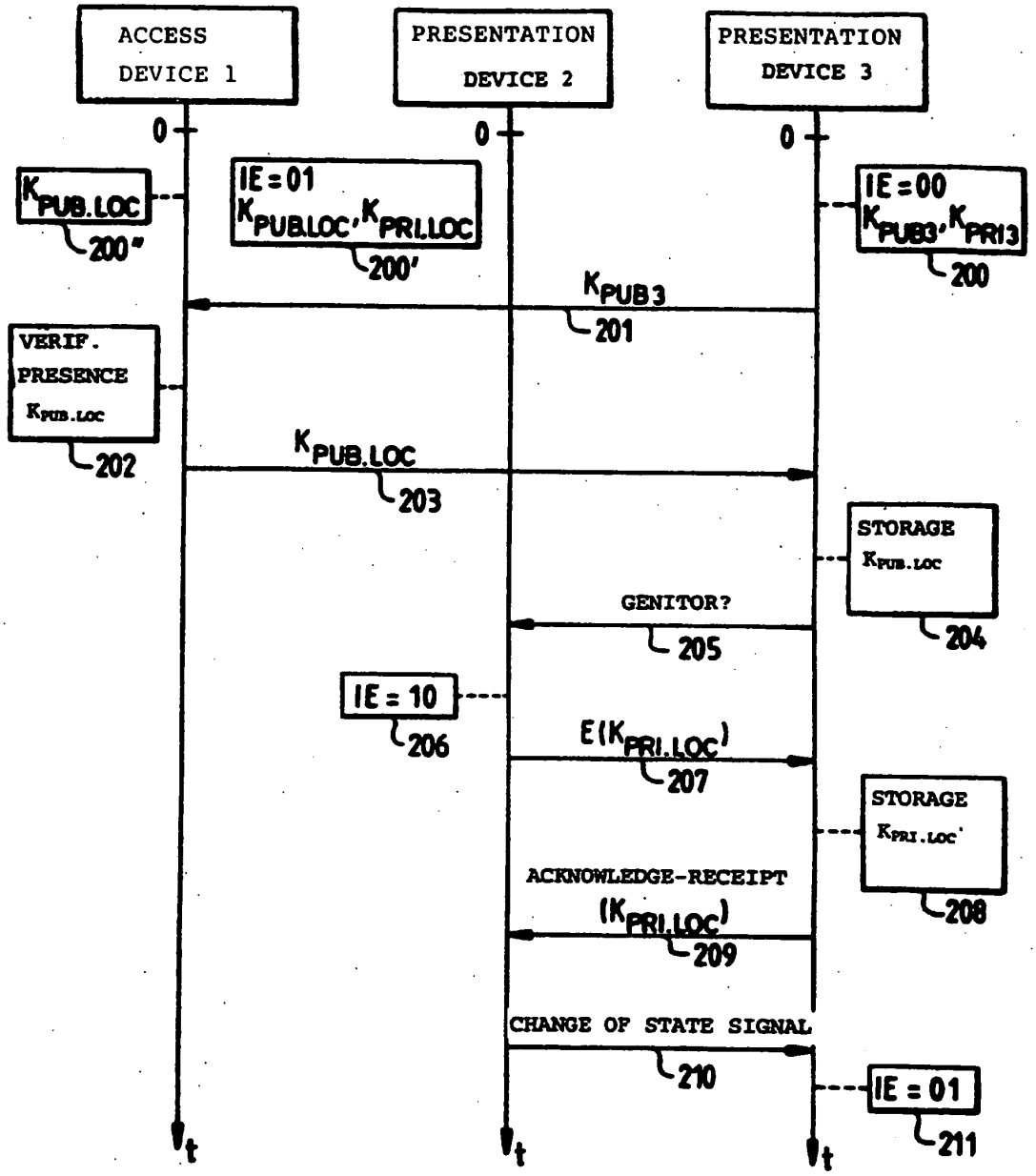

ACCESS DEVICE 1
PRESENTATION DEVICE 2
PRESENTATION DEVICE 3
0
0
0
$K_{PUB.LOC}$
200"
IE=01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE=00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
VERIF. PRESENCE $K_{PUB.LOC}$
202
$K_{PUB.LOC}$
203
STORAGE $K_{PUB.LOC}$
204
GENITOR?
205
IE = 10
206
$E(K_{PRI.LOC})$
207
STORAGE $K_{PRI.LOC}$'
208
ACKNOWLEDGE-RECEIPT
$(K_{PRI.LOC})$
209
CHANGE OF STATE SIGNAL
210
IE = 01
211
t
t
t

FIG.3

INTERNATIONAL SEARCH REPORT

Inte 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)

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/314,199	12/20/2005	John J. Giobbi	25000-11062

CONFIRMATION NO. 4469

FORMALITIES LETTER

00758
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

RECEIVED
FEB 08 2006
FENWICK & WEST

Date Mailed: 02/06/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

03/14/2006 MBELETE1 00000006 11314199

01 FC:2011	150.00 OP	
02 FC:2111	250.00 OP	
03 FC:2311	100.00 OP	
04 FC:2051	65.00 OP	
05 FC:2201	100.00 OP	
06 FC:2202	25.00 OP	

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit $ **300** *to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **$250** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$1380** for a Large Entity

- **$300** Statutory basic filing fee.
- **$130** Surcharge.

- The application search fee has not been paid. Applicant must submit **$500** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit **$200** to complete the examination fee for a large entity

- Total additional claim fee(s) for this application is **$250**

  - **$200** for **1** independent claims over 3.
  - **$50** for **1** total claims over 20.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

Ted

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 1 - ATTORNEY/APPLICANT COPY

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM *(to be used for all correspondence during pendency of filed application)*		Application Number	**11/314,199**
		Filing Date	**December 20, 2005**
		First Named Inventor	**John J. Giobbi**
		Group Art Unit Number	**2131**
		Examiner Name	**Unassigned**
Total Number of Pages in This Submission	13	Attorney Docket Number	**25000-11062**

ENCLOSURES ***(check all that apply)***

- ☒ Fee Transmittal Form (in duplicate)
  - ☒ Check Enclosed
- ☒ Return Receipt Postcard
- ☒ Response to Notice to File Missing
- ☒ Copy of Notice to File Missing Parts
- ☒ Declaration
- ☐
- ☒ Power of Attorney
- ☐ Information Disclosure Statement & PTO/SB/08A
  - ☐ Copies of IDS Cited References
- ☒ Statement Under 37 CFR 3.73(b) w/copy of Assignment
- ☐ Request for Correction of Recorded Assignment
- ☐ Response: [ ] Page(s)
  - ☐ After Final
- ☐ Status Request
- ☐ Revocation and Substitute Power of Attorney
- ☐ Issue Fee Transmittal
- ☐ Letter to Chief Draftsperson
- ☐ Formal Drawing(s): [ ] Sheet(s) of Figure(s) [ ]
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Certified Copy of Priority Document(s)
- ☐ After Allowance Communication to Group
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

REMARKS:

SIGNATURE OF ATTORNEY OR AGENT

Signature:			
Attorney/Reg. No.:	**Brian M. Hoffman**, Reg. No.: 39,713	Dated:	3/7/06

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.

Signature:			
Typed or Printed Name:	**Brian M. Hoffman**	Dated:	3/7/06
Express Mail Mailing Number (*optional*):			

25000/11062/SF/5163706.1

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT $690.00

Complete if Known	
Application Number	11/314,199
Filing Date	December 20, 2005
First Named Inventor	John Giobbi
Examiner Name	Not yet known
Art Unit	2131
Attorney Docket No.	25000-11062

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number: 19-2555

Deposit Account Name: Fenwick & West LLP

The Commissioner is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge all required fee(s) or any underpayment of fee(s) due under 37 CFR §1.16 or §1.17 during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
					500

SUBTOTAL (1) ($) 500

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims	21	-20**=	1	x	25	=	25
Independent Claims	4	-3** =	1	x	100	=	100
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	**Reissue independent claims over original patent
1205	50	2205	25	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)125.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath or declaration	65
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive - unavoidable	
1453	1,500	2453	750	Petition to revive - unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1100	2503	550	Plant issue fee	
1460	—	1460	—	Petitions to the Director	
1807	50	1807	50	Processing fee for Provisional Applications	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify) Petition Under § 1.47(a)					

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) $ 65.00

SUBMITTED BY				Complete (if applicable)
Name (Print/Type)	Brian M. Hoffman	Registration No. (Attorney/Agent)	39,713	Telephone: (415) 875-2484
Signature		Date		March 7, 2006

25000/11062/SF/5163705.1

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANT(S):	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Not Yet Known
GROUP ART UNIT:	2131
ATTY. DKT. NO.:	25000-11062

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Missing Parts, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: March 7, 2006 By: _____

Brian M. Hoffman, Reg. No.: 39,713

MAIL STOP MISSING PARTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

SIR:

Responsive to the Notice to File Missing Parts dated February 6, 2006, received in the above-identified patent application,

☒ Enclosed are:

- ☒ a copy of the Notice to File Missing Parts;
- ☒ an original, signed Declaration;
- ☒ Power of Attorney to Prosecute Before the USPTO;
- ☒ Statement Under 3.73(b); and
- ☒ a copy of the Assignment.

☒ payment in the amount of $690.00 for the

- ☒ statutory basic filing fee;
- ☒ application search fee;
- ☒ application examination fee;
- ☒ missing parts surcharge; and
- ☒ additional claim fees.

☒ Applicant claims small entity status under 37 C.F.R. § 1.27.

Respectfully submitted,
JOHN J. GIOBBI

Dated: March 7, 2006

By: _____

Brian M. Hoffman, Reg. No.: 39,713
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax.: (415) 281-1350

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☐ Declaration Submitted With Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	25000-11062
First Named Inventor	John Giobbi
COMPLETE IF KNOWN	
Application Number	11/314,199
Filing Date	December 20, 2005
Art Unit	2131
Examiner Name	Not yet assigned

I hereby declare that:

Each inventor's residence, mailing address, and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

(Title of the Application)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 12/20/2005 as United States Application Number or PCT International Application Number 11/314,199 and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? Yes	No
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

DECLARATION – Utility or Design Patent Application

Direct all correspondence to: ☒ Customer Number: 758 OR ☐ Correspondence address below			
Name			
Address			
City	State	ZIP	
Country	Telephone	Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any]) John J.		Family Name or Surname Globbi	
Inventor's Signature			Date 3/6/06
Residence: City Bend	State OR	Country USA	Citizenship USA
Mailing Address 689 NW Stonepine Dr.			
City Bend	State OR	ZIP 97701	Country USA

☐ Additional inventors or a legal representative are being named on additional sheet(s)

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b)

I hereby appoint:

☒ Practitioners associated with the Customer Number **758**

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Assignee Name and Address:

Proxense, LLC
689 NW Stonepine Dr.
Bend, OR 97701

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record
The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Name	John J. Giobbi		
Signature		Date 1/31/06	Jan 31, 2006
Title	Managing Partner	Telephone	(541)382-5745

25000/01000/DOCS/1594189.1

OIPE IAP69
MAR 13 2006
PATENT & TRADEMARK OFFICE

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: John J. Giobbi

Application No./Patent No.: 11/314,199 Filed/Issue Date: December 20, 2005

Entitled: Biometric Personal Data Key (PDK) Authentication

Proxense, LLC, a Delaware Corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
   The extent (by percentage) of its ownership interest is _____%

in the patent application/patent identified above by virtue of either:

A. [x] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

B. [ ] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From _____ To: _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
2. From _____ To: _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
3. From _____ To: _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet.

[ ] Copies of assignments or other documents in the chain of title are attached.
[NOTE: A separate copy (*i.e.*, a true copy of the original document) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

March 7, 2006
Date

Brian M. Hoffman
Typed or printed name

415.875.2484
Telephone number

Signature

Attorney for Applicant
Title

25000/11062/SF/5163702.1

NOT FOR RECORDATION

PATENT

ASSIGNMENT

For good and valuable consideration, the receipt of which is hereby acknowledged, the person(s) named below (referred to as "INVENTOR" whether singular or plural) has sold, assigned, and transferred and does hereby sell, assign, and transfer to Proxense, LLC, a Delaware corporation, having a place of business at 689 NW Stonepine Dr., Bend, OR 97701, ("ASSIGNEE"), for itself and its successors, transferees, and assignees, the following:

1. The entire worldwide right, title, and interest in all inventions and improvements ("SUBJECT MATTER") that are disclosed in the provisional application filed under 35 U.S.C. §111(b) or non-provisional application filed under 35 U.S.C. §111(a) and entitled BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION ("APPLICATION"), which:

   ☒ was filed on **December 20, 2005**, and now bears U.S. application serial number **11/314,199**.

2. The entire worldwide right, title, and interest in and to:

(a) the APPLICATION; (b) all applications claiming priority from the APPLICATION; (c) all provisional, utility, divisional, continuation, substitute, renewal, reissue, and other applications related thereto which have been or may be filed in the United States or elsewhere in the world; (d) all patents (including reissues and re-examinations) which may be granted on the applications set forth in (a), (b), and (c) above; and (e) all right of priority in the APPLICATION and in any underlying provisional or foreign application, together with all rights to recover damages for infringement of provisional rights.

INVENTOR agrees that ASSIGNEE may apply for and receive patents for SUBJECT MATTER in ASSIGNEE's own name.

INVENTOR agrees to do the following, when requested, and without further consideration, in order to carry out the intent of this Assignment: (1) execute all oaths, assignments, powers of attorney, applications, and other papers necessary or desirable to fully secure to ASSIGNEE the rights, titles and interests herein conveyed; (2) communicate to ASSIGNEE all known facts relating to the SUBJECT MATTER; and (3) generally do all lawful acts that ASSIGNEE shall consider desirable for securing, maintaining, and enforcing worldwide patent protection relating to the SUBJECT MATTER and for vesting in ASSIGNEE the rights, titles, and interests herein conveyed. INVENTOR further agrees to provide any successor, assign, or legal representative of ASSIGNEE with the benefits and assistance provided to ASSIGNEE hereunder.

INVENTOR represents that INVENTOR has the rights, titles, and interests to convey as set forth herein, and covenants with ASSIGNEE that the INVENTOR has not made and will not hereafter make any assignment, grant, mortgage, license, or other agreement affecting the rights, titles, and interests herein conveyed.

INVENTOR grants the attorney of record the power to insert on this Assignment any further identification that may be necessary or desirable in order to comply with the rules of the United States Patent and Trademark Office for recordation of this document.

This Assignment may be executed in one or more counterparts, each of which shall be deemed an original and all of which may be taken together as one and the same Assignment.

Title of Document: ASSIGNMENT

NOT FOR RECORDATION

PATENT

Re:
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION
Filed: December 20, 2005
Application No.: 11/314,199

Name and Signature

John Giobbi

Date of Signature

3/6, 2006

Case Docket # 25000-11062

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/314,199	12/20/2005	John J. Giobbi	25000-11062

CONFIRMATION NO. 4469
FORMALITIES LETTER

00758
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

Date Mailed: 02/06/2006

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit $ **300** *to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **$250** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$1380** for a Large Entity

- **$300** Statutory basic filing fee.
- **$130** Surcharge.

- The application search fee has not been paid. Applicant must submit **$500** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit **$200** to complete the examination fee for a large entity

- Total additional claim fee(s) for this application is **$250**

  - **$200** for **1** independent claims over 3.
  - **$50** for **1** total claims over 20.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

Ted

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382
PART 3 - OFFICE COPY

20427 U.S.PTO
122005

112935 U.S.PTO
11/314199
122005

NEW UTILITY PATENT APPLICATION TRANSMITTAL

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

Attorney Docket Number	25000-11062
First Named Inventor	John J. Giobbi
Title	Biometric Personal Data Key (PDK) Authentication
Express Mail Label No.	EV 301187013 US

APPLICATION ELEMENTS

1. ☐ Fee Transmittal Form (in duplicate)
2. ☒ Applicant claims small entity status. See 37 CFR 1.27
3. ☒ Specification *Total Pages* 25
   (preferred arrangement set forth below)
   - Descriptive Title of the Invention
   - Cross Reference(s) to Related Case(s)
   - Statement Regarding Fed sponsored R & D
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawing(s)
   - Detailed Description
   - Claim or Claims
   - Abstract of the Disclosure
4. ☒ Drawing(s) *(35 U.S.C. 113)* *Total Sheets* 6
5. Oath or Declaration
   a. ☐ New Declaration *Total Pages* ☐
      ☐ Executed (original or copy)
   b. ☐ Copy from a prior application (37 CFR 1.63(d))
      (for continuation/divisional with Box 18 completed)
      i. ☐ DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
9. ☐ Power of Attorney or Authorization of Agent
10. ☐ 37 CFR 3.73(b) Statement
11. ☐ Preliminary Amendment
12. ☐ Information Disclosure Statement & PTO/SB/08A
    ☐ Copies of IDS Citation(s)
13. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent
14. ☒ Return Postcard
15. ☐
16. ☐
17. ☐

ADDRESS TO:

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

18. **If a CONTINUING APPLICATION,** *check appropriate box and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: ___/_____

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

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuing or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☒ *Customer Number* 00758

Name (Print/Type)	Brian M. Hoffman	*Registration No. (Attorney/Agent)*	39,713
Signature		*Date*	December 20, 2005

25000/01000/SF/5157778.1

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

INVENTOR: JOHN J. GIOBBI

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application 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 both applications being herein 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 allowing 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, a biometric key persistently (or permanently) stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a fingerprint or retinal scan) can be compared against the biometric data. Once the user has been verified by the integrated device, the code can be wirelessly transmitted to indicate that the user has been successfully verified.

[0008] In one embodiment, an authentication module sends the code to a trusted key authority. The trusted key authority checks a list of enrolled biometric keys to determine whether the code is valid. If the code is valid, the authentication module allows the user to access an application.

[0009] In another embodiment, the trusted key authority can store a profile associated with the biometric key having the code. The profile can contain user information such as name, age, account numbers, preferences, and the like. In addition, the profile can describe the status of the key, identify the trusted key authority, and/or contain other information. The profile can also be sent to the authentication module for use by the application (e.g., an age of user sent to a casino machine).

[0010] Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in a single key. Furthermore, a keyless en-

vironment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the key can be authenticated for an application that is open to the public (i.e., in an open loop system).

[0011] 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

[0012] The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

[0013] 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.

[0014] FIG. 2 is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

[0015] FIG. 3 is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

[0016] FIG. 4 is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

[0017] FIG. 5 is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

[0018] 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.

[0019] 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

[0020] 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.

[0021] 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.

[0022] 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. Biometric key 100 comprise 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 a automobile remote control) such that it can be unobtrusively carried by a user.

[0023] 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.

[0024] 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.

[0025] 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.

[0026] 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 combina-

tion of hardware and software components as described above. In one embodiment, biometric key 100 comprises a modified key fob.

[0027] 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.

[0028] Biometric portion 220 comprises enrollment module 222, validation module 224, and biometric data base 226. In one embodiment, enrollment module 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.

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] 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 communication module 230 can actively send out connection requests, or passively detect connection requests.

[0034] Battery 260 can be a conventional power source suitable for the components of biometric key 100. Battery 260 can be either replaceable or re-

chargeable. Alternatively, battery 260 can be embedded within key 100 such that the key must be discarded or recycled upon expiration of the battery.

[0035] 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.

[0036] 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.

[0037] 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, and the like. 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.

[0038] 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.

[0039] 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.

[0040] 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.

[0041] 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 biometric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

[0042] 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.

[0043] 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.

[0044] 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 notary, 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.

[0045] 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.

[0046] 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.

[0047] 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.

[0048] 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).

[0049] 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.

[0050] 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.

[0051] 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.

[0052] 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.

[0053] 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.

[0054] 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.

[0055] 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, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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 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;

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.

2. The method of claim 1, wherein the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.

3. The method of claim 1, further comprising:

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

4. The method of claim 1, wherein the code uniquely identifies the integrated device.

5. The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. The method of claim 1, wherein persistently storing biometric data comprises:

permanently storing biometric data.

7. The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. The method of claim 1, further comprising:

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.

10. An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user in a tamper-resistant format;

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.

11. The integrated device of claim 10, wherein the persistent storage permanently stores biometric data.

12. The integrated device of claim 10, wherein the code is registered with a trusted authority, wherein the code can be authenticated to a third party by the trusted authority.

13. The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. A method for authenticating a verified user, comprising:

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.

16. The method of claim 15, further comprising:

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.

17. The method of claim 16, further comprising:

registering a date of birth or age with the trusted authority.

18. The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. 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;

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.

20. The system of claim 19, wherein 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.

21. The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

ABSTRACT

[0060] Systems and methods are provided for an integrated device that persistently (or permanently) stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a fingerprint) can be compared against the biometric data. Once the user has been verified by the integrated device, a code can be wirelessly transmitted for authentication. The authentication module sends the code to a trusted key authority. The trusted key authority checks a list of enrolled integrated devices for a match. If there is a match, the authentication module sends a message to an application to allow access by the user. The trusted key authority also stores a profile associated with the code. The profile can contain user information such as name, age, account numbers, preferences, etc. and can also describe the status of the integrated device.

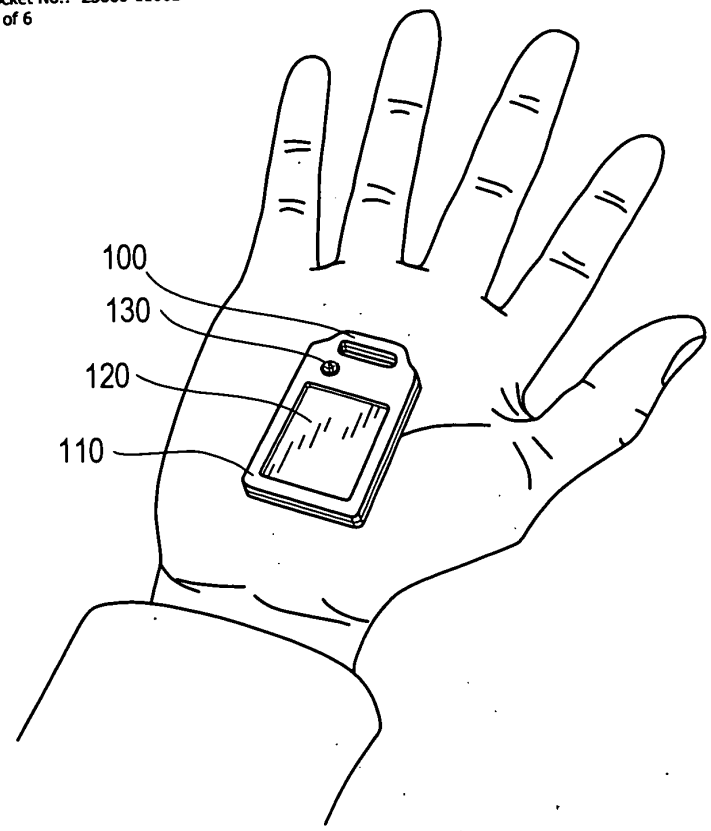

100
130
120
110

FIG. 1

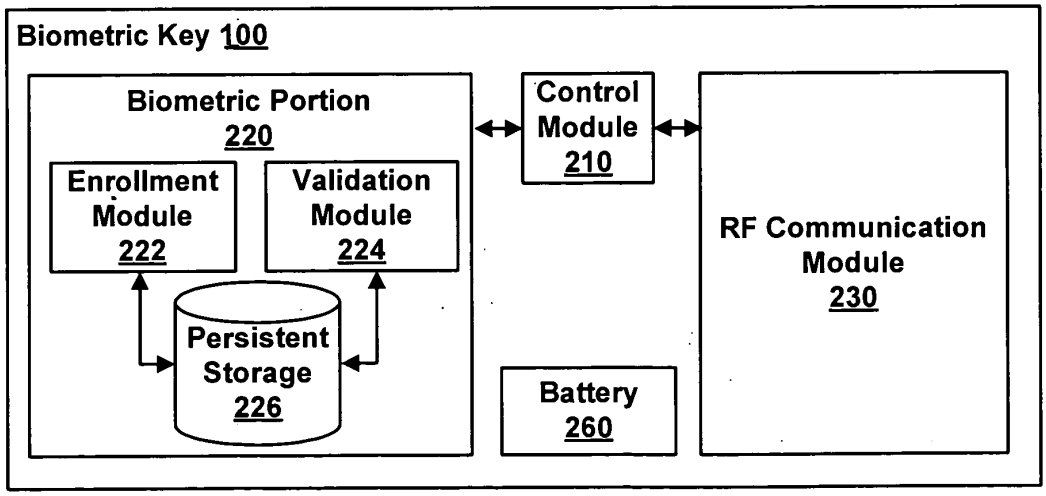

Biometric Key 100
Biometric Portion 220
Enrollment Module 222
Validation Module 224
Persistent Storage 226
Control Module 210
Battery 260
RF Communication Module 230

FIG. 2

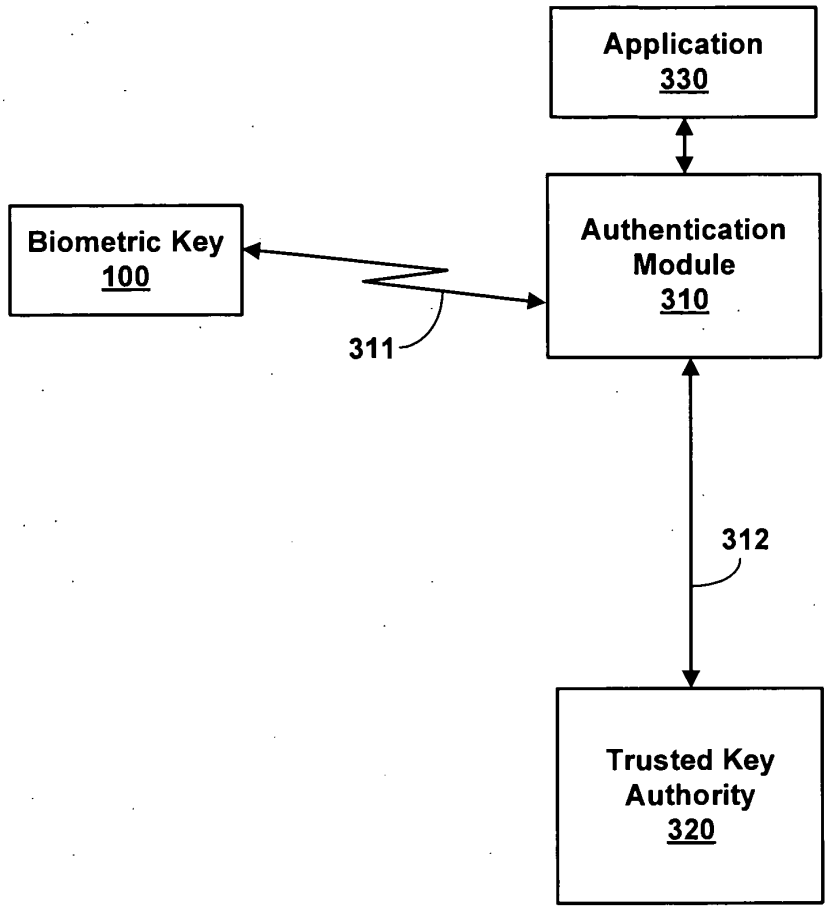

Application
330
Biometric Key
100
Authentication Module
310
311
312
Trusted Key Authority
320

FIG. 3

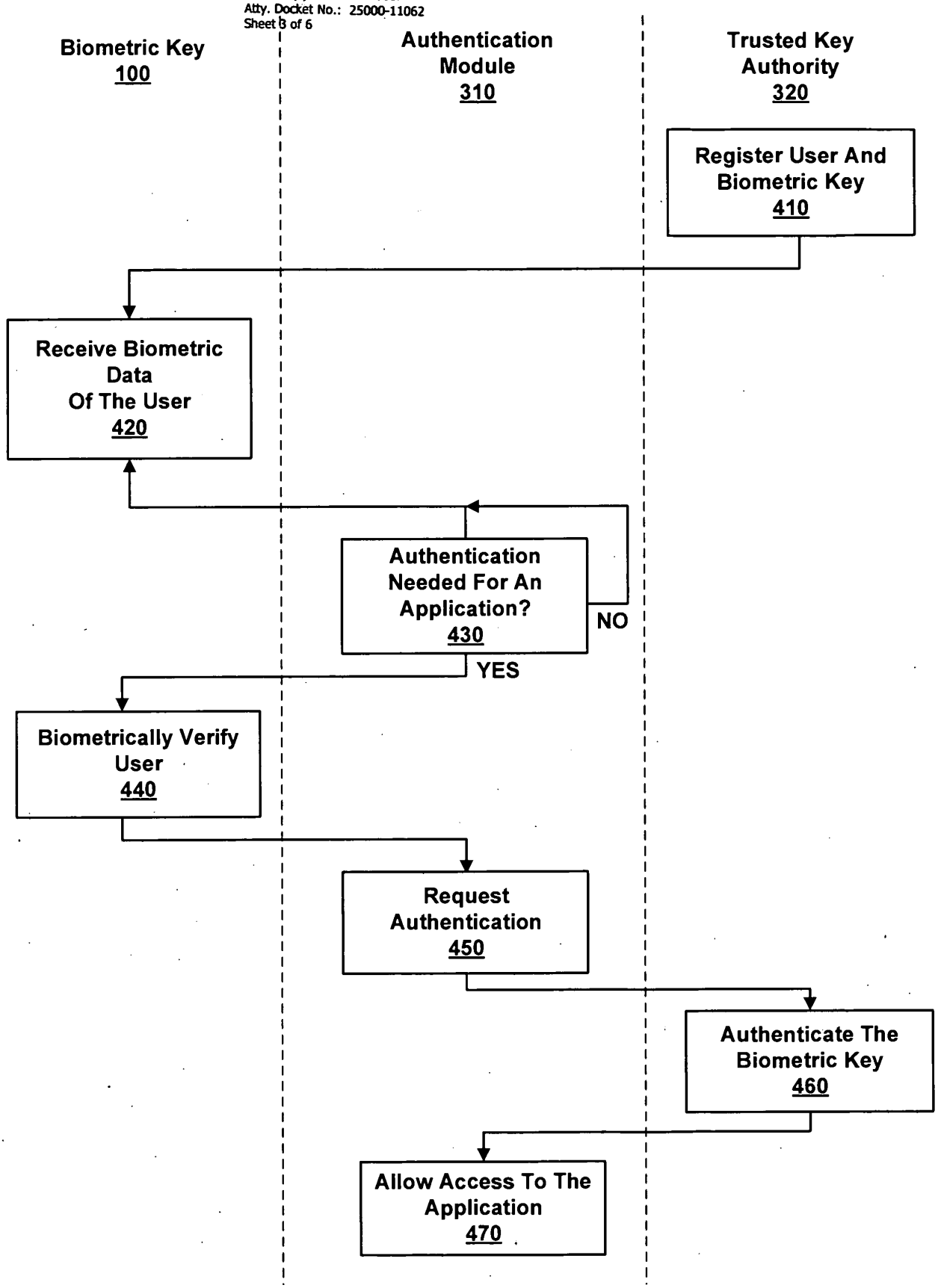

Biometric Key
100
Authentication Module
310
Trusted Key Authority
320
Register User And Biometric Key
410
Receive Biometric Data Of The User
420
Authentication Needed For An Application?
430
NO
YES
Biometrically Verify User
440
Request Authentication
450
Authenticate The Biometric Key
460
Allow Access To The Application
470

FIG. 4

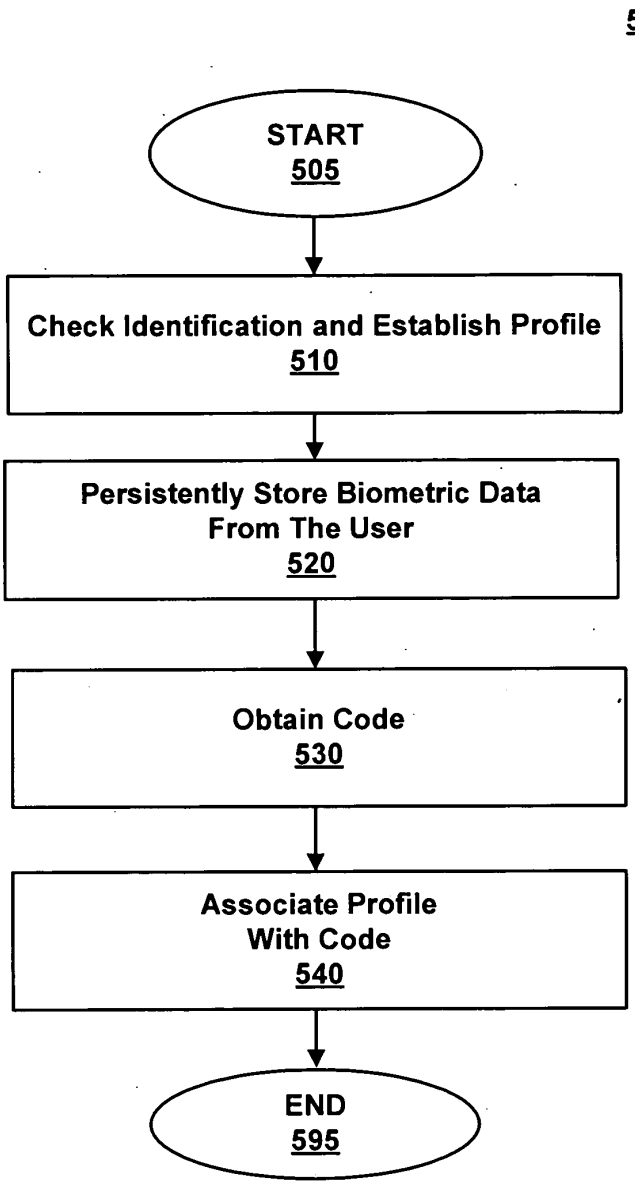

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data From The User
520
Obtain Code
530
Associate Profile With Code
540
END
595

FIG. 5

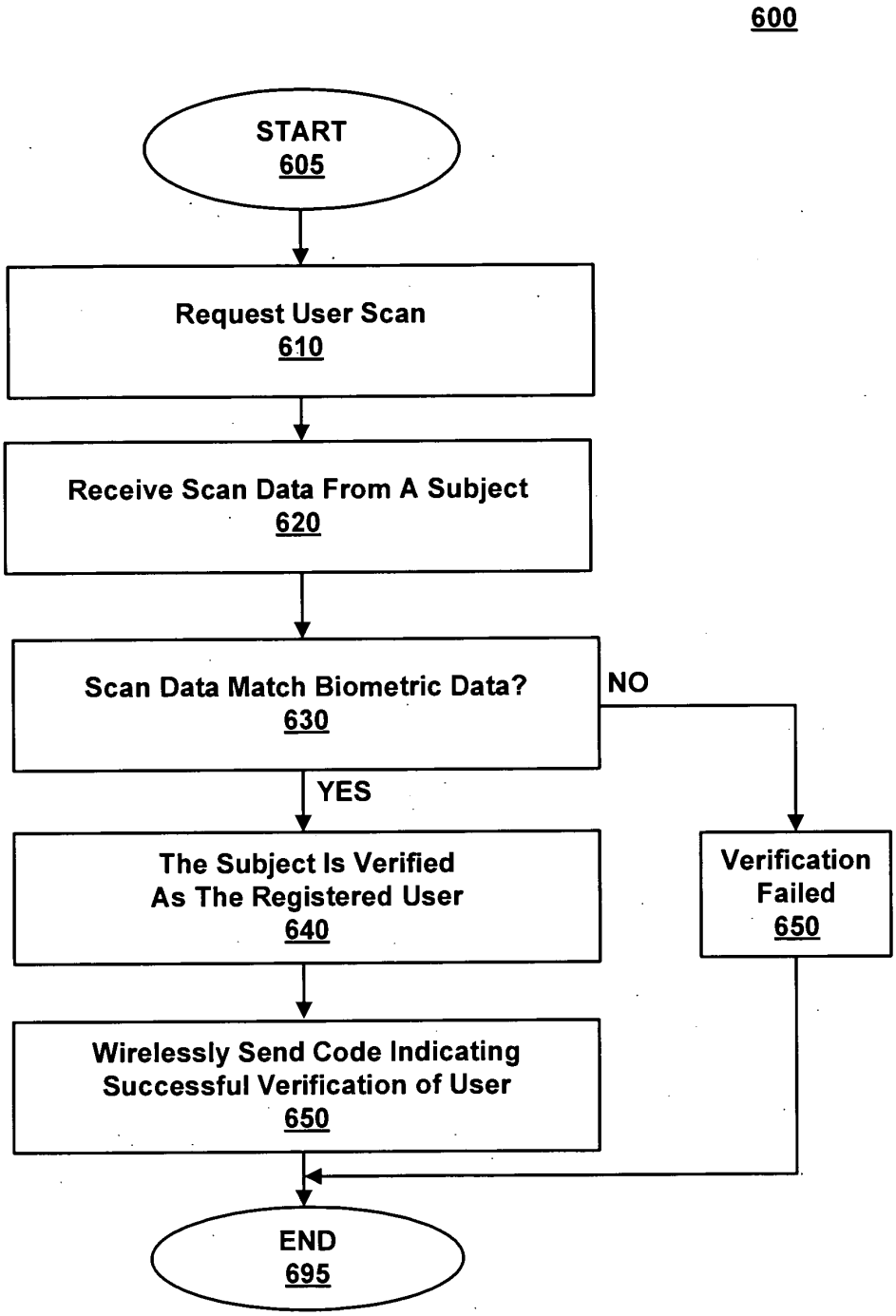

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified As The Registered User
640
Verification Failed
650
Wirelessly Send Code Indicating Successful Verification of User
650
END
695

FIG. 6

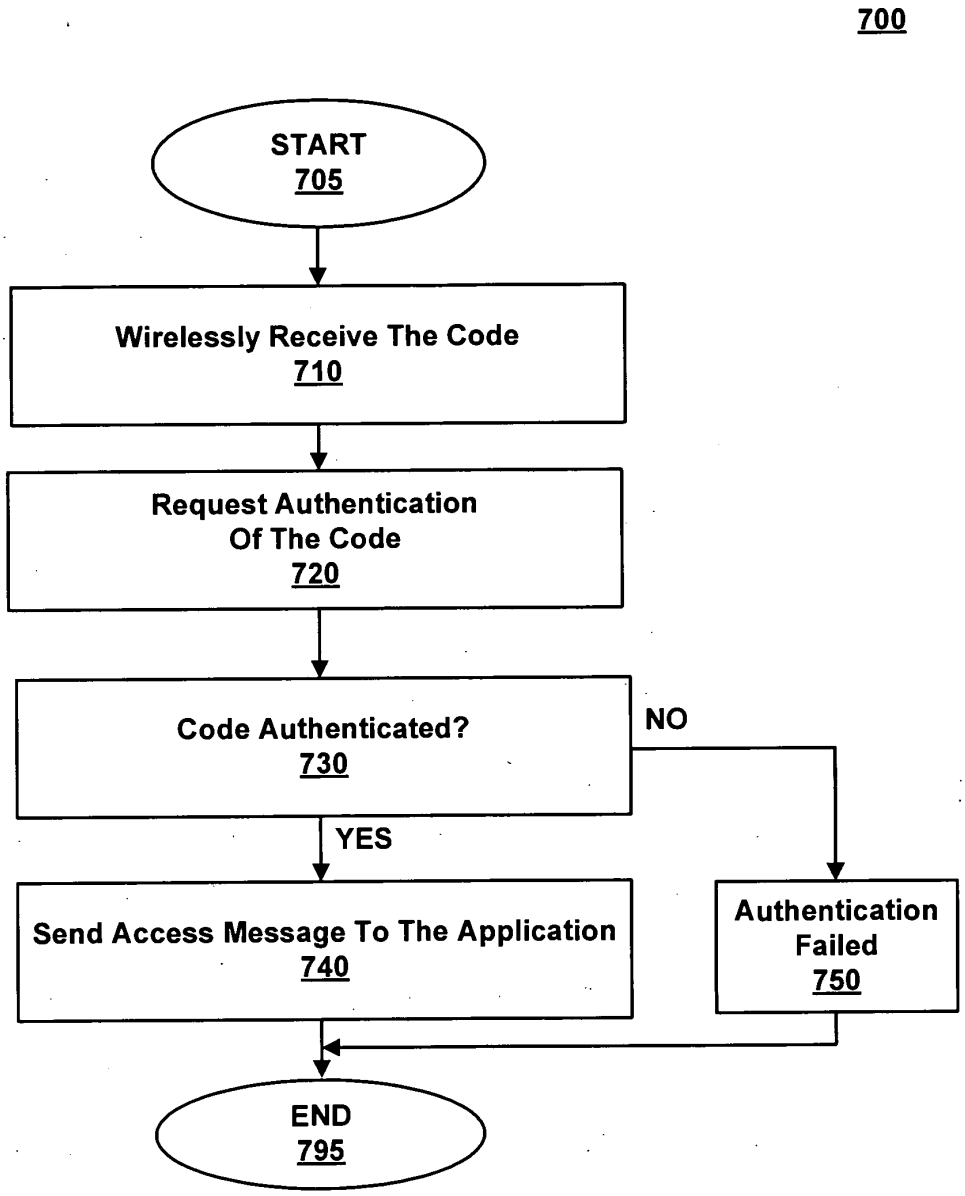

700
START
705
Wirelessly Receive The Code
710
Request Authentication Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication Failed
750
END
795

FIG. 7

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 11314199

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	150		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	250		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	100		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	X$ 25=	25	OR	X$50=	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	X$100=	100		X$200=	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A			N/A	
			TOTAL	625		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

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 ($)	SMALL ENTITY ADDI-TIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDI-TIONAL FEE ($)
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))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDI-TIONAL FEE ($)	OR	RATE ($)	ADDI-TIONAL FEE ($)
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))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

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

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Paten 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.