PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

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

Secrecy Order 37 CFR 5.2

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

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	David	L.	Brown	

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

City	Jupiter	State/Province	FL	Country of Residence i	US

Mailing Address of Inventor:

Address 1	c/o Proxense, LLC		
Address 2	689 NW Stonepine Drive		
City	Bend	**State/Province**	OR
Postal Code	97701	**Country** i	US

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

Correspondence Information:

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

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

Customer Number	89194		
Email Address	docketing@patentlawworks.net	Add Email	Remove Email

Application Information:

Title of the Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use		
Attorney Docket Number	10001-04293 US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	15	**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

Publication Information:

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

Representative Information:

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

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	89194		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13445825	2012-04-12

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13445825	Continuation of	12329329	2008-12-05	8171528	2012-05-01

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12329329	Claims benefit of provisional	60992953	2007-12-06

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

Foreign Priority Information:

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

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

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

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

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

(•) Assignee	( ) Legal Representative under 35 U.S.C. 117	( ) Joint Inventor
( ) Person to whom the inventor is obligated to assign.	( ) Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. [X]

Organization Name	Proxense, LLC		
Mailing Address Information:			
Address 1	689 NW Stonepine Drive		
Address 2			
City	Bend	**State/Province**	O
Country [i]	US	Postal Code	97701
Phone Number		Fax Number	

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

Email Address	

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

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/Kanda Ishihara/			Date (YYYY-MM-DD)	2014-02-03
First Name	Kanda	Last Name	Ishihara	Registration Number	56607

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10001-04293 US
	Application Number	
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use	

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE

INVENTOR:
DAVID L. BROWN

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority under 35 U.S.C. § 120 to U.S. Patent Application 13/445,825 entitles "Hybrid Device Having a Personal Digital Key and Receiver Decoder Circuit and Method of Use," filed April 12, 2012, which claims priority under 35 U.S.C. § 120 to U.S. Patent Application 12/329,329 entitled "Hybrid Device Having a Personal Digital Key and Receiver Decoder Circuit and Method of Use," filed December 5, 2008, now U.S. Patent No. 8,171,528, which claims the benefit of priority under 35 U.S.C. § 119(e) of U.S. Provisional Application No. 60/992,953 entitled "Reverse Prox," filed on December 6, 2007 by David L. Brown, John J. Giobbi and Fred S. Hirt. The entire contents of all of the foregoing are incorporated by reference herein.

BACKGROUND

1. FIELD OF ART

[0002] The invention generally relates to personal digital keys and corresponding sensors, capable of proximity detection/location determination and auxiliary data services/application services. Still more particularly, the present invention relates to a hybrid device including a personal digital key (PDK) and a receiver-decoder circuit (RDC) and methods for using same.

2. DESCRIPTION OF THE RELATED ART

[0003] Proximity sensors and location tracking are technologies with many applications. For example, proximity sensors can be used to provide secure access to physical and/or digital assets, based on biometrics, passwords, PINs, or other types of authentication. Proximity sensors typically have advantages of being less cumbersome, easier to use, and more flexible in form factor and implementation. Proximity sensors can be used to control access to resources and/or to authenticate individuals, for example.

[0004] One possible application that can take advantage of proximity sensors is location tracking. RFID tracking is one example. In RFID, RFID tags are attached to objects to be tracked. RFID readers then interact with the RFID tags to determine the location of the tag. Regardless of how it is accomplished, location tracking (i.e., knowledge about the location of an object or person) is generally useful. For example, location tracking information can be used to track inventory and trace the route of objects through various locations. It can be used for time and motion studies. If tags are attached to people, then tracking of people can be used to better understand their behavior. Knowledge about a person's location (and/or their past locations and projected future locations) could be used to provide better services to that person.

[0005] However, most proximity systems and location tracking systems have limited capabilities. Typically, the proximity sensor, RFID tag or similar device is a dumb device, in the sense that the device is designed and has the capability only to report its location. For example, such devices typically do not have the capabilities to run different applications or to even interact with different applications. Furthermore, these systems typically are proprietary and narrowly tailored for a specific situation, thus preventing easy expandability to other situations or third party applications.

SUMMARY

[0006] Various drawbacks of the prior art are overcome by providing a hybrid device including a personal digital key (PDK) and a receiver-decoder circuit (RDC). The PDK and RDC of the hybrid device are coupled for communication with each other. In one embodiment, the hybrid device also provides a physical interconnect for connecting to other devices to send and receive control signals and data, and receive power. The hybrid device operates in one of several modes including, PDK only, RDC only, or PDK and RDC. This allows a variety of system configurations for mixed operation including: PDK/RDC, RDC/RDC or PDK/PDK. The present invention also includes a number of system configurations for use of the hybrid device including: use of the hybrid device in a cell phone; simultaneous use of the PDK and the RDC functionality of hybrid device; use of multiple links of hybrid device to generate an authorization signal, use of multiple PDK links to the hybrid device to generate an authorization signal; use of the hybrid device for authorization inheritance and use of the hybrid device for automatically disabling a service or feature.

[0007] Other aspects of the invention include systems and components corresponding to the above, and methods corresponding to all of the foregoing.

BRIEF DESCRIPTION OF THE FIGURES

[0008] FIG. 1 is a block diagram illustrating one embodiment of a system according to the invention.

[0009] FIG. 2 is a block diagram illustrating one embodiment of a Personal Digital Key (PDK).

[0010] FIG. 3 is a block diagram illustrating one embodiment of a sensor.

[0011] FIGS. 4-6 are block diagrams illustrating further embodiments of systems according to the invention.

[0012] FIG. 7 is a block diagram illustrating one embodiment of a system with networked sensors.

[0013] FIGS. 8-9 are block diagrams illustrating operation of the system in FIG. 7.

[0014] FIG. 10 is a diagram illustrating operation of the system in FIG. 7.

[0015] FIG. 11 is a block diagram of one embodiment of a hybrid device in accordance with the present invention.

[0016] FIG. 12 is a block diagram of one embodiment of a system in which the hybrid device is part of a cell phone in accordance with the present invention.

[0017] FIG. 13 is a block diagram of one embodiment of a system using the PDK and the RDC functionality of hybrid device in accordance with the present invention.

[0018] FIG. 14 is a block diagram of one embodiment of a system using the multiple links of hybrid device to generate an authorization signal in accordance with the present invention.

[0019] FIG. 15 is a block diagram of one embodiment of a system using the multiple PDK links to the hybrid device to generate an authorization signal in accordance with the present invention.

[0020] FIG. 16 is a block diagram of one embodiment of a system using the hybrid device for authorization inheritance in accordance with the present invention.

[0021] The figures depict various embodiments of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

DETAILED DESCRIPTION

[0022] FIG. 1 is a high level block diagram illustrating a system for allowing access to multiple applications (or services). The system 100 comprises a Personal Digital Key (PDK) 102, a sensor 108, a network 110 and one or more applications 120 (including services). The sensor 108 is coupled to the PDK 102 by a wireless link 106 and coupled to a network 110 by either a wired or wireless link. In this example, the applications 120 are also accessed over network 110. The sensor 108 is also adapted to receive a biometric input 104 from a user and is capable of displaying status to a user. In alternative embodiments, different or additional resources and databases may be coupled to the network 110, including for example registries and databases used for validation or to check various registrations of the user. In another embodiment, the sensor 108 operates as a standalone device without a connection to the network 110.

[0023] The PDK 102 includes multiple service blocks 112A-N as described in more detail in FIG. 2. Each service block 112 is accessed using a corresponding service block access key 118. In this example, the sensor 108 contains three of the service block access keys 118A, D, F. The service block access keys 118 allow the sensor 108 to unlock information stored in the corresponding service blocks 112, which information is used as local secured information.

[0024] In one example, a biometric is required in order to access specific service blocks 112 in the PDK 102. Verification of the biometric is achieved by using service block 112A. The sensor 108 stores the corresponding service block access key 118A and uses this key to unlock the biometric service block 112A, which stores a valid biometric. A current biometric is received using biometric input 104. The sensor 108 then verifies the stored biometric (from service block 112A) against the recently acquired biometric (from input 104). Upon proper verification, various applications 120 are permitted to connect to the PDK 102 via the sensor 108 and/or to gain access to other service blocks 112.

[0025] The system 100 can be used to address applications 120 where it is important to authenticate an individual for use. Generally, the sensor 108 wirelessly receives information stored in the PDK 102 that uniquely identifies the PDK 102 and the individual carrying the PDK 102. The sensor 108 can also receive a biometric input 104 from the individual. Based on the received information, the sensor 108 determines if access to the application 120 should be granted. In this example, the system 100 provides authentication without the need for PINs or passwords (although PINs and passwords may be used in other implementations). Moreover, personal biometric information need not be stored in any local or remote storage database and is only stored on the user's own PDK (in one embodiment).

[0026] The credibility of the system 100 is ensured by the use of a PDK 102 that stores trusted information. The PDK 102 is a compact, portable uniquely identifiable wireless device typically carried by an individual. The PDK 102 stores digital information in a tamper-proof format that uniquely associates the PDK 102 with an individual. Example embodiments of PDKs are described in more detail in U.S. Patent Application No. 11/292,330, entitled "Personal Digital Key And Receiver/Decoder Circuit System And Method" filed on November 30, 2005; U.S. Patent Application No. 11/620,581 entitled "Wireless Network Synchronization Of Cells And Client Devices On A Network" filed on January 5, 2007; and U.S. Patent Application No. 11/620,577 entitled "Dynamic Real-Time Tiered Client Access" filed on January 5, 2007, the entire contents of which are all incorporated herein by reference.

[0027] The sensor 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone (i.e., within a microcell) of the sensor 108. The proximity zone can be, for example, several meters in radius and preferably can be adjusted dynamically by the sensor 108. Thus, in contrast to many conventional RF ID devices, the sensor 108 can detect and communicate with the PDK 102 without requiring the owner to remove the PDK 102 from his/her pocket, wallet, purse, etc. Generally, the sensor 108 receives uniquely identifying information from the PDK 102 and initiates an authentication process for the individual carrying the PDK 102. In one embodiment, the sensor 108 is adapted to receive a biometric input 104 from the individual. The biometric input 104 comprises a representation of physical or behavioral characteristics unique to the individual. For example, the biometric input 104 can include a fingerprint, a palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample or any other biometric information such as DNA, RNA or their derivatives that can uniquely identify the individual. The sensor 108 compares the biometric input 104 to

information received from the PDK 102 to determine authentication. Alternatively, the biometric input 104 can be obtained by a biometric sensor on the PDK 102 and transmitted to the sensor 108 for authentication. In additional alternative embodiment, some or all of the authentication process can be performed by the PDK 102 instead of the sensor 108.

[0028] In this example, the sensor 108 is further communicatively coupled to the network 110 in order to receive and/or transmit information to remote databases for remote authentication. In an alternative embodiment, the sensor 108 includes a non-volatile data storage that can be synchronized with one or more remote databases or registries. Such an embodiment alleviates the need for a continuous connection to the network 110 and allows the sensor 108 to operate in a standalone mode and for the local data storage to be updated when a connection is available. For example, a standalone sensor 108 can periodically download updated registry entries and perform authentication locally without any remote lookup.

[0029] In yet another alternative, a standalone sensor 108 may have a pre-configured secure access key 118 and encryption algorithm, or a variable access key 118 that changes, for example based on time and sensor ID. One example application would be a sensor 108 located in a hotel room door, where the sensor could constantly compute a different access key 118 based on time, and the PDK 102 could be associated with this key during the hotel registration process.

[0030] The network 110 provides communication between the sensor 108 and various validation databases and/or registries, in addition to the applications 120. In one embodiment, the network 110 uses standard communications technologies and/or protocols. Thus, the network 110 can include links using technologies such as Ethernet, 802.11, 802.16, integrated

services digital network (ISDN), digital subscriber line (DSL), asynchronous transfer mode (ATM), etc. Similarly, the networking protocols used on the network 110 can include the transmission control protocol/Internet protocol (TCP/IP), the hypertext transport protocol (HTTP), the simple mail transfer protocol (SMTP), the file transfer protocol (FTP), etc. The data exchanged over the network 110 can be represented using technologies and/or formats including the hypertext markup language (HTML), the extensible markup language (XML), etc. In addition, all or some of links can be encrypted using conventional encryption technologies such as the secure sockets layer (SSL), Secure HTTP and/or virtual private networks (VPNs). In another embodiment, the entities can use custom and/or dedicated data communications technologies instead of, or in addition to, the ones described above.

[0031] In one aspect, the sensor 108 may connect to a validation database that stores additional information that may be used for authorizing a transaction to be processed at the sensor. For example, in purchase transactions, the sensor 108 may interact with a credit card validation database that is separate from the merchant providing the sale. Alternatively, a different database may be used to validate different types of purchasing means such as a debit card, ATM card, or bank account number.

[0032] In another aspect, the sensor 108 may connect to various registries that store, among other items, PDK, notary, and/or sensor information. In one embodiment, a registry stores biometric or other types of information in an encoded format that can only be recovered using an algorithm or encoding key stored in the PDK. Information stored in the registries can be accessed by the sensor 108 via the network 110 for use in the authentication process. Two basic types of registries are private registries and a Central Registry. Private registries are generally established and administered by their controlling entities (e.g., a merchant, business

authority, or other entity administering authentication). Private registries can be custom configured to meet the specialized and independent needs of each controlling entity. A Central Registry is a highly-secured, centrally-located database administered by a trusted third-party organization. In one embodiment, all PDKs 102 are registered with the Central Registry and may be optionally registered with one or more selected private registries. In alternative embodiments, a different number or different types of registries may be coupled to the network 110.

[0033] The service blocks 112 can be used for purposes other than user authentication. For example, information used or produced by an application 120 can be transferred back and forth to the corresponding service block 112. That is, each service block 112 can be used as a local secure memory for the corresponding application 120. Thus, a service 120B may store certain sensitive information in service block 112B, and a separate service 120C will not be able to access that information without the corresponding access key 118B. In this example, the sensor 108 only holds access keys 118A, D, F and does not hold access key 118B. The application 120B may hold the access key 118B, thus allowing it to access service block 112B but preventing application 120C from accessing the service block 112B. Note that this implementation would also prevent the sensor 108 acting alone from accessing the service block 112B.

[0034] Turning now to FIG. 2, an example embodiment of a PDK 102 is illustrated. The PDK 102 comprises a memory 210, control logic 250, wireless application 260 and a transceiver 270. The PDK 102 can be standalone as a portable, physical device or can be integrated into commonly carried items. For example, a PDK 102 can be integrated into a portable electronic device such as a cell phone, Personal Digital Assistant (PDA), or GPS unit, an employee

identification tag, clothing, or jewelry items such as watches, rings, necklaces or bracelets. In one embodiment, the PDK 102 can be, for example, about the size of a Subscriber Identity Module (SIM) card and be as small as a square inch in area or less. In another embodiment, the PDK 102 can be easily contained in a pocket, on a keychain, or in a wallet. The PDK can also contain other components not shown, for example various other inputs, outputs and/or interfaces (serial or parallel).

[0035] The memory 210 can be a read-only memory, a once-programmable memory, a read/write memory or any combination of memory types, including physical access secured and tamperproof memories. The memory 210 typically stores a unique PDK ID 212. The PDK ID 212 comprises a public section and a private section of information, each of which can be used for identification and authentication. In one embodiment, the PDK ID 212 is stored in a read-only format that cannot be changed subsequent to manufacture. The PDK ID 212 is used as an identifying feature of a PDK 102 and distinguishes between PDKs 102 in private or Central registry entries. In an alternative embodiment, the registries can identify a PDK 102 by a different ID than the PDK ID 212 stored in the PDK 102, or may use both the PDK ID 212 and the different ID in conjunction. The PDK ID 212 can also be used in basic PDK authentication to ensure that the PDK 102 is a valid device.

[0036] The memory 210 also stores the various service blocks 112A-N. Whether a particular service block 112 is stored in volatile or non-volatile memory may be determined by the specific application. In one approach, the original issuer of the PDK defines how the internal memory 210 may be used for service blocks 112. In some cases, the issuer may choose to only allow their service blocks to be stored, in which case third party applications will not be able to store service blocks in memory 210. In other cases, the issuer may allow any third party service

120 to use available service blocks 112. If a new service block is created, then memory for that service block is allocated. The specific location of the service block and generation of the corresponding service block access key can be handled by the PDK 102, or can be handled via an external service.

[0037] Regardless of how created, once created, external applications (such as applications 120 in FIG. 1) can gain access to a specific service block 112 by proving the corresponding access key 118. In FIG. 2, this is shown conceptually by control logic 250. The wireless application 260 on the PDK 102 communicates to the sensor (not shown in FIG. 2) via transceiver 270. The wireless application provides a service block select 226 and a service block access key 118 in order to store, retrieve and/or modify data in a service block 112. The selector 252 selects a service block 112 based on the select signal 226 and the access key 118. The encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key). In an alternate method, the service block 112 may be selected based on the service block access key 118, eliminating the need for a separate select signal 226.

[0038] The PDK 102 may also include other data and applications. For example, the PDK 102 typically will include various profiles. Many different types of profiles are possible. A biometric profile, for example, includes profile data representing physical and/or behavioral information that can uniquely identify the PDK owner. A PDK 102 can store multiple biometric profiles, each comprising a different type of biometric information. The same biometric information can also be stored multiple times in a PDK 102. For example, two different applications may use the right index fingerprint, and that biometric information may be stored in two different service blocks, one for each application. In addition, the PDK 102 may also store

one or more biometric profile "samples" associated with each biometric profile. Profiles may also store one or more PINs or passwords associated with the PDK owner, or one or more pictures of the PDK owner. A profile can further include personal identification information such as name, address, phone number, etc., bank information, credit/debit card information, or membership information. This information can be useful for transactions.

[0039] The transceiver 270 is a wireless transmitter and receiver for wirelessly communicating with a sensor 108 or other wireless device. The transceiver 270 can send and receive data as modulated electromagnetic signals. Moreover, the data can be encrypted by the transceiver 270 and transmitted over a secure link. Further, the transceiver 270 can actively send connection requests, or can passively detect connection requests from another wireless source. In one embodiment, the transceiver 270 is adapted to communicate over a range of up to around 5 meters. In another embodiment, the transceiver 270 range can be varied.

[0040] Turning now to FIG. 3, an example embodiment of a sensor 108 is illustrated. The embodiment includes one or more biometric readers 302, a receiver-decoder circuit (RDC) 304, a processor 306, a network interface 308 and an I/O port 312. In alternative embodiments, different or additional modules can be included in the sensor 108.

[0041] The RDC 304 provides the wireless interface to the PDK 102. Generally, the RDC 304 wirelessly receives data from the PDK 102 in an encrypted format and decodes the encrypted data for processing by the processor 306. An example embodiment of an RDC is described in U.S. Patent Application No. 11/292,330 entitled "Personal Digital Key And Receiver/Decoder Circuit System And Method," the entire contents of which are incorporated herein by reference. Encrypting data transmitted between the PDK 102 and sensor 108

minimizes the possibility of eavesdropping or other fraudulent activity. In one embodiment, the RDC 304 is also configured to transmit and receive certain types of information in an unencrypted, or public, format.

[0042] The biometric reader 302 receives and processes the biometric input 104 from an individual. In one embodiment, the biometric reader 302 is a fingerprint scanner. Other embodiments of biometric readers 302 include retinal scanners, iris scanners, facial scanner, palm scanners, DNA/RNA analyzers, signature analyzers, cameras, microphones, and voice analyzers. Furthermore, the sensor 108 can include multiple biometric readers 302 of different types.

[0043] The network interface 308 can be a wired or wireless communication link between the sensor 108 and network 110. For example, in one type of authentication, information is received from the PDK 102 at the RDC 304, processed by the processor 306, and transmitted to external authentication databases through the network interface 308. The network interface 308 can also receive data sent through the network 110 for local processing by the sensor 108. In one embodiment, the network interface 308 provides a connection to a remote system administrator to configure the sensor 108 according to various control settings.

[0044] The I/O port 312 provides a general input and output interface to the sensor 108. The I/O port 312 may be coupled to any variety of input devices to receive inputs such as a numerical or alphabetic input from a keypad, control settings, menu selections, confirmations, and so on. Outputs can include, for example, status LEDs, an LCD, or other display that provides instructions, menus or control options to a user.

[0045] FIGS. 4-6 are high level block diagrams illustrating additional examples of applications accessing service blocks. FIGS. 4 and 5 illustrate that the application 120 need not be located at any particular location on the network. Rather, the service block 112 is accessed from any application 120 that can attach (in a network sense) to the sensor 108.

[0046] In FIG. 4, the sensor 108 attaches to the PDK 102 within its microcell, using service block access key 118(A) and service block 112(A). A personal computer or other standalone device 510 is attached to the sensor 108, either directly or via a network. In this example, the device 510 communicates with the sensor via a standardized API 520. An application 120 executes on the device 510 and has access to the service block access key 118(B). It uses this key to gain access to the corresponding service block 112(B). This is an example of a local application 120.

[0047] FIG. 5 illustrates a remote application. In this example, the sensor 108 attaches to the PDK 102 in the same manner as FIG. 4, using service block access key 118A and service block 112A. However, application 120 is not executing on a local device. Rather, it executes remotely. Here, it is shown as an external service 120. However, service 120 can still gain access to service block 112B by use of service block access key 118B, although it does so via network 110 and intermediate device 512. Although the sensor 108 is the device that attaches to the PDK 102, a local or remote application 120 with the right credentials may store or retrieve information in a service block 112 in the PDK 102.

[0048] The PDK itself can also be configured to prevent the same source from repeating invalid access attempts to the PDK's service blocks. The PDK may monitor access to the service blocks. When an attached service makes multiple unsuccessful attempts to unlock a service

block, the PDK tracks this and eventually ignores the requests from that service for a period of time. Alternately, the PDK may disconnect from the network or take other actions.

[0049] An example of a local application (FIG. 4) is an auto login/logoff of a personal computer. When a PDK 102 is within the proximity of the personal computer 510, the PDK 102 is detected and the sensor 108 attaches to the PDK 102 (using service block 112A). The login/logoff application 120 then sends the service block access key 118B along with a request for the contents of the service block 112B to the PDK 102 via the sensor 108. For example, a standard may specify that particular service block 112B contains username and password. These are returned to the application 120, allowing automatic login to the personal computer 510.

[0050] An example of a remote application (FIG. 5) is a credit card transaction. The sensor 108 in this case could be a credit card terminal. When the PDK 102 is brought in close proximity, the credit card terminal 108 attaches to the PDK 102 (using service block 112A). The terminal 108 then sends the PDK ID 212 to the credit card issuer (the external service) for identification. The credit card issuer may then send a service block access key 118B back to the sensor 108, where it is passed on to the PDK 102 to unlock a specific service block 112B. The contents of the service block 112B could then be sent back to the credit card issuer where further decryption could occur and the credit card holder could be verified. Once verified, the credit card terminal displays that the transaction is approved.

[0051] These two examples illustrate basic concepts of the capabilities of the service blocks and how an application (service) may use them. Since service blocks preferably are both readable and writable, services may use them as they see fit (i.e. debit, username/password,

credit card information, etc.). In some sense, the service block acts as a secure local memory on the PDK.

[0052] FIGS. 4 and 5 illustrate a basic case where a single application accesses a single service block on a single PDK via a single sensor. The invention is not limited to this case. FIG. 6 illustrates a case with multiple applications, sensors, and service blocks. This illustrates the sharing of service blocks. As shown, service blocks may be limited to a single service or source or may be shared across multiple services and sources. A service block 112 is a protected memory element which allows an application 120 with the right credentials to access it. In this example, applications 120W, 120X and 120Y1 can each access service block 112C since each application has access to service block access key 118C. Similarly, applications 120V, 120Z2 and 120Z3 can each access service block 112B. Although not shown in FIG. 6, it is also possible for an application to access more than one service block. FIG. 6 also shows a situation where applications 120Z1-3 running on different devices 510Z1-3 all access the PDK 102 through the same sensor 108Z. Each sensor 108 covers a certain proximity zone (i.e., microcell). The presence of the PDK 102 within a microcell indicates proximity of the PDK to that particular sensor.

[0053] Also shown is a device 510Y with two applications 120Y1 and 120Y2, each of which accesses a different service block. In some cases, the first application 120Y1 is enabled from a first service block 112C, thus allowing a second application 120Y2 to operate using a second service block 112F (although the two applications need not be on the same device 510). For example, the first application 120Y1 might be the auto login/logoff, where a user logs in to a personal computer via a service block 112C that provides a username and password. Now that the user is logged in, the user wishes to attach to his credit card company. The user types in the

web address of the credit card provider, where the credit card provider requests the user's credentials. First, the user may have to provide some live biometric information. Application 120Y2 compares this against a biometric stored in a second service block 112F on the PDK. After the sensor108Y verifies the correct biometrics, the sensor indicates to the PDK that external services may now access their service blocks. The credit card provider 120Z1 then sends its service block access key 118A to the PDK where this third service block 112A is retrieved and sent back to the credit card issuer. The credit card issuer then verifies the data and authorizes the user's transaction.

[0054] Furthermore, although the above scenarios focus mostly on service blocks in the PDK, applications may also use the basic authentication function that allows the PDK and sensor to verify each other. In this scenario, once the sensor and PDK finish their verification the application is signaled. The application may then use this information as an assurance that the PDK is a legitimate device (but not necessarily that the holder of the device is legitimate).

[0055] In certain cases, access to a service block 112 may allow the application 120 to access various input/outputs on the PDK. For example, the PDK may have several inputs and/or outputs, as well as a serial (or other) interface. The inputs may be either transition triggered or level triggered. An example of a transition triggered event might be a button press, where level triggered might be turning a switch on. Multiple outputs may also exist where they may also be pulsed or level outputs. Finally an interface may allow attachment of an external device, which may then send data through the PDK to the application. In many cases, the inputs and outputs may be simple push button switches and LEDs used to allow a user to interact with an application.

[0056] Since the number of applications is limitless, different applications may use the inputs and outputs for different functionality. For example, a user walking into a casino may require attention from a service representative and if the casino has enabled button 1 for this functionality, when the user depresses button 1, an attendant is alerted with information related to the user and the location of the user. In a different application, an actual button may not exist, but it may be tied to an output of another device indicating when a piece of equipment was in use. Whenever the device was in use, the PDK transmits the input 1 active alert back to the backend application. The backend application may then be using this information to determine when the equipment must be recalibrated based on its usage.

[0057] This is also true for outputs and any interfaces. Outputs may be used to turn on a light or sound an audible tone used to locate an asset in a building. For example, there may be 20 pieces of equipment in a room which all show up using a location tracking program, but the user would then have to sift through each piece of equipment until the right one is located. Using an output as described above, a light could be lit and the equipment could be immediately located within the room. The interface allows another attached application to the PDK to send information to an end application attached to the sensor. In this case the sensor provides a medium to push data to an external source.

[0058] FIG. 7 is a high level block diagram illustrating one embodiment of a system with networked sensors. In this example, multiple sensors (marked "S") are attached to a Sensor Management Module (SMM) 730. The SMM 730 provides data routing for the sensors (e.g., to and from applications 720A-E). In this example, the SMM 730 also receives data from the sensors and processes this data to provide location tracking of PDKs (marked "P") that are within the sensor field. In this implementation, the system also includes an application layer

message bus 740, over which the SMM 730 and applications 720 can exchange messages. This allows multiple applications 720 to simultaneously communicate with PDKs and make use of the location tracking of the PDKs. The application layer message bus 740 may also be extended to other applications via a remote application interface.

[0059] In FIG. 7, each sensor's microcell (i.e., proximity zone) is denoted by a circle around the sensor. Similarly, the PDK's range is shown by the heavy larger circle. In the example shown, the PDK is in range of four different sensor zones and any of the four sensors may establish communications to the PDK. Using a network topology as shown, the SMM may instruct a specific sensor to attach to the PDK. Once established, the communication link will allow the PDK to communicate with various applications 720, in this example via the SMM 730 and bus 740. Applications 720 will be able to access service blocks on the PDK through the use of service block access keys, as described above.

[0060] In addition, in this example, the sensors are at known locations, preferably at fixed locations. For example, sensors may be distributed throughout a building or other structure or site (including outdoors). The sensors interact with the PDK in a manner that allows the sensors to gather position data about the PDK. This position data is sent by the sensors to the SMM 730, which processes the data to determine the PDK's position and to provide location tracking of the PDK over time. The position and/or location tracking information can then be made available to applications 720 via bus 740, in addition to allowing the applications 720 to communicate with the PDK.

[0061] Location tracking of the PDK by the sensor network can be achieved in different ways, one of which will be described below. The example in FIG. 7 uses a coordination module

(marked "C") or simply coordinator, although this is not required in other implementations. The large dashed circle shows the coordinator's cell. In this example, the sensors preferably contain two transceivers, one to communicate with the coordinator on what will be referred to as the control channel and another to communicate with the PDK on what will be referred to as the traffic channel.

[0062] FIG. 8 illustrates operation of the system in FIG. 7. The coordinator C broadcasts 810 a periodic beacon on a control channel. The sensors and PDKs synchronize to this periodic beacon. On the control channel, when a sensor is not receiving the broadcasted beacon, it is timesharing between listening for a PDK ALOHA response and possibly sending a command to a specific PDK. The PDK, after detecting the beacon, remains on the control channel and continues to periodically wake up, receive the beacon, and realign its timing. By using system related information found in the beacon and its own serial number, the PDK calculates the wakeup time to synchronize to the beacon and broadcast 820 an ALOHA response. As shown, the PDK's broadcasted ALOHA response may overlap several sensors causing multiple sensors to receive the information simultaneously. Each sensor that receives an ALOHA response from a PDK performs a store and forward 830 of the responses to the SMM 730 on a periodic basis.

[0063] The coordinator and sensors communicate to the SMM 730 via a backend network. This communications method used to attach each device to the SMM may be wired or wireless provided it has the bandwidth required to transport the information between the devices. When a PDK ALOHA response is detected by a sensor, the sensor collects information such as the PDK ID, receiver signal strength indication, and timestamp. After receiving this information from the sensors, the SMM independently applies the new information for each PDK from the sensors, to the previous history of that PDK and through location deterministic algorithms

computes the most likely sensor microcell in which the PDK is located. There are multiple known algorithms for doing so. In one approach, location (proximity) is determined based on prior location history, time at the current location, RF signal strength and geographic contours. The SMM may also store the raw data for further alternate processing methods or for diagnostic purposes.

[0064] The SMM 730 can broadcast this information on the application layer messaging bus 740 for applications 720 to use. For example, one application 720A might be a location tracking application with a graphical user interface that shows the current position or trail of the PDK. The SMM 730 (or applications 720) may also store the location information and make it available on an on-demand basis.

[0065] In this particular example, access is allocated using a time division multiple access (TMDA) system, where an RF logical channel is distributed over time and each device has a specific period known as a timeslot in which they are allowed to respond. Each timeslot has a preamble and timeslot synchronization character followed by a packet, and lastly a guard period. The content of each packet is dependent on the source device, channel type (control or traffic), and timeslot location.

[0066] For example, the coordinator broadcasts the beacon on a period basis. All sensors and PDKs receive the beacon. Each PDK then broadcasts its ALOHA response at a specific timeslot allocated for that purpose. In addition to the handshake messages that occur on the control channel, the beacon and ALOHA response may also carry auxiliary data. This data may be in the form of an alarm indication, command/status, or user/application data, for example. It could be provided by an end application, SMM network command, external device interface

(such as a terminal interface), or via an internal alarm functions such as low battery, input signal change, or setting an output signal polarity.

[0067] After an ALOHA response is broadcast from a PDK, the PDK listens for a command from nearby sensors. Based on the type of PDK and time it is present in one geographical location, one or more nearby sensors that detected the ALOHA response, may also send additional paging or auxiliary data in the sensor command response timeslot for a specific PDK.

[0068] Other timeslots can be allocated to traffic channels and/or to other messages over the control channel. Various TDMA approaches can be used to allocate the wireless communications channel. Non-TDMA approaches can also be used.

[0069] The sensor network system of FIG. 7 provides a closed loop system. With the SMM 730 being the central hub, broadcasting auxiliary data through the coordinator (and sometimes sensor devices) and collecting PDK auxiliary data through the sensors, it is possible to determine if in an asymmetrical system a command was successfully completed.

[0070] FIG. 9 illustrates an example of how the closed loop system works. In step 910, the SMM 730 (via the coordinator) broadcasts a beacon that also contains auxiliary information. This auxiliary information contains a command from an application 720 to be executed by the PDK. Assume that, for this particular command, the PDK is expected to acknowledge execution of the command. After the PDK executes the command, the PDK sends 920 the acknowledge message as auxiliary data in one of the PDK's ALOHA responses. The sensor receives the ALOHA response and passes 930 the information back to the SMM 730. The SMM 730 has now verified that the command was successfully executed. Such commands could be as simple

as set an output to turn on a light or generate an audible sound. It is also possible that an application 720 attached to the SMM 730 may request to pass data to the specific PDK where that data may then be passed to an external terminal application where the system acts only as a transport mechanism. In this mode, the applications attached at each end would be responsible for verifying and acknowledging the data was sent and received successfully.

[0071] A second example is shown in FIG. 10, where the PDK initiates an alert. The coordinator periodically transmits a beacon and the PDK periodically returns an ALOHA response. In the example, a user carrying a PDK is located within a service oriented business, such as a department store, casino, restaurant, etc. The user desires to talk with a service representative from the organization and depresses 1010 the service button on their PDK (button 1). The next time the PDK wakes up to send an ALOHA response, the PDK attaches the button 1 alert to the ALOHA messages and broadcasts 1020A it. A local sensor receives the location response containing the button 1 alert and eventually sends 1020B the received ALOHA responses back to the SMM. The SMM may reformat the data and passes 1020C the indication back to the application. The application then indicates 1030 a button 1 request from the particular PDK serial number (and other related user information) on the application console. The PDK continues to send back the button 1 alert until cleared or a timeout period occurs. This allows devices that have inadequate coverage (e.g., on the edge of a cell boundary) to continue to send the alert until detected.

[0072] Eventually the console operator becomes aware of the service request and dispatches a representative to the user and clears 1040 the button1 alert on the console. The clear button 1 alert is then sent 1050A-B to the coordinator where it is queued to go out 1050C on the proper beacon when the PDK will be awake. Once the PDK wakes up and receives 1050C its

next beacon, the PDK clears out 1060 the button 1 alert indicator and returns to a basic ALOHA state with no auxiliary data pending.

[0073] The example shown may have also had a visible indicator in the PDK where the visible indicator may have become lit when the button was depressed. Once the button 1 alert was cleared the indicator would be unlit.

[0074] In this example, neither the application nor SMM verified the PDK actually received the clear button 1 alert. In one approach, each auxiliary message (page, alert, etc.) sent by a device contains a sequence number. If a device continues to send the information after it is acknowledged or cleared, the device is aware of the condition because of the sequence number. Any time a new auxiliary message is sent, the sequence number is incremented to alleviate the confusion as to how new or old any message is.

[0075] For some systems, redundancy is important. Redundancy can be implemented in the example system of FIG. 7 in a number of ways. For example, it is possible to provide multiple coordinators where these coordinators can be used to extend a coverage area or as a redundant backup. In one approach, each coordinator broadcasts its beacon on the same RF channel with a slight timing offset from the other coordinators. This creates a simulcast system where if one coordinator fails, the second coordinator can still resume system operation. This may also counter the issues of multipath by providing spatial diversity with the coordinators. Another redundancy measure is that information can be sent to PDK via the sensors, in addition to or in place of the coordinator. Another example of redundancy is that multiple sensor may receive messages from the PDK so there may be multiple paths back to the SMM via different sensors.

[0076] Referring now to FIG. 11, one embodiment of a hybrid device 1102 in accordance with the present invention will be described. The hybrid device 1102 comprises a PDK 102a and an RDC 304a. Depending on the embodiment, the hybrid device 1102 utilizes the PDK functionality, the RDC functionality or both the PDK functionality and the RDC functionality. Those skilled in the art will recognize that in other embodiments, the hybrid device 1102 has multiple instances of PDK functionality or multiple instances of the RDC functionality or multiple instances of both. As illustrated in FIG. 11, the PDK 102a is coupled by signal line 1104 to the RDC 304a. This direct coupling allows the PDK 102a and the RDC 204a to communicate control signals and data for various applications will be described below. The signal line 1104 is also used to provide power to the PDK 102a via the RDC 304a in configurations where the RDC 204a is coupled to a power source via signal line 1106. In this embodiment, the RDC 304a is also coupled to signal line 1106 for communication with other devices (not shown). The signal line 1106 can be used to send and receive control signals and data as well as to receive power. Thus, in certain embodiments, the hybrid device 1102 need not have its own independent power source. Moreover, in other embodiments not shown, signal line 1106 is coupled directly to the PDK 102a to provide power.

[0077] In one embodiment, the PDK 102a is similar to the PDK 102 described above with reference to FIG. 2 and includes the same functionality as described above. Those skilled in the art will recognize that in other embodiments, the PDK 102a includes less functionality than that described above with reference to FIG 2. In a minimal embodiment, the PDK 102a includes an antenna and a transceiver for communicating with a RDC (not shown) and a controller and memory for storing information particular to a user. In yet other embodiments, the PDK 102a includes functionality beyond that described above with reference to FIG. 2. The PDK 102a

implements the PDK functionality as will be described below with reference to FIGS. 11-16 using a processor and memory of the PDK 102a.

[0078] For simplicity and ease of understanding, the hybrid device 1102 is shown as including an RDC 304a. In one embodiment, the RDC 304a is similar to that described above with reference to FIG. 3 above. In another embodiment, the RDC 304a represents and includes the functionality described above as being provided by the sensor 108. Those skilled in the art will recognize that the RDC 304a may have more or less functionality that described above with reference to FIG. 3 above. The RDC 304a implements RDC functionality as will be described below with reference to FIGS. 11-16 using a processor and memory of the RDC 304a. The RDC 304a is coupled to an antenna for communication with other PDKs 102 and coupled to signal line 1106 to send and receive data and control signals from other devices (not shown). In certain embodiments, signal line 1106 also provides power to the RDC 304a.

[0079] Referring now to FIG. 12, one embodiment a system 1200 of the present invention in which the hybrid device 1102 is part of a cell phone 1202 will be described. The system 1200 comprises a PDK 102b and the cell phone 1202. The cell phone 1202 further comprises cell phone components and a battery 1204 and the hybrid device 1102. As described above with reference to FIG. 11, the hybrid device 1102 includes PDK 102a and RDC 304a coupled for communication with each other via signal line 1104. In this embodiment, the cell phone components and a battery 2004 are coupled to the RDC 304a by signal line 1106. This allows the RDC 304a to use the communication capabilities of the cell phone 1202 including the voice and data channels provided by conventional cell phone to communicate with other networks and devices (not shown). The RDC 304a and the PDK 102a are adapted to communicate wirelessly with other devices, such as the PDK 102b. While FIG. 12 shows the

hybrid device 1102 as including both the RDC 304a and the PDK 102a, in another embodiment the hybrid device 1102 includes only the RDC 304a.

[0080] In one embodiment, the cell phone 1202 including the hybrid device 1102 collectively forms a secure cell phone or a generic access point. In such an embodiment, the hybrid device 1102 has a form factor similar to that of a conventional SIM card for cell phones. This is particularly advantageous because the hybrid device 1102 can be used with a variety of existing cell phones without any modification and the hybrid device 1102 is merely inserted in place of a conventional SIM card to provide this functionality. The conventional SIM card is replaced with the hybrid device 1102 that provided the RDC functionality. In other words, the hybrid device 1102 provides authorization control as well as a storage area for storing information specific to a user. The SIM content (Cell phone account, contact information, and credit card information) that is normally stored in the cell phone 1202 is instead stored in the PDK 102b carried by the user. In one embodiment, the PDK 102b stores the original SIM content in its local memory. For example, the PDK 102b defines a SIM slot 1208 to receive the original SIM card 1206, communicatively couples to the SIM card 1206 and copies the information from the SIM card 1206, effectively giving the original SIM card 1206 a wireless extension.

[0081] Such a configuration is particularly advantageous for a number of reasons. First, the cell phone 1202 is rendered useless (except 911) if the PDK 102b is out of range of the RDC 304a of the hybrid device 1102. Second, the local phone content such as calendar, contacts, etc. is protected because it resides on the PDK 102b, and is secure and not accessible by the cell phone 1202, its hybrid device 1102 or its RDC 304a without the PDK 102b. Third, the RDC function provided by the RDC 304a of the hybrid device 1102 in the cell phone 1202 becomes a

generic access point and allows any PDK 102, not just the PDK 102b, to access it. Thus, any user that has an account with a specific service provider may "bond" or "link" their PDK 102 to the cell phone 1202, allowing their account to be charged for any services rendered. Both the bonding process and service access may be performed via the keypad, voice activated, or via bio-functions of the cell phone 1202. Fourth, any PDK 102 may store and provide contract based account information (such as a cell phone account), or may provide credit information (such as a credit or debit card) that is billed for the service. This allows any person that carries a PDK 102 with credit card information store thereon to use their credit card to gain wireless voice and data services without signing a long term contract. Fifth, since the content is carried on the PDK 102, any type of cell phone may be used. The PDK 102 provides active updates to its internal contents allowing for "last call received" or "last number dialed" to be saved. By bonding the PDK 102 to another phone and hitting redial, the last number that was dialed from any other phone associated with the PDK, is now redialed. There is no need to transfer information from phone to phone or to have back up contact information stored on a personal computer. In an alternate embodiment, the contents (including last number dialed) are stored at the service provider (or in a user defined path – i.e. personal website, etc.) and become available on the cell phone 1202 when the PDK 102 "bonds" to the phone 1202. The referenced account is obtained and the data is transferred to that phone in volatile memory using the network of the service provider to which the cell phone 1202 is coupled. Moreover, the PDK "phone" contents may also be synchronized to a personal computer application via an RDC attached to the personal computer. The phone does not have to be present, only the PDK with a correct password or entry method (bio, etc). The above application/configuration makes cell phones generic allowing any subscriber carrying a PDK 102 with either a cell phone account or credit account to acquire

any phone and start using it. Since the user's information stays with the user, it is possible the user could span across multiple cell phone providers in different countries and still maintain a single virtual cell phone account.

[0082] In another embodiment, the hybrid device 1102 contains a copy of the contents of SIM card 1206 information. In this embodiment, the contents that are stored in hybrid device 1102 may only be accessible if PDK102b is within proximity of the Cell Phone 1202. In this embodiment, SIM card 1206 is not required to be present in the PDK 102b.

[0083] In a variation to the embodiment described above with reference to FIG. 12, a second embodiment of the system 1200 does not include the PDK 102b. Instead the functionality described above with reference to the PDK 102b is provided by the PDK 102a that is part of the hybrid device 1102. The hybrid device 1102 uses the PDK function provided by PDK 102a. The hybrid device 1102 is coupled to the cell phone 1202, in particular the cell phone components and battery 1204, via internal integration or an access port. Such a configuration is particularly advantageous because the PDK function then becomes part of the cell phone 1202 using battery power from the cell phone 1202 and providing the same type of access as described above. Moreover, PDK 102a can provide access control passwords etc. for any type of functions enabled by the phone such as but not limited to gaming, personal computer access, e-commerce, etc. Additionally, the PDK enabled phone uses the back channel to perform other validation / update functions via the cellular infrastructure.

[0084] In a variation to the embodiment described above with reference to FIG. 12, the hybrid device 1102 includes and uses both the RDC 304a and the PDK 102a. This adds the hybrid functionality of being capable of performing both simultaneous RDC and PDK functions

to the cell phone 1202. The hybrid functionality extends the type of offerings and functionality by allowing the cell phone 1202 to perform the functionality described above as well as additional functionality described below with reference to FIGS. 13-16.

[0085] Referring now to FIGS. 13-16, the hybrid functionality provided by the hybrid device 1102 will be described in more detail. The hybrid device 1102 allows for many different configurations and operations of the secure PDK/RDC protocol. The hybrid device 1102 allows mixed operations including: RDC/PDK, RDC/RDC or PDK/PDK combinations. For purposes of explanation below, each device is enabled with either or both RDC and PDK functionality.

[0086] FIG. 13 is a block diagram of one embodiment of a system 1300 simultaneously using the PDK and the RDC functionality of the hybrid device 1102 in accordance with the present invention. FIG. 13 shows the system 1300 comprising a hybrid device 1102 having a first PDK 102a and a first RDC 304a, a second PDK 102b, and a second RDC 304b. In this configuration of the system 1300, the hybrid device 1102 maintains two separate simultaneous links: a first link 1302 between the second PDK 102b and the first RDC 304a of the hybrid device 1102; and a second link 1304 between the first PDK 102a of the hybrid device 1102 and the second RDC 304b. In this system 1300, the second PDK 102b, possibly carried by a user, enables the first RDC 304a of the hybrid device 1102. The hybrid device 1102 in turn with its first PDK 102a enables the second RDC 304b, for example being associated with a third component such as endpoint RDC function.

[0087] In one embodiment, each link 1302, 1304 of the system 1300 provides an independent authorization. In FIG. 13, the hybrid device 1102 provides authorization to the second RDC 304b. The hybrid device 1102 carries credentials (credit card, account information,

etc.) that are used to enable a service associated with the second RDC 304b. For example, a cell phone includes the hybrid device 1102 and the hybrid device 1102 stores credit card information. A user makes a purchase using the cell phone as their credit source. The same user also carries the second PDK 102b. The second PDK 102b provides authorization to the hybrid device 1102 to enable specific functionality (charging using of the credit card information) provided by the hybrid device 1102. In other words, the second PDK 102b is used to enable specific features in the hybrid device 1102. The second PDK 102b carries the user's cellular service account information that is used to enable specific cellular services. If the second PDK 102b is no longer present, those services are disabled. Each the authorizations, credit card and cell service, is independent of the other.

[0088] In another embodiment, the links 1302, 1304 of the system 1300 provide a daisy chained authorization. In FIG. 13, the second PDK 102b authorizes the hybrid device 1102 which in turn authorizes the second RDC 304b. It is mandatory for the second PDK 102b to have a connection to the hybrid device 1102 before the hybrid device 1102 can initiate a request for authorization from the second RDC device 304b. For example, a parent could give a child conditional charging privileges where the child may only charge if the parent is present. The child carries the hybrid device 1102 (possibly in a cell phone), and chooses to make a purchase in a local video store. That store has a specific account for the child that is linked to his/her PDK 102a of the hybrid device 1102. When the child walks up to the counter to make the purchase, he/she is identified by their personal ID (included on PDK 102a of the hybrid device 1102 and transmitted to the RDC 304b) and their account is opened. Since the parent is in the same vicinity, the hybrid device 1102 communicates with the parents PDK 120b and obtains authorization to charge to the parent's account. If the parent was not present, the child would still

be identified, but would not have charging privileges. In an alternate embodiment, the RDC 304a of the hybrid device 1102 allows different PDKs with different credentials to "bond" with it (i.e. Fathers, Mothers, guardian, adult sibling, etc.), any one of which could be used for authorization.

[0089] Referring now to FIG. 14, one embodiment of a system 1400 using the multiple links to the hybrid device 1102 to generate an authorization signal in accordance with the present invention will be described. More specifically, only when the hybrid device 1102 has multiple links 1402, 1404 will the hybrid device 1102 generate an authorization or enable signal on signal line 1406. In this embodiment, the hybrid device 1102 has a physical output or connection for providing the authorization signal. Any variety of different types of devices may be coupled to signal line 1406 to receive the authorization or enabling signal. Without receipt of such a signal, the associated devices (not shown) are not operable. As illustrated in FIG. 14, the hybrid device 1102 requires authorization from both the second RDC 304b and the second PDK 102b to enable functionality. As an example, the hybrid device 1102 is coupled to and secures a personal computer (not shown). For the personal computer to operate, it must authenticate with a specific RDC 304b or fixed equipment at a specific physical location. A user carrying a PDK 102b with the correct privileges must also be present to gain access to the computer. If either the RDC 304b or PDK 102b is not present, the hybrid device 1102 does not allow operation of the personal computer. This prevents theft and illegal use of the property.

[0090] Referring now to FIG. 15, one embodiment of a system 1500 that uses multiple PDK links 1502, 1504 to the hybrid device 1102 to generate an authorization signal is shown. For the system 1500, only when multiple PDK links 1502, 1504 to the hybrid device 1102 exist, will an authorization/enablement signal be generated on signal line 1506. Again, in this

embodiment, the hybrid device 1102 has a physical output or connection for providing the authorization signal. The system 1500 comprises the hybrid device 1102 and a plurality of PDKs 102a-102 n. Although only two PDKs are shown in FIG. 15, those skilled in the art will recognize that the system 1500 may be configured to include any number of PDKs greater than two. As shown in FIG. 15, the hybrid device 1102 requires authorization (e.g., that a link be established) from multiple PDKs 102b, 102n in order to enable functionality. As an example, the hybrid device 1102 is coupled to control an electronic lock for a safety deposit box. The office manager and the customer each with respective PDKs 102b, 102n need to be present before the hybrid device 1102 generates an enable signal on signal line 1506 to unlock the safety deposit box and allow access to it.

[0091] Referring now to FIG. 16, one embodiment of a system 1600 using the hybrid device 1102b for authorization inheritance is shown. One particular advantage of using hybrid devices 102 is that they provide a mechanism for authorization inheritance within the system 1600. Authorization inheritance is when a first device passes selected information to a second device and the second device then "inherits" that information for use. The use of the information can be a one-time use during the presence of the first device, multiple uses with or without the presence of the first device or permanent use. Furthermore, there are multiple types of inheritance including service inheritance, feature inheritance and personality inheritance. Service inheritance is authorization of the second device for any functionality provided by a given service. Feature inheritance is similar to service inheritance but for a limited set of features offered by a given service. Personality inheritance is where the preferences of a user or holder of a first device are shared with a user or holder of a second device.

[0092] These inheritance concepts and the operation of the hybrid device 1102b will now be described in the specific context of system 1600 shown in FIG. 16 as including a PDK 102b operating as the first device, the hybrid device 1102b operating as the second device and the RDC 304b operating as the third device. The system 1600 illustrates a hybrid device 1102b with simultaneous PDK and RDC functionality to provide inheritance. In this context, the inheritance promulgates the authorization or features from the first device to the second device and onto the third device. However, those skilled in art will recognize that in another embodiment, the first and second devices both communicate directly with the third device to perform the same function. For example, the PDK 102b and the hybrid device 1102b both directly communicate to the RDC 304b and both provide permissions to allow the RDC 304b to generate an authorization or access (without the PDK 102b going through the hybrid device 1102b).

[0093] As shown in FIG. 16, the PDK 102b is similar to the PDK 102 described above with reference to FIG.2 and includes like components and has similar functionality. The PDK 102b also includes service inheritance storage 1602, feature inheritance storage 1604 and personality inheritance storage 1606. The service inheritance storage 1602, feature inheritance storage 1604 and personality inheritance storage 1606 are used to store information that is provided from the PDK 102b, the first device, and inherited by the second device, the hybrid device 1102b. The PDK 102b is carried by a first user and the PDK 102b has multiple accounts on this first device. For example, the service inheritance information stored in service inheritance storage 1602 includes a first credit card account, a first cell phone account, Wi-Fi access information, and computer A access information. The feature inheritance storage 1604 and personality inheritance storage 1606 are used to store information used for feature and personality inheritance as will be described below. Those skilled in the art will recognize that in

another embodiment, the service inheritance storage 1602, the feature inheritance storage 1604 and the personality inheritance storage 1606 is a shared or unified memory space with the service inheritance storage 1602, the feature inheritance storage 1604 and the personality inheritance storage 1606 each being a set of references or pointers to the information in the shared or unified memory space. Those skilled the art will recognize that working memory of the PDK 102b may be used for storing the inheritance information, and that in another embodiment, the PDK 102b need not have service inheritance storage 1602, feature inheritance storage 1604 and personality inheritance storage 1606, but may have only one or two of them.

[0094] The hybrid device 1102b is similar to the hybrid device 1102 described above with reference to FIG. 11 and includes like components and has similar functionality. The hybrid device 1102b also includes service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616. The hybrid device 1102b is communicatively coupled to the service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616. The service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616 are also used to store inheritance information specific to the user of the hybrid device 1102b. The service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616 are used to store inheritance information received from PDKs, e.g., the PDK 102b. In one embodiment, the hybrid device 1102b is carried by a second user that has a different set of accounts than the user of the first device. For example, the service inheritance information stored in the service inheritance storage 1612 includes a second credit card account, a second cell account, no Wi-Fi access information, and computer B access information. Again, the service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616 are portions of working memory of the

hybrid device 1102b and the hybrid device 1102b need not have service inheritance storage 1612, feature inheritance storage 1614 and personality inheritance storage 1616, but may have only one or two of them.

[0095] In yet another embodiment, the RDC rather than the hybrid device 1102b collects and uses inherited information. For example, in a configuration where there are 2 PDKs, a first PDK and a second PDK, the first PDK links and communicates with an RDC. The first PDK then signals the RDC that inherited information is available from the second PDK. The RDC establish a link with the second PDK and gets the inherited information from the second PDK. This is particularly advantageous because it avoids having to send the inherited data through the hybrid PDK 1102b as shown in FIG. 16. It also allows inheritance to be performed without a hybrid PDK 1102.

[0096] The RDC 304b operates as the third device and is used to access or enable a Wi-Fi Service. In this embodiment, the RDC 304b receives inheritance information and uses it to enable or disable the services associate with the RDC 304b. While the RDC 304b does not store the inheritance information, in another embodiment it includes service inheritance storage, feature inheritance storage and personality inheritance storage for doing so.

[0097] An example method of using the system 1600 will now be described. Both a first user and a second user are at an airport. A Wi-Fi service is offered in the airport and has RDC 304b controlling access and use of the Wi-Fi service. The first user has and is in possession of the PDK 102b, and the second user has and is in possession of the hybrid device 1102b. The second user with the hybrid device 1102b wants to obtain Wi-Fi access to check email, but the second user doesn't have a Wi-Fi Access account. The first user having the PDK 102b allows

the second user to inherit the Wi-Fi access for a one time use. The PDK 102b provides this information to the RDC 304a of the hybrid device 1102b and the hybrid device 1102b stores the inherited information in its service inheritance storage 1612 for use as represented by line 1650. The hybrid device 1102b then communicates with the RDC 304b to access the Wi-Fi service using the first user's account as represented by line 1652. The hybrid device 1102b is able to access and receive the service using the first user's account which it inherited. Depending on the terms with which the information was inherited, the inherited information allows any number of accesses, access for a predetermined amount of time (e.g., for 30 minutes), a single access, or access up to a particular dollar amount of charges.

[0098] In another embodiment, the inheritance information is transferred prior to the service being available. For example, the first user is a parent with a debit card account that is associated with or stored in PDK 102b. A child or minor of the parent is associated or in possession of the hybrid device 1102b. The system 1600 allows the first user to transfer to their child, a specific dollar amount that the child could spend. In one embodiment, the money is transferred from PDK 102b to the hybrid device 1102b by transferring account information, a dollar amount and spending restrictions from the service inheritance storage 1602 of PDK 102b to the service inheritance storage 1612 of the hybrid device 1102b. In another embodiment, the actual transfer is done via a backend server (not shown) where the child's device 102b and the hybrid device 1102b are only referenced and the backend server actually carries the charge type and amount available. In yet another embodiment, attributes stored in the hybrid device 1102b and the backend server can be combined to determine the amount and charge types allowed.

[0099] The system 1600 is also used to provide feature inheritance. Feature inheritance is similar to service inheritance except feature inheritance is limited to a portion of a service. An

example of feature inheritance is where a parent, the first user having the PDK 102b, allows a child, the second user, to play a teen video game or access a specific website while the parent is present. The child is in possession of the hybrid device 1102b, and when in proximity, it enables the computer that has the RDC 304 controlling its use and access to the internet. When the parent is in the room or within proximity of the child, the hybrid device 1102b then acquires permission from the PDK 102b and is then able to pass additional attributes to the RDC 304 of the personal computer or video game that allow a different rating to be in place. When the parent and the PDK 102b leave the room, the child's hybrid device 1102b loses the privileges and the child must return to lower rated games and sites. Those skilled in the art will recognize how the system 1600 may be integrated as part of a DVD player to control what movies may be viewed. If a movie or other video has selective portions of content that are associated with different ratings, the portions of video content that are output depend on a PDK 102 and a hybrid device 1102b and their associated authorizations. This would allow a single DVD and DVD player to present one version of a movie to an adult viewer while providing a different version of a movie to a child. More specifically, violent or mature content would be removed from the version of the movie output by the DVD system when only the child's hybrid device 1102b is present.

[00100] The system 1600 is also used to provide personality inheritance. Personality inheritance is where the preferences of a user or holder of a first device are shared with a user or holder of a second device which are then be used to make informed decisions or provide guidance to the second device. For example, assume 2 children who are friends like to play video games. Let's assume that each child is associated with a hybrid device 1102b that accumulates information related to the purchases, rentals, and play of these games (i.e. the game

may have an RDC as well). Around Christmas, the 2 friends choose to exchange game related personality information -- hybrid device 1102 to hybrid device 1102. Now each friend knows what the other one has played, they type of games they like to play, and if a particular game was rented, purchased, played online, etc. Each friend can now go and purchase, using the information in their hybrid device 1102, a game that they want to give to the other friend for Christmas. In a second example, a work colleague has collected information on the internet related to a specific subject and wants to now share that information with a second colleague. Personality Inheritance can be done via accumulation in the hybrid device 1102, the PDK 102 or via a backend server or both.

[00101] The hybrid device 1102b is also particularly advantages for automatically disabling a service or feature. The concept of "service and/or feature disability" is to remove a capability when a device is within proximity of a zone. There are conditions where it is highly desirable to disable a function in a portable device. An example is cell phones in movie theatres, or phone cameras in an office building, etc. In these settings, it is possible that the present invention disables or changes the personality or feature set of a device based on the presence of the RDC 304. For example, in a theatre having an associated RDC, any phone that includes the hybrid device 1102 is placed into a vibrate mode, silent mode, or disabled. When the person leaves the theatre, the phone would return to its normal operation. Of course, the user may still need to have their PDK 102 to obtain service, but both of these features can work in conjunction with the other feature. In another example, when an outside vendor attends a meeting for a corporation, his/her cell phone camera is disabled and possibly his/her phone volume is lowered. There are features that can be controlled by the PDK 102, RDC 304 or the hybrid device 1102 located in a corporate office environment. In addition to the switching (or inhibiting) of features

when visiting a facility, these same types of attributes can change when any PDK 102, RDC 304 or hybrid device 1102 comes in to proximity of any other PDK 102, RDC 304 or hybrid device 1102. The above examples described how the functionality of a portable device changes depending upon the devices in its vicinity. In addition, the operational state of the fixed (or semi-portable) type of devices could change as well. For example, the parents are watching an R-rated movie and a pre-teen child walks in the room. The movie becomes immediately blocked (or paused) by the display device so that the pre-teen is protected against the content. In another example, an employee of a recreational facility carries an ID badge including a PDK 102. The recreational facility provides areas for access by customers only, not for employees during predefined hours. When an employee gets close to the entrance, their PDK 102 is recognized by the RDC controlling the door locks, and the employee is not permitted into the area.

[0101] Finally, the hybrid device 1102 has been described above as being capable of propagating information between the PDK 102 and the RDC 304. Those skilled in the art will recognize that in environments where there are a plurality of hybrid devices 1102, there are any number of communication paths that can be established between the plurality of hybrid devices 1102 by effectively creating a "daisy chain" of PDKs 102 an RDCs 304 to propagate information from one hybrid device 1102 to another. Such a network of hybrid devices 1102 provides the capability for complex decisions and/or capabilities. There can be any number of information and control transfers between devices having an associated hybrid device 102 such as but not limited to portable to portable, portable to fixed, fixed to fixed, and backend equipment. In such an environment, any device with an associated hybrid device 1102 is able to allow, remove, or alter, the features and capabilities of any other device having an associated hybrid device 102 given the proper authority.

[0102] Various other modifications, changes and variations which will be apparent to those skilled in the art may be made in the arrangement, operation and details of the method and apparatus of the present invention disclosed herein without departing from the spirit and scope of the invention as defined in the appended claims. Therefore, the scope of the invention should be determined by the appended claims and their legal equivalent.

CLAIMS

1. A hybrid device for use in a proximity system, the hybrid device comprising:

a personal digital key (PDK) for storing information and capable of communicating wirelessly, the PDK for linking with RDCs;

a receiver-decoder circuit (RDC) for linking with PDKs, the RDC capable of communicating wirelessly, the RDC coupled to the PDK by a first signal line, the RDC coupled to a second signal line for communicating and enabling an external device.

HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE

ABSTRACT OF THE DISCLOSURE

A hybrid device includes a personal digital key (PDK) and a receiver-decoder circuit (RDC). The PDK and RDC of the hybrid device are coupled for communication with each other. In one embodiment, the hybrid device also provides a physical interconnect for connecting to other devices to send and receive control signals and data, and receive power. The hybrid device operates in one of several modes including, PDK only, RDC only, or PDK and RDC. This allows a variety of system configurations for mixed operation including: PDK/RDC, RDC/RDC or PDK/PDK. The present invention also includes a number of system configurations for use of the hybrid device including: use of the hybrid device in a cell phone; simultaneous use of the PDK and the RDC functionality of hybrid device; use of multiple links of hybrid device to generate an authorization signal, use of multiple PDK links to the hybrid device to generate an authorization signal; and use of the hybrid device for authorization inheritance.

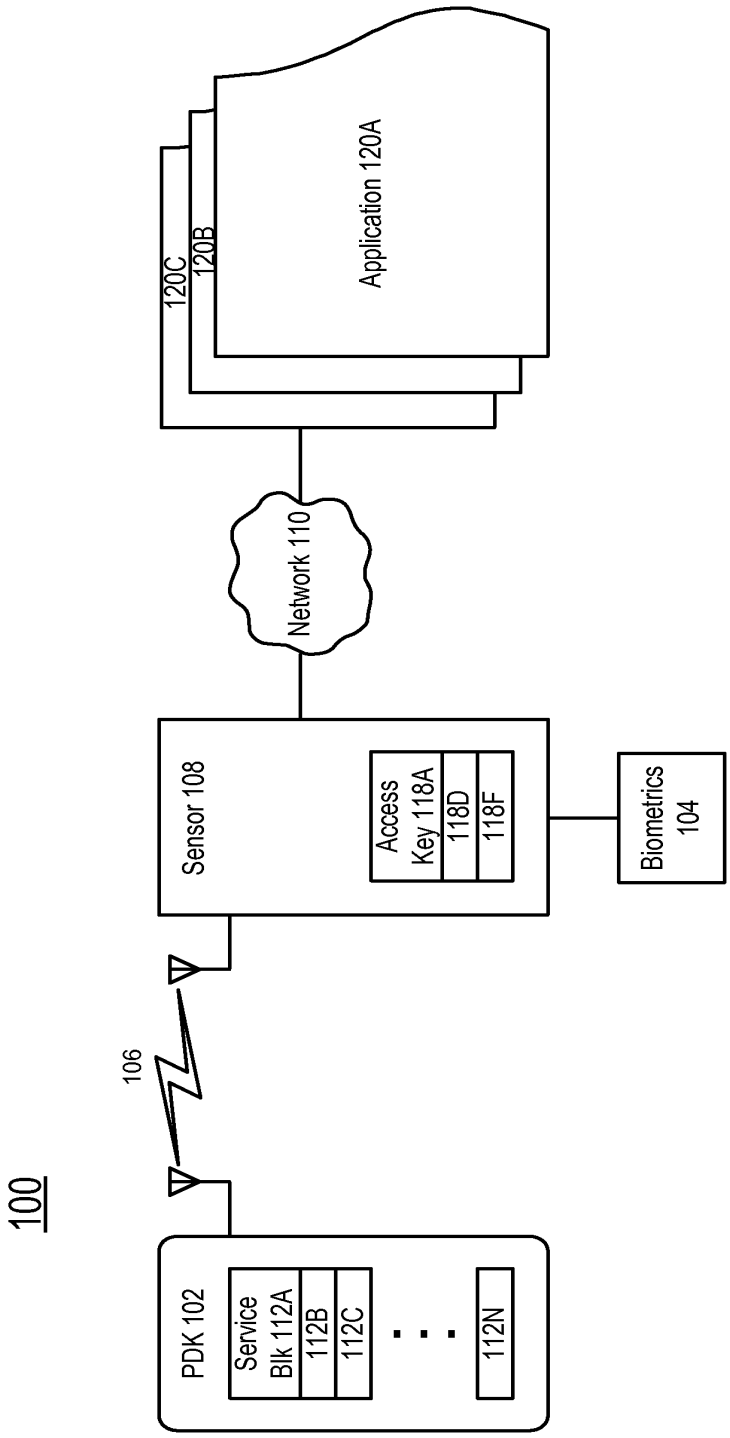

100
PDK 102
Service Blk 112A
112B
112C
112N
106
Sensor 108
Access Key 118A
118D
118F
Biometrics 104
Network 110
120C
120B
Application 120A

FIG. 1

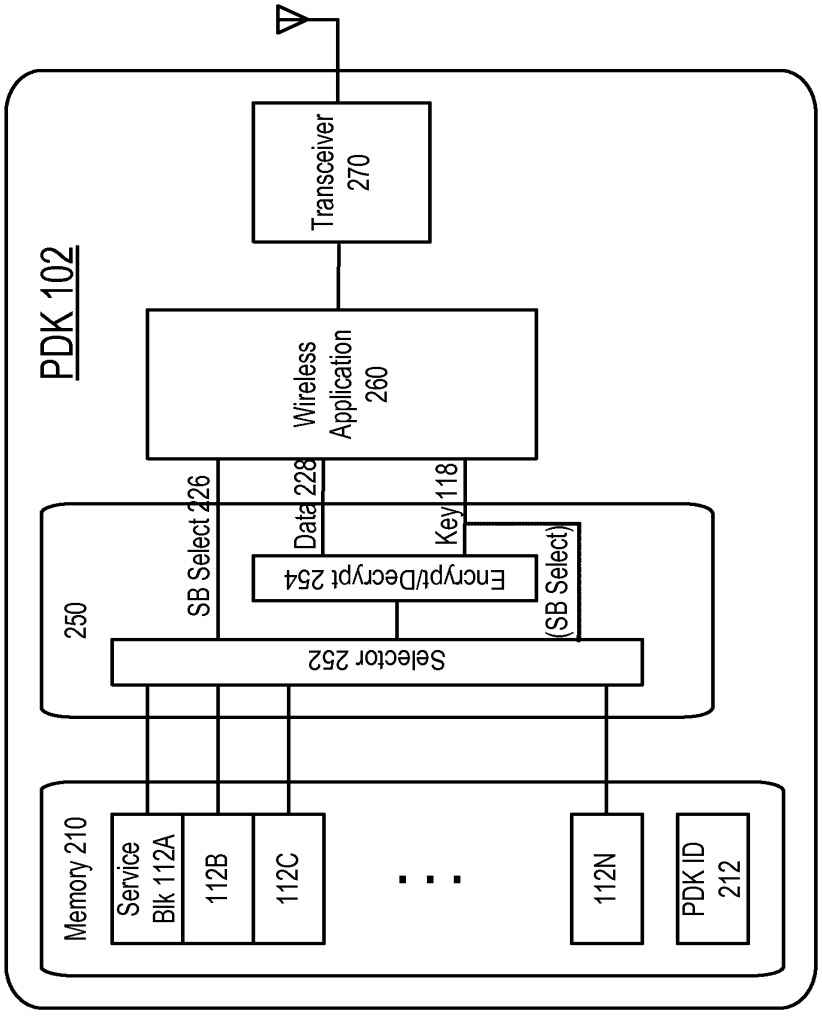

PDK 102
Transceiver 270
Wireless Application 260
SB Select 226
Data 228
Key 118
250
Encrypt/Decrypt 254
(SB Select)
Selector 252
Memory 210
Service Blk 112A
112B
112C
112N
PDK ID 212

FIG. 2

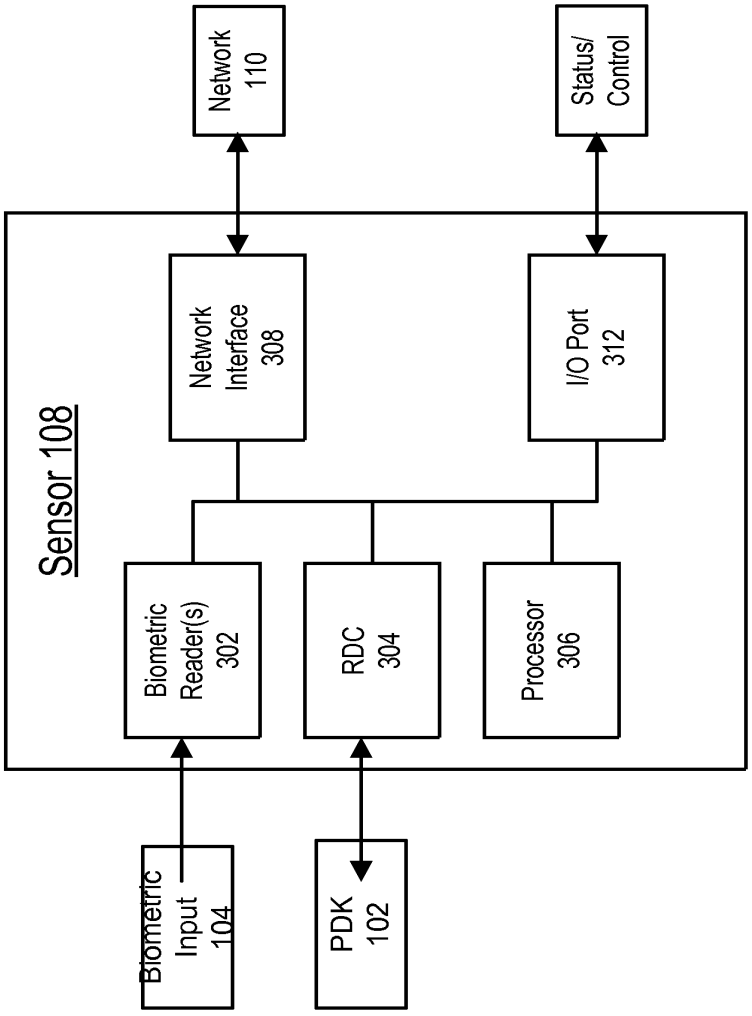

Network 110
Status/ Control
Sensor 108
Network Interface 308
I/O Port 312
Biometric Reader(s) 302
RDC 304
Processor 306
Biometric Input 104
PDK 102

FIG. 3

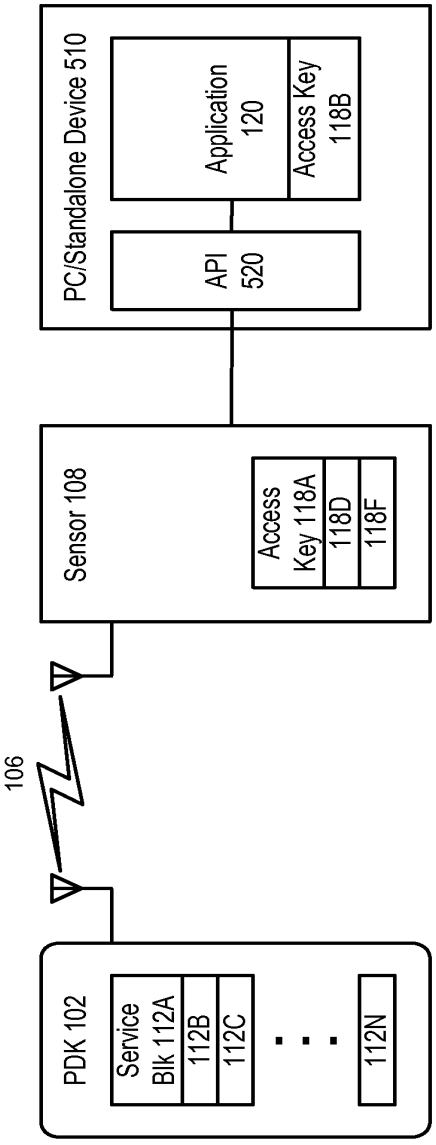

PC/Standalone Device 510
Application 120
Access Key 118B
API 520
Sensor 108
Access Key 118A
118D
118F
106
PDK 102
Service Blk 112A
112B
112C
112N

FIG. 4

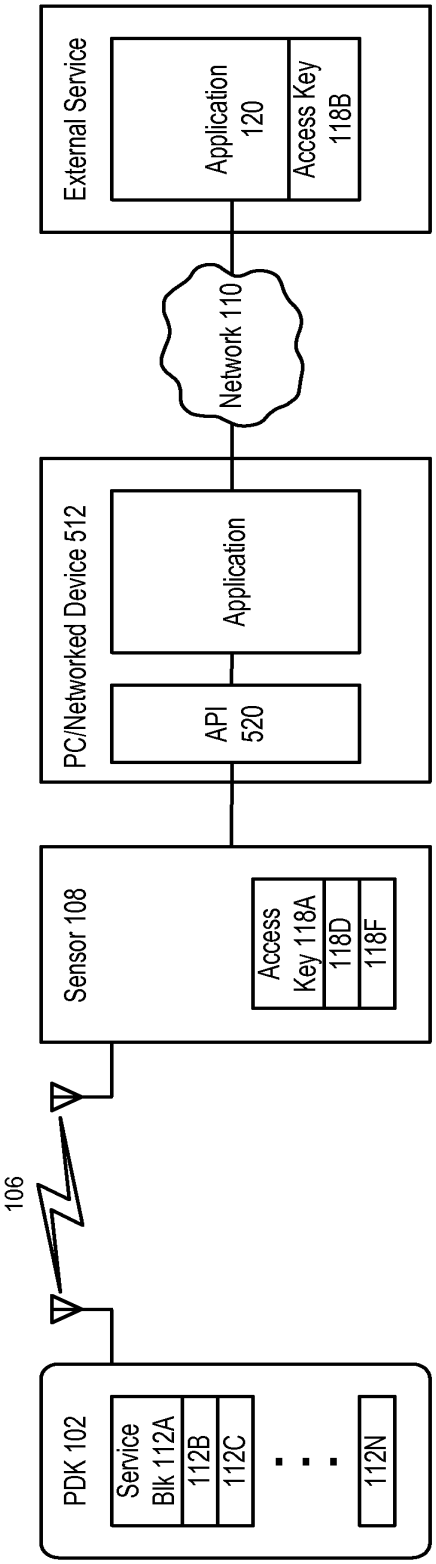

PDK 102
Service Blk 112A
112B
112C
112N
106
Sensor 108
Access Key 118A
118D
118F
PC/Networked Device 512
API 520
Application
Network 110
External Service
Application 120
Access Key 118B

FIG. 5

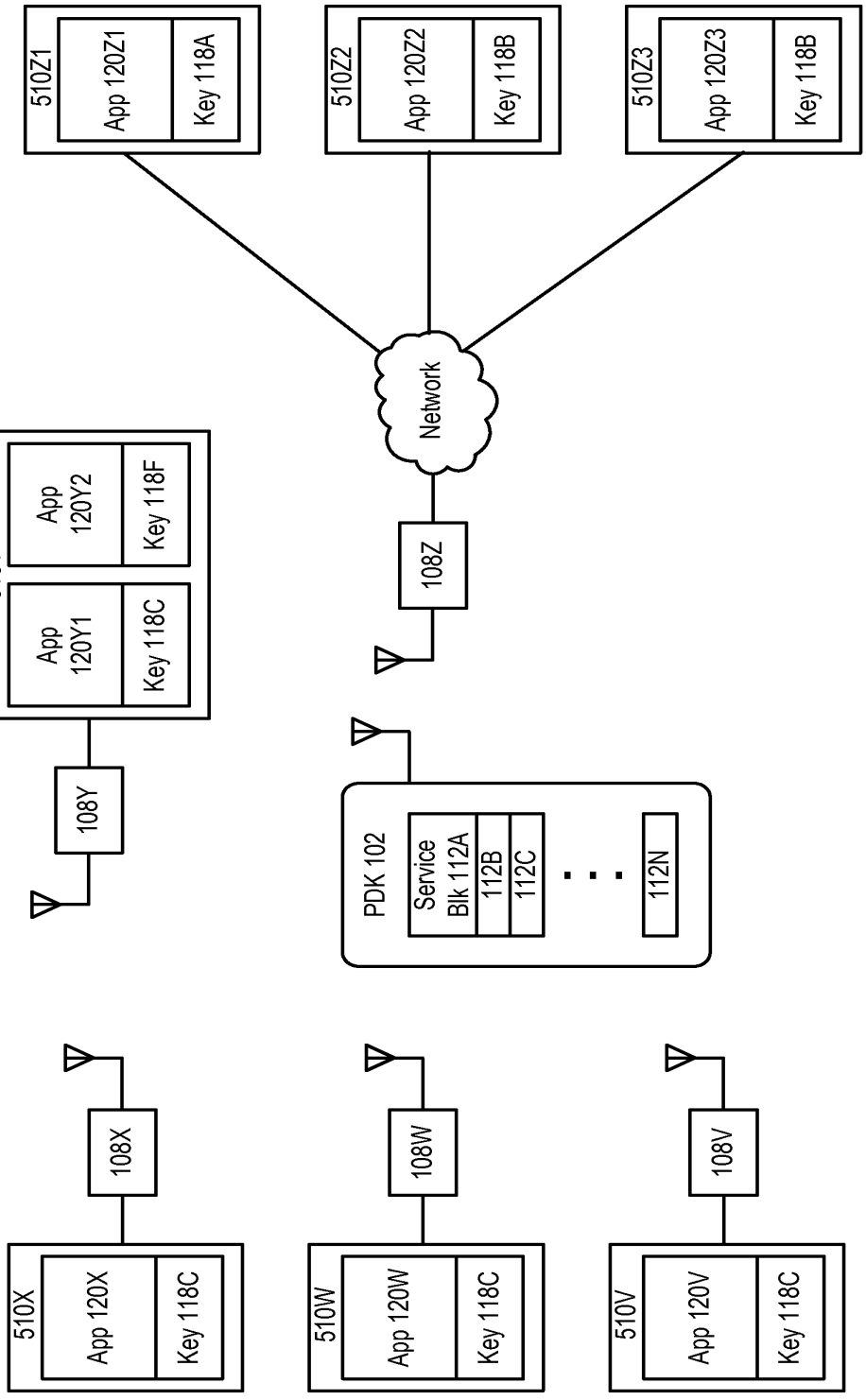

510Z1
App 120Z1
Key 118A
510Z2
App 120Z2
Key 118B
510Z3
App 120Z3
Key 118B
Network
510Y
App 120Y2
Key 118F
App 120Y1
Key 118C
108Z
108Y
PDK 102
Service Blk 112A
112B
112C
112N
510X
App 120X
Key 118C
510W
App 120W
Key 118C
510V
App 120V
Key 118C
108X
108W
108V

FIG. 6

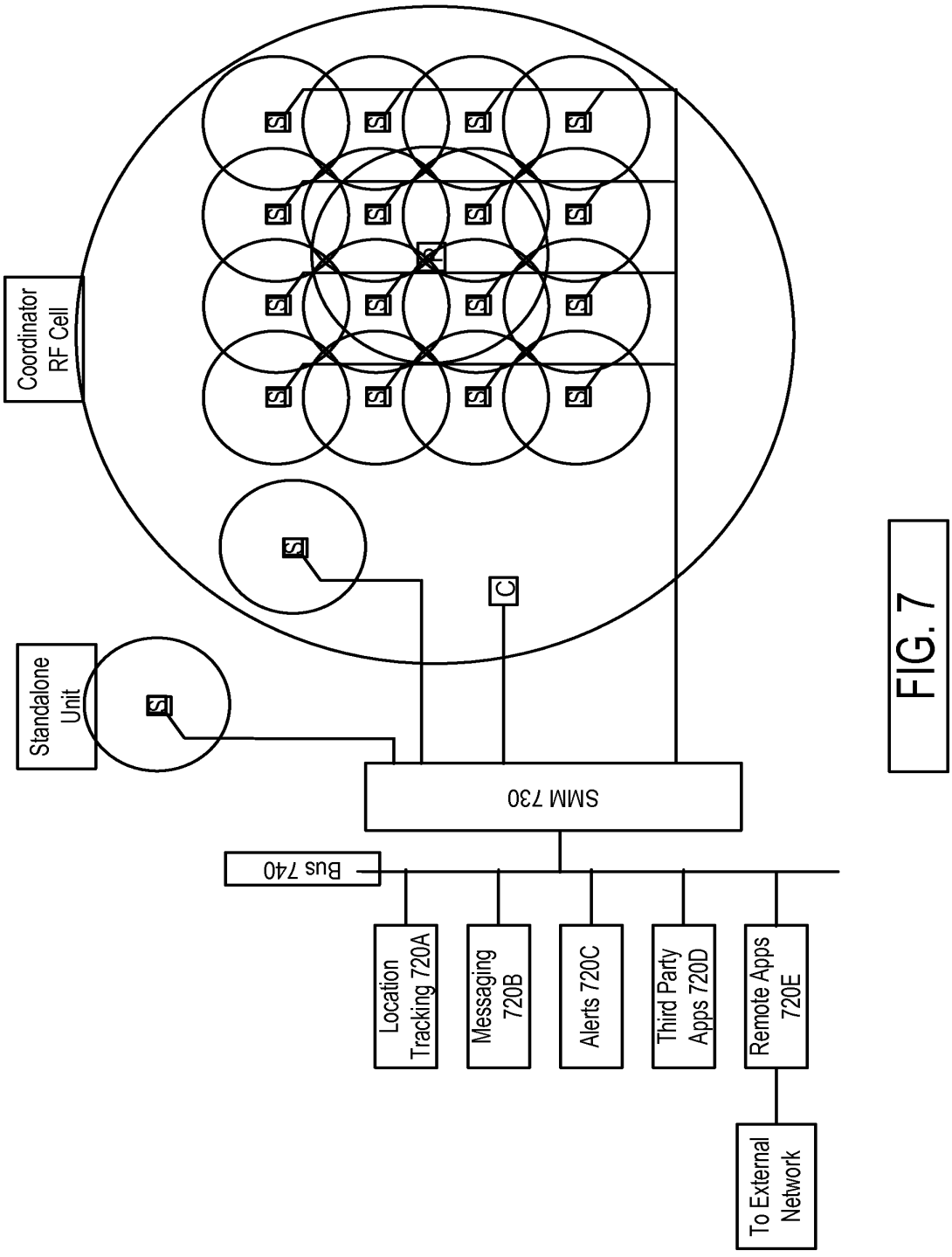

Coordinator RF Cell
Standalone Unit
S
C
SMM 730
Bus 740
Location Tracking 720A
Messaging 720B
Alerts 720C
Third Party Apps 720D
Remote Apps 720E
To External Network

FIG. 7

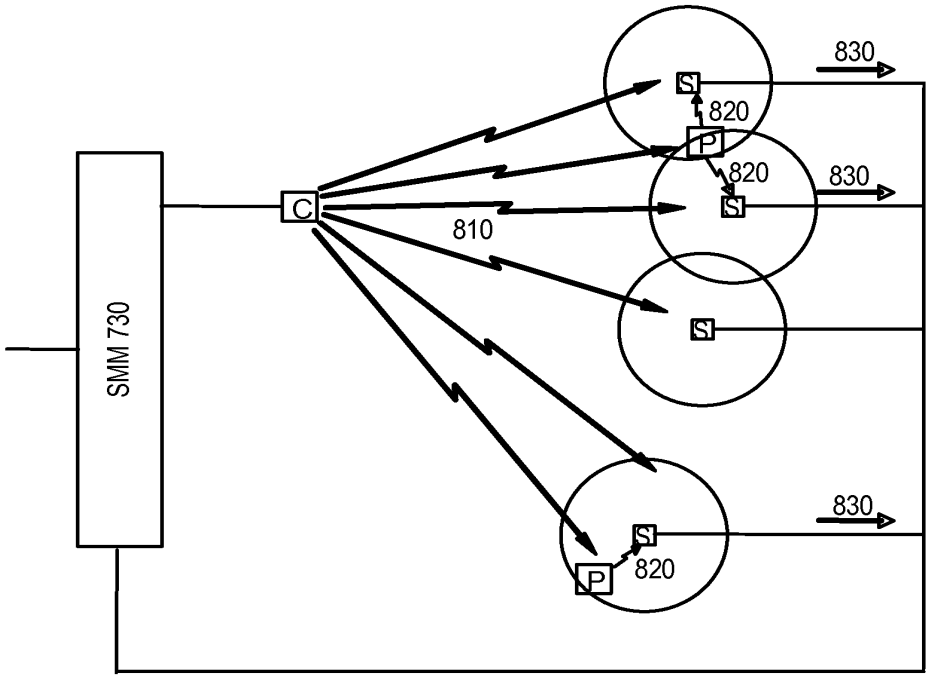


FIG. 8

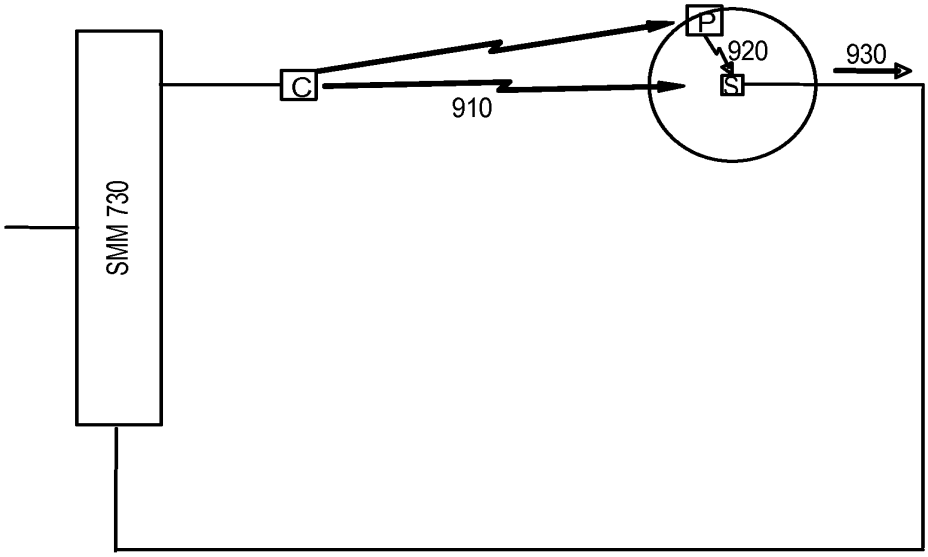


FIG. 9

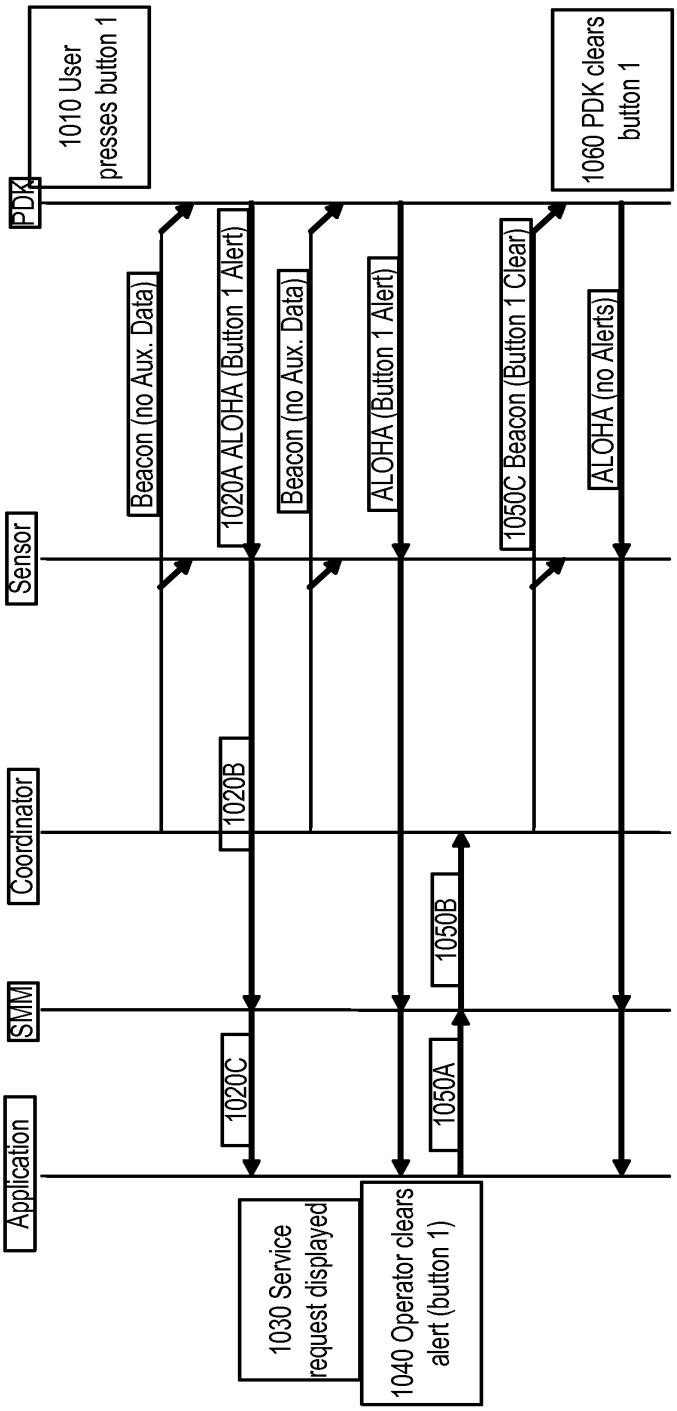

PDK
Sensor
Coordinator
SMM
Application
1010 User presses button 1
Beacon (no Aux. Data)
1020A ALOHA (Button 1 Alert)
1020B
1020C
Beacon (no Aux. Data)
ALOHA (Button 1 Alert)
1050B
1050A
1050C Beacon (Button 1 Clear)
ALOHA (no Alerts)
1060 PDK clears button 1
1030 Service request displayed
1040 Operator clears alert (button 1)

FIG. 10

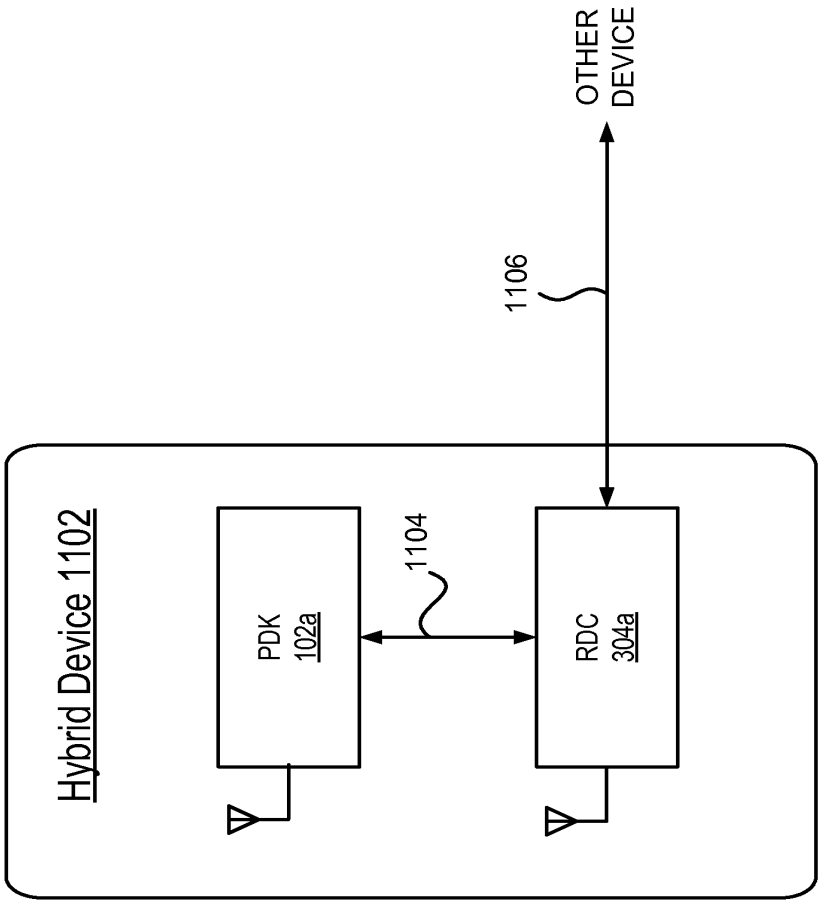


FIG. 11

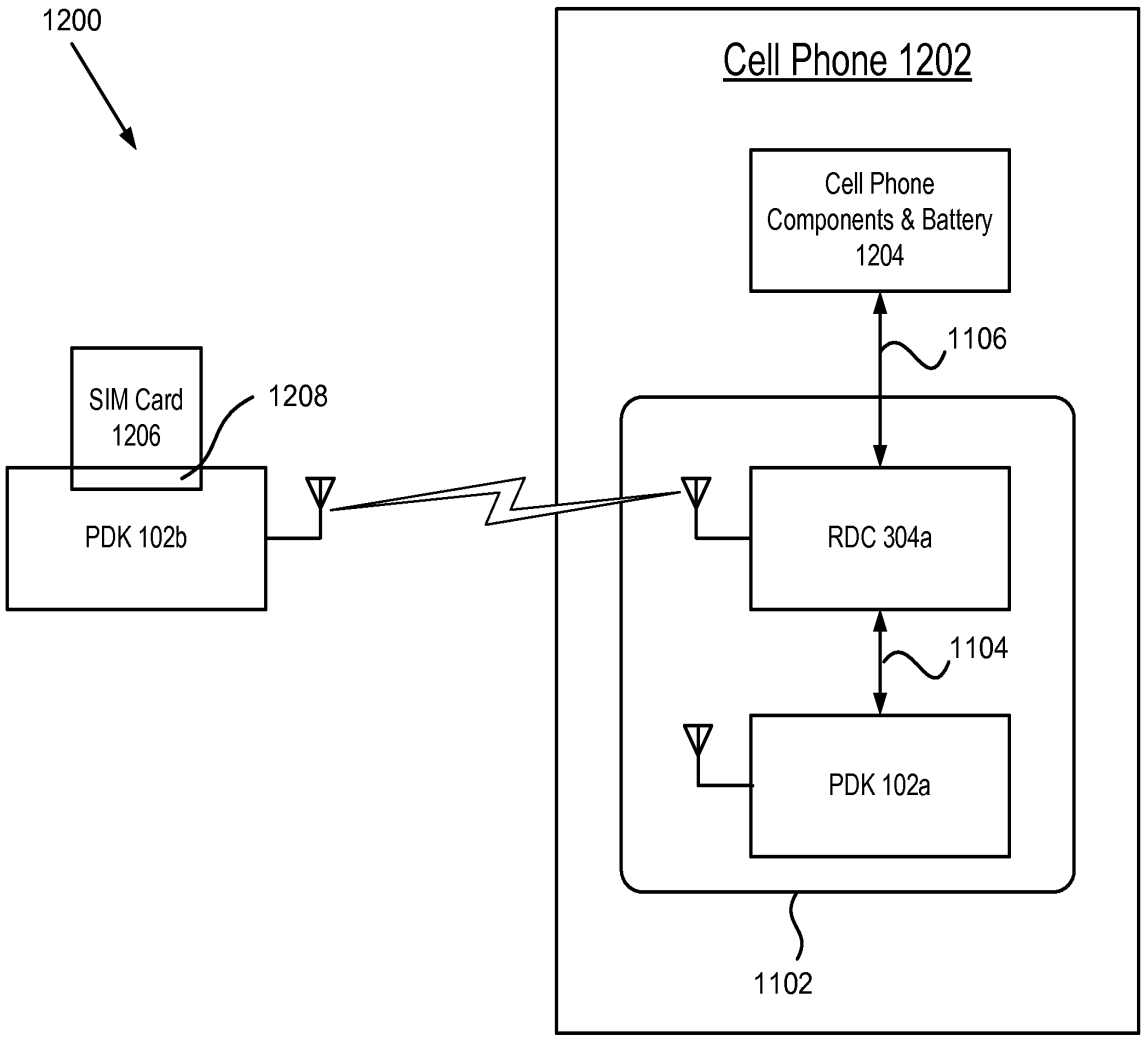


FIG. 12

APPLE Ex. 1002, Page 62

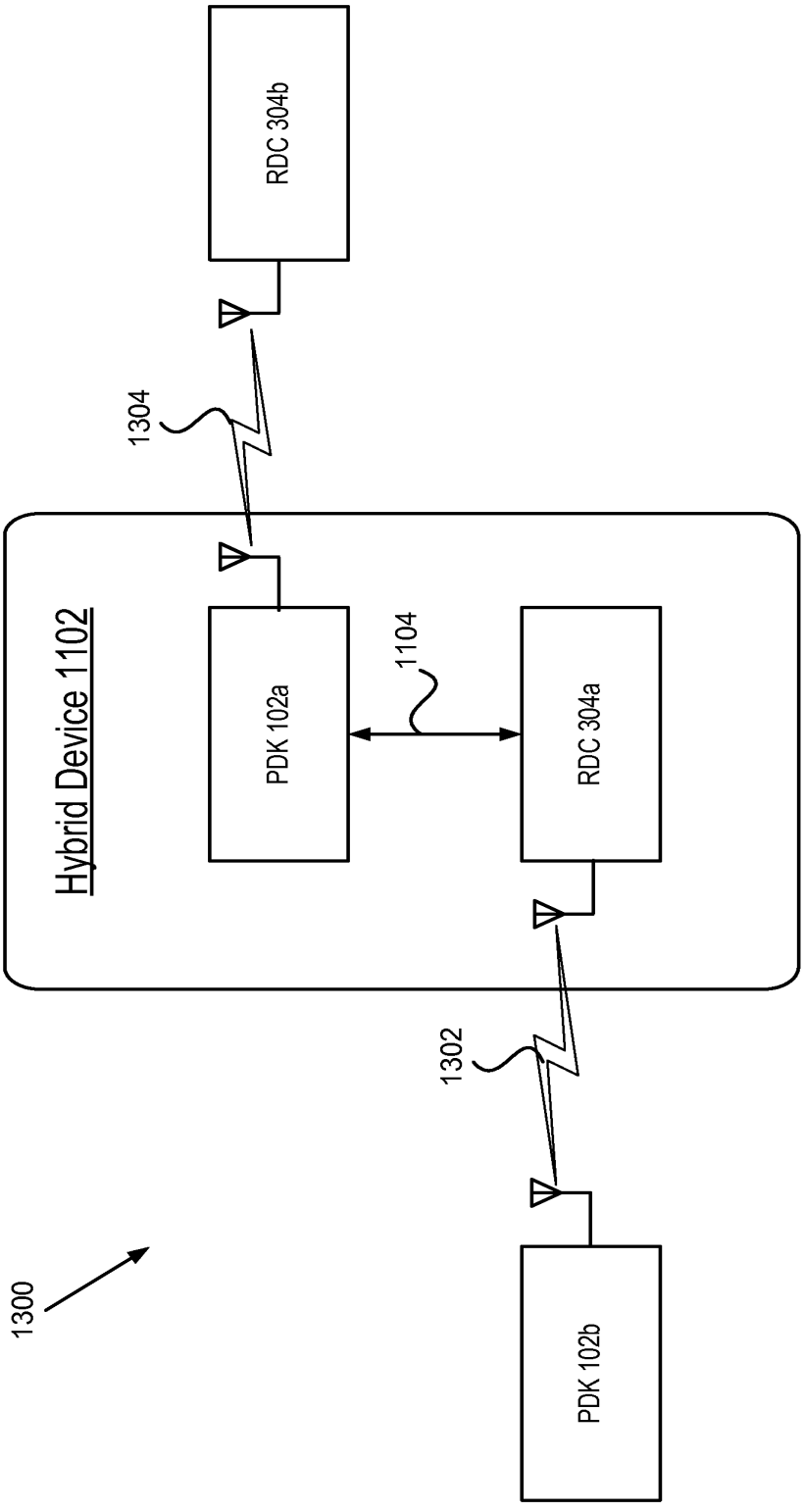

1300
Hybrid Device 1102
PDK 102a
1104
RDC 304a
RDC 304b
1304
1302
PDK 102b

FIG. 13

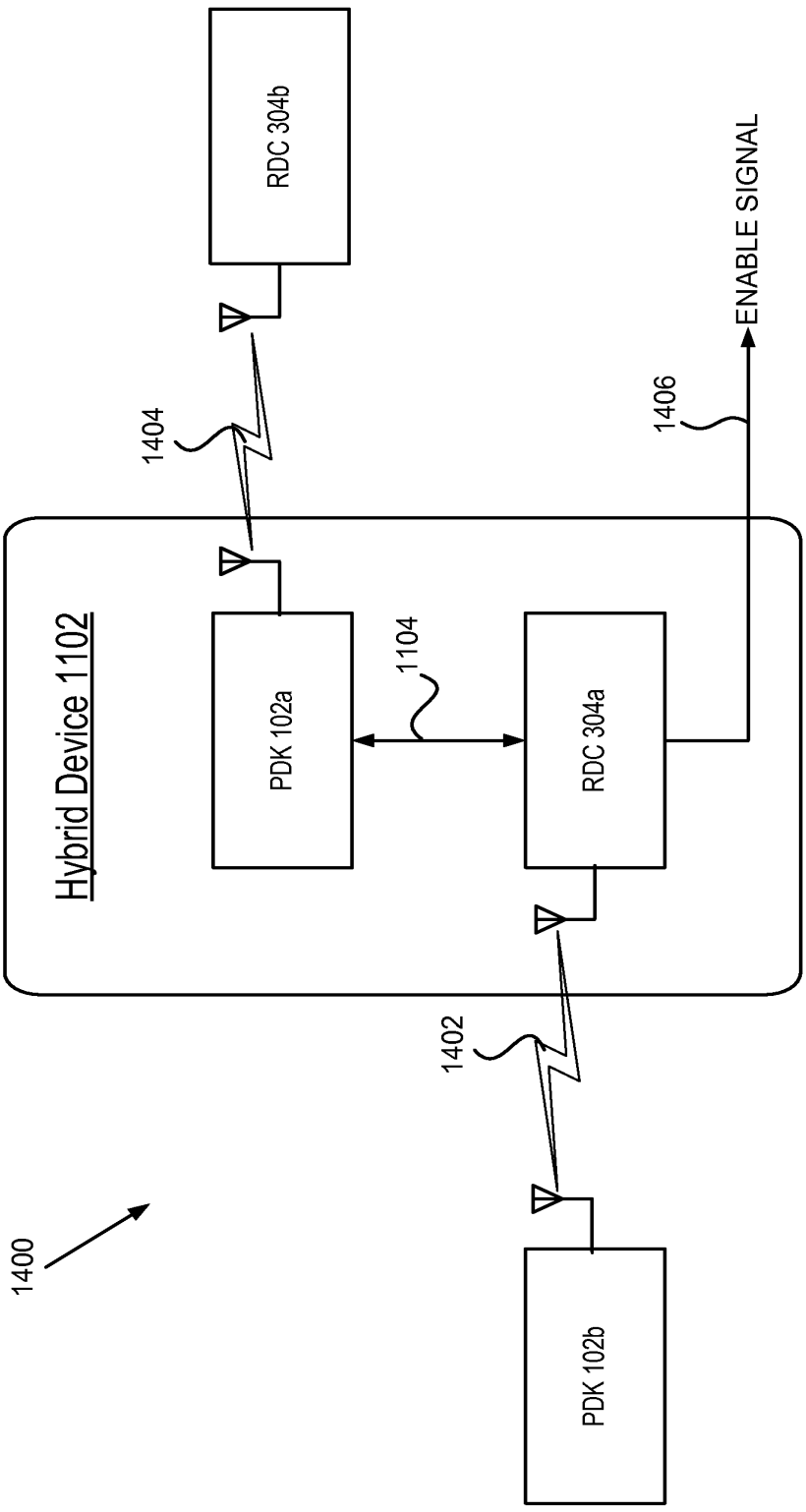

1400
Hybrid Device 1102
PDK 102a
1104
RDC 304a
PDK 102b
RDC 304b
1402
1404
1406
ENABLE SIGNAL

FIG. 14

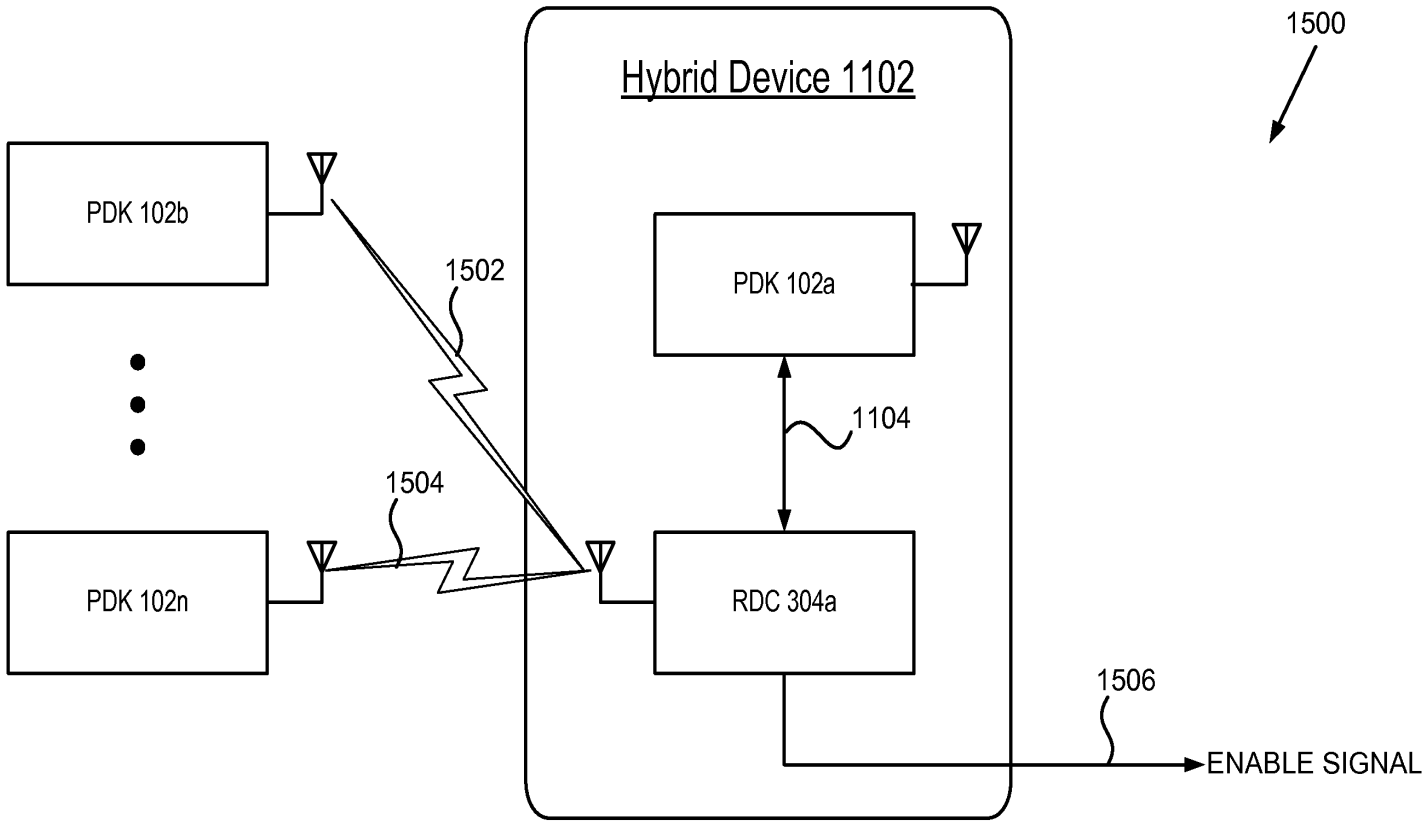


FIG. 15

APPLE Ex. 1002, Page 65

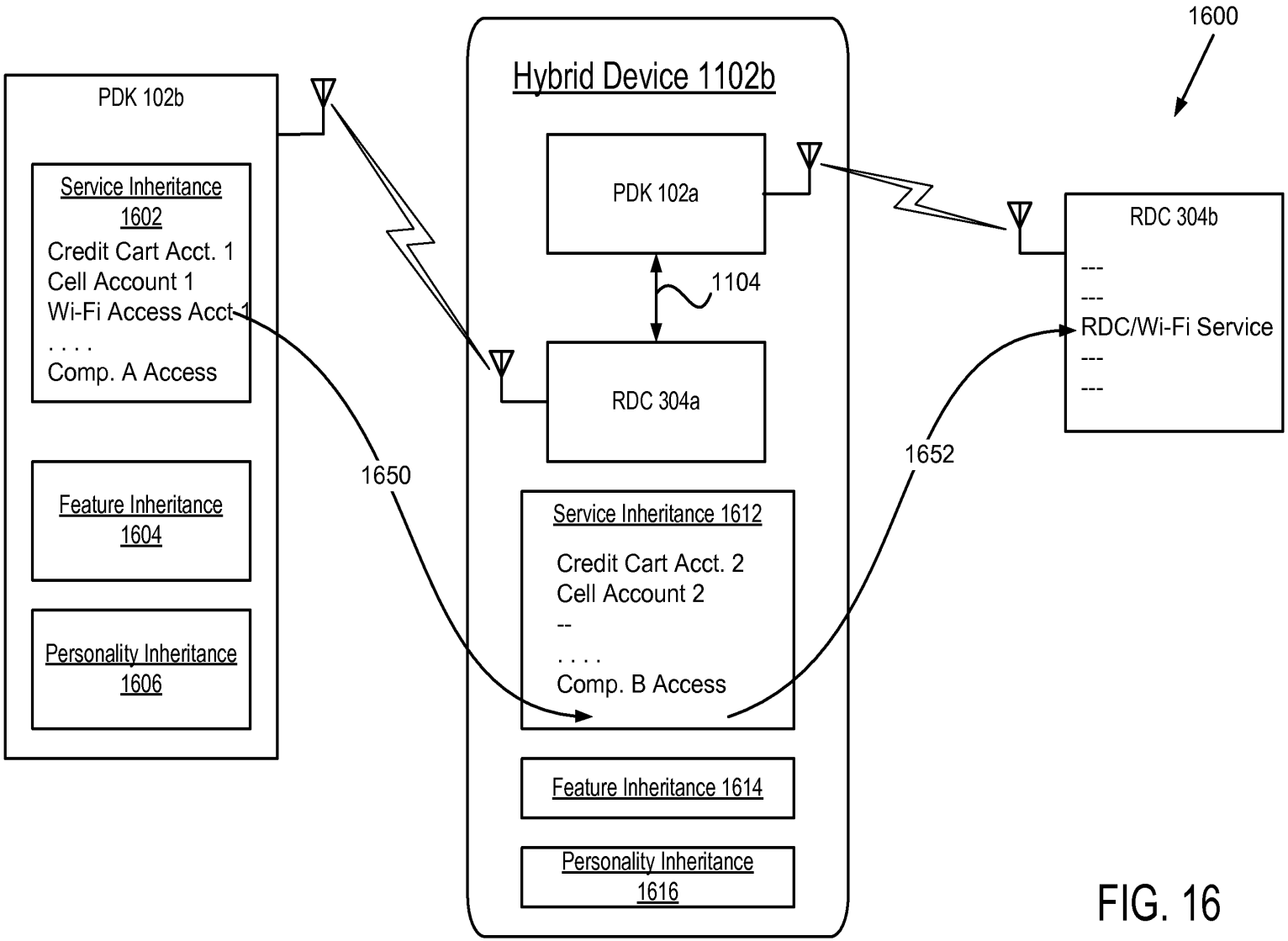


FIG. 16

APPLE Ex. 1002, Page 66

Electronic Acknowledgement Receipt

EFS ID:	18102217
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	03-FEB-2014
Filing Date:	
Time Stamp:	21:03:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	04293US_ApplicationDataSheet_03022014.pdf	1279700 93762194693e136709cc10e9bf7c55e9e118d129	no	7

Warnings:	
Information:	

2		04293US_Specification_03022014.pdf	245732 f3f789407e68157bfc90d8fca3e7a2a65d3fba53	yes	44

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	42
	Claims	43	43
	Abstract	44	44

Warnings:					
Information:					
3	Drawings-only black and white line drawings	04293US_Drawings_03022014.pdf	99076 b549a6dbbb7f7feafa635d89c9d26706f6d6edef	no	15
Warnings:					
Information:					
		Total Files Size (in bytes):	1624508		

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/171,705	02/03/2014	David L. Brown	10001-04293 US

CONFIRMATION NO. 7167

89194
Patent Law Works/Proxense
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FORMALITIES LETTER

OC000000066859854

Date Mailed: 02/28/2014

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** basic filing fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0.00**) previous unapplied payment amount.
- $ **800** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's

oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  David L. Brown

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/rerry/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/171,705

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

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

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/171,705	02/03/2014	1648	0.00	10001-04293 US	1	1

CONFIRMATION NO. 7167

89194
Patent Law Works/Proxense
201 South Main Street, Suite 250
Salt Lake City, UT 84111

FILING RECEIPT

OC000000066859853

Date Mailed: 02/28/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)
David L. Brown, Jupiter, FL;

Applicant(s)
Proxense, LLC, Residence Not Provided

Assignment For Published Patent Application
Proxense, LLC

Power of Attorney: None

Domestic Priority data as claimed by applicant
This application is a CON of 13/445,825 04/12/2012 PAT 8646042
which is a CON of 12/329,329 12/05/2008 PAT 8171528
which claims benefit of 60/992,953 12/06/2007

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 02/27/2014
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/171,705**
Projected Publication Date: Request for Non-Publication Acknowledged
Non-Publication Request: Yes
Early Publication Request: No
** **SMALL ENTITY** **

Title

Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

Preliminary Class

424

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	David L. Brown
APPLICATION NO:	14/171,705
FILING DATE:	February 3, 2014
TITLE:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
EXAMINER:	Not Yet Known
GROUP ART UNIT:	1648
ATTY. DKT. NO:	10001-04293 US
CONFIRMATION NO:	7167

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: April 28, 2014 By: /Kanda Ishihara/
Kanda V. Ishihara, Reg. No.56,607

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

RESPONSE TO NOTICE TO FILE MISSING PARTS OF AN APPLICATION

Sir/Madam:

Responsive to the Notice of Missing Parts dated February 28, 2014, received in the above-identified application,

☒ Enclosed are:

☒ an executed Substitute Statement in Lieu of an Oath or Declaration;

☒ payment in the amount of $800 for the

☒ application filing fee;

(continued)

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

☐ fee for additional claims; and

☒ missing parts surcharge.

☒ Other: Application search fee

☒ an executed Power of Attorney;

☒ Applicant claims small entity status under 37 C.F.R. § 1.27.

Respectfully submitted,
DAVID L. BROWN

Dated: April 28, 2014 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (650) 537-4505
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

Doc code: Oath
Document Description: Oath or declaration filed

RECEIVED
PATENT DOCKETING
Patent Law Works
3/19/2014 8:45:23 am

PTO/AIA/02 (07-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

This statement is directed to:

☐ The attached application,

OR

☒ United States application or PCT international application number 14/171,705 filed on February 3, 2014.

LEGAL NAME of inventor to whom this substitute statement applies:

(*E.g.*, Given Name (first and middle (if any)) and Family Name or Surname)

David L. Brown

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Jupiter	FL	US

Mailing Address (except for a deceased or legally incapacitated inventor):

17708 127th Dr. North

City	State	Zip	Country
Jupiter	FL	33478	US

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only),
- ☒ Assignee,
- ☐ Person to whom the inventor is under an obligation to assign,
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/AIA02 (07-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased.
- ☐ Inventor is under legal incapacity.
- ■ Inventor cannot be found or reached after diligent effort, or
- ☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ■ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: John J. Giobbi | Date (Optional):

Signature:

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer:

Applicant Name:

Title of Person Executing This Substitute Statement: Chief Executive Officer

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City Bend | State OR | Country US

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

689 NW Stonepine Drive

City Bend | State OR | Zip 97701 | Country US

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

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.

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82A (07-12)

Approved for use through 11/30/2014. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	14/171,705
Filing Date	February 3, 2014
First Named Inventor	David L. Brown
Title	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
Art Unit	1648
Examiner Name	Not Yet Assigned
Attorney Docket Number	10001-04293 US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Kanda Ishihara/	Date	April 28, 2014
Name	Kanda V. Ishihara	Telephone	650-537-4505
Registration Number	56,607		

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

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

89194

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.*, a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	02/20/14
Name	John J. Giobbi	Telephone	
Title and Company	Chief Executive Officer		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14171705
Filing Date:	03-Feb-2014
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Filer:	Kanda Ishihara/Cynthia Kersey
Attorney Docket Number:	10001-04293 US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	800

Electronic Acknowledgement Receipt	
EFS ID:	18883278
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	28-APR-2014
Filing Date:	03-FEB-2014
Time Stamp:	20:13:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$800
RAM confirmation Number	8066
Deposit Account	
Authorized User	

File Listing:

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

1	Applicant Response to Pre-Exam Formalities Notice	04293US_ResponsetoMissingParts.pdf	74792 3cb50dae701a4e417307e7415a9faf02eb471069	no	2
Warnings:					
Information:					
2	Oath or Declaration filed	04293US_SignedSubstituteStatement_GiobbiforBrown.pdf	1028699 3c639f04a376727d7b8a97be4e6d4b2bd0916ecc	no	3
Warnings:					
Information:					
3	Power of Attorney	04293US_PowerofAttorney.pdf	312488 e1fd9151da4dac12c26b903d63edd9148348db65	no	3
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	36842 95e45cc6f218bb0bf8808be915cf0878245a47f4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1452821		

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/171,705

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

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

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/171,705	02/03/2014	David L. Brown	10001-04293 US

CONFIRMATION NO. 7167

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

IMPROPER CPOA LETTER

OC000000068147632

Date Mailed: 05/07/2014

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the power of attorney filed 04/28/2014. The power of attorney in this application is not accepted for the reason(s) listed below:

- The power of attorney has not been accepted because the party who is giving power has not been identified. Power of attorney may only be signed by the applicant for patent (37 CFR 1.42) or the patent owner. A party who is not the applicant must become the applicant in accordance with 37 CFR 1.46(c) and appoint any power of attorney in compliance with 37 CFR 3.71 and 3.73. For a reissue application, reexamination proceeding, or supplemental examination proceeding, a patent owner who was not the applicant under 37 CFR 1.46 must appoint any power of attorney in compliance with 37 CFR 3.71 and 3.73. See 37 CFR 1.32(b)(4).

/cnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/171,705	02/03/2014	David L. Brown	10001-04293 US

CONFIRMATION NO. 7167

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

NOTICE

OC000000068147610

Date Mailed: 05/07/2014

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  David L. Brown
- The substitute statement is signed by a person who is not identified as the applicant under 37 CFR 1.46 in an application data sheet (ADS). Only an applicant under 37 CFR 1.43, 1.45 or 1.46 may execute a substitute statement. See 37 CFR 1.64(a). An application data sheet in compliance with 37 CFR 1.76 identifying the person (i.e., assignee, obligated assignee, or person who otherwise shows sufficient proprietary interest) executing the substitute statement as the applicant, or an inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to the inventor for whom the substitute statement was provided, is required.
  David L. Brown

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/171,705	02/03/2014	1648	800	10001-04293 US	1	1

CONFIRMATION NO. 7167

UPDATED FILING RECEIPT

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

OC000000068147609

Date Mailed: 05/07/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

David L. Brown, Jupiter, FL;

Applicant(s)

Proxense, LLC, Residence Not Provided

Assignment For Published Patent Application

Proxense, LLC

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/445,825 04/12/2012 PAT 8646042
which is a CON of 12/329,329 12/05/2008 PAT 8171528
which claims benefit of 60/992,953 12/06/2007

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 02/27/2014
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/171,705**
Projected Publication Date: Request for Non-Publication Acknowledged
Non-Publication Request: Yes
Early Publication Request: No
** **SMALL ENTITY** **

Title

Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

Preliminary Class

424

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82A (07-12)

Approved for use through 11/30/2014. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B or equivalent) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5. If the Power of Attorney by Applicant form is not accompanied by this transmittal form or an equivalent, the Power of Attorney will not be recognized in the application.

Application Number	14/171,705
Filing Date	February 3, 2014
First Named Inventor	David L. Brown
Title	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
Art Unit	1648
Examiner Name	Not Yet Assigned
Attorney Docket Number	10001-04293 US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Kanda Ishihara/	Date	July 24, 2014
Name	Kanda V. Ishihara	Telephone	650-537-4505
Registration Number	56,607		

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

■ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

89194

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.*, a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	02/20/14
Name	John J. Giobbi	Telephone	
Title and Company	Chief Executive Officer Proxense, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	19678542
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Kanda Ishihara
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	24-JUL-2014
Filing Date:	03-FEB-2014
Time Stamp:	20:26:16
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	04293US_PowerofAttorney.pdf	979628 2cabdf97b4cf429a82856c2014d1e2ee4ab0f05f	no	3
Warnings:					
Information:					

Total Files Size (in bytes):	979628

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/171,705	02/03/2014	David L. Brown	10001-04293 US

CONFIRMATION NO. 7167

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

POA ACCEPTANCE LETTER

OC000000069838047

Date Mailed: 07/28/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/24/2014.

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.

/sibrahim/

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	02/03/2014	David L. Brown	10001-04293 US	7167

89194 7590 09/22/2014

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

EXAMINER	
LEE, JASON T	
ART UNIT	**PAPER NUMBER**
2438	

NOTIFICATION DATE	DELIVERY MODE
09/22/2014	ELECTRONIC

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

The time period for reply, if any, is set in the attached communication.

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

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

Office Action Summary	Application No. 14/171,705	Applicant(s) BROWN, DAVID L.	
	Examiner JASON LEE	Art Unit 2438	AIA (First Inventor to File) Status No

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

Period for Reply

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

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

Status

1)☒ Responsive to communication(s) filed on *02/03/2014* .

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

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

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

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

Disposition of Claims*

5)☒ Claim(s) *1* 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* is/are rejected.

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

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

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

Application Papers

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

11)☒ The drawing(s) filed on *2/3/14* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions. The following is a Non-Final Office action in response to the application filed on February 03, 2014. Claim 1 is presented for examination.

Drawings

2. The drawings replacement filed on 02/03/2014 are accepted.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 04/28/2014 has been accepted.

Priority

4. This application is a continuation related to and claimed the benefits of U.S. application No. 60/992,953 dated 12/06/2007.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

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

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Independent claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of US the patent No. 8,171,528 B1 and claim 1 of US the patent No. 8, 646,042 B1.

Although the conflicting claims are not identical, they are not patentably distinct from (see one-on-one claim comparison table below) each other because claim 1 of the instant application is anticipated by the subject matter recited in claim 1 of U.S patent 8,171,528 correspondingly and also anticipated by the subject matter recited in claim 1 of the U.S patent 8, 646,042 correspondingly.

Claim Comparison Table

Instant application	U.S patent 8,171,528 (filed by same inventive entity and common assignee)	U.S patent 8, 646,042 (filed by same inventive entity and common assignee)
1. A hybrid device for use in a proximity system, the hybrid device comprising: a personal digital key (PDK) for storing information and capable of communicating	1. A hybrid device for use in a proximity system, the hybrid device comprising: a first personal digital key (PDK) for storing information and capable of	1. A hybrid device comprising: an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with at least

wirelessly, the PDK for linking with RDCs; a receiver-decoder circuit (RDC) for linking with PDKs, the RDC capable of communicating wirelessly, the RDC coupled to the PDK by a first signal line, the RDC coupled to a second signal line for communicating and enabling an external device.	communicating wirelessly, the PDK for linking with at least one external receiver-decoder circuit (RDC); and a receiver-decoder circuit (RDC) for linking with at least one external PDKs, the RDC capable of communicating wirelessly with the external PDK, the RDC coupled to the PDK by a first signal line and coupled for communication with the first PDK, the RDC coupled to a second signal line for communicating and enabling an external device.	one external receiver-decoder circuit (RDC); and an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the

		external RDC.

Claim Rejections - 35 USC § 103

7. 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.

8. Claims 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Finn et al (US 2006/0208066 A1), hereinafter Finn, in view of Hochstein et al (US 2006/0113381 A1) hereinafter Hochstein.

As for claim 1:

Finn discloses **a hybrid device for use in a proximity system,** (See Finn [0034-0036]") A contact smart card (or contact chip card) is a plastic card about the size of a credit card that has an embedded integrated circuit (IC) chip to store data. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor device. Contactless smart cards do not require direct contact with the reader because they employ the passive transponder technology of Radio Frequency Identification (RFID). By just waving the card near the reader, secure identification, electronic payment transaction and authentication are completed in milliseconds.") **the hybrid device comprising: a personal digital key (PDK) for storing information and capable of communicating wirelessly,** (See Finn

[0228-0236] “In this embodiment 140, a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications. The memory management for the device may be handled by a crypto controller operating system with an 8 bit address bus in the dual interface (DI) chip. The flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card. (A crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.) **the PDK for linking with RDCs; a receiver-decoder circuit (RDC) for linking with PDKs, the RDC capable of communicating wirelessly,** (See Finn [0090-0094]” Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.” And [0256] “A compact personal token apparatus comprises a connection module; a translation module; a processor module; and an input/output module. The connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and the interface is selected from the group consisting of USB, FireWire, standard serial port, IR, Bluetooth, WLAN. The Internet-capable appliance may comprise a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cell phone. The translation module moves signals between a USB interface and a smart card interface. The smart card interface may be selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.) **the RDC coupled to the PDK by a first signal line, the RDC coupled to a second signal line for communicating and enabling an external device.** (See

Finn [0185] “a RFID token apparatus comprises: two or more internal USB devices; and a USB hub controller integrated into the apparatus for facilitating communication (enabling transmission of data) between the internal USB devices and a host computer into which the USB apparatus is plugged. The internal USB devices are selected from the group

consisting of USB (NAND) flash memory device, USB hard disk drive (HDD), USB devices with RFID that can adopt the smart card protocol, USB smart card devices and USB wireless devices. The hub controller may be accompanied by a second micro controller for the purpose of accelerating an encryption/decryption process.”)

Finn discloses a USB devices using RFID integrated into the apparatus for facilitating communication (enabling transmission of data) between the internal USB devices and a host computer into which the USB apparatus is plugged. USB devices with RFID that can adopt the smart card protocol, USB smart card devices and USB wireless devices. The hub controller may be accompanied by a second micro controller for the purpose of accelerating an encryption/decryption process. Therefore, Finn teaches the claimed limitations of PDK with the RDC that communicating wirelessly for exchange information (i.e. encryption/decryption process).

Hochstein, also teaches the same field of endeavor of smart token in contactless for information exchange as Finn, further discloses “a smartcard reader--the facility access control system ("security control panel") receives a signal from the card reader that the user has exited and suspends the cardholder's access privileges until the user is biometrically re-authenticated.” (See Hochstein [0027])

Therefore, it would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Finn to include the teaching of Hochstein for “receive signal for communicating and enable an external device (e.g. controlled facility) and “perform contactless functions within the facility, once contactless functions are appropriately enabled” for enhancing authorization.(See Hochstein [0028])

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/JASON LEE/

Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/171,705	Applicant(s)/Patent Under Reexamination BROWN, DAVID L.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0113381	06-2006	Hochstein et al.	235/382
*	B	US-2006/0208066	09-2006	Finn et al.	235/380
	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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	3,4	9/16/14	JL

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched	9/16/14	JL
google patent searched with RFID smartcard with signal receiver	9/16/14	JL

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

BIB DATA SHEET

CONFIRMATION NO. 7167

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/171,705	02/03/2014	726	2438	10001-04293 US

APPLICANTS
Proxense, LLC, Residence Not Provided, Assignee (with 37 CFR 1.172 Interest);

INVENTORS
David L. Brown, Jupiter, FL;

**** CONTINUING DATA ***************************
This application is a CON of 13/445,825 04/12/2012 PAT 8646042
which is a CON of 12/329,329 12/05/2008 PAT 8171528
which claims benefit of 60/992,953 12/06/2007

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
02/27/2014

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /JASON T LEE/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		FL	15	1	1

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

TITLE
Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	**Art Unit**
	JASON LEE	2438

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

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

CLAIM		DATE								
Final	Original	09/17/2014								
	1	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	3	"20060113381".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/17 11:43
L3	2	"20060208066".pn. and signal	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/17 12:37
S1	2	"8171528".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:18
S2	2	"8646942".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:19
S3	2	"8646042".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:19
S4	2	"20060208066".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 19:50

EAST Search History (Interference)

< This search history is empty>

9/ 17/ 2014 12:38:11 PM
C:\ Users\ jlee16\ Documents\ EAST\ Workspaces\ 14171705-091614.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	14171705
Filing Date	2014-02-03
First Named Inventor	David L. Brown
Art Unit	2438
Examiner Name	Jason T. Lee
Attorney Docket Number	10001-04293 US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4759060	A	1988-07-19	Hayashi et al.	
	2	5187352	A	1993-02-16	Blair et al.	
	3	5296641	A	1994-03-22	Stelzel	
	4	5392433	A	1995-02-21	Hammersley et al.	
	5	5422632	A	1995-06-06	Bucholtz et al.	
	6	5450489	A	1995-09-12	Ostrover et al.	
	7	5619251	A	1997-04-08	Kuroiwa et al.	
	8	5629980	A	1997-05-13	Stefik et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	9	5644354	A	1997-07-01	Thompson et al.	
	10	5666412	A	1997-09-09	Handelman et al.	
	11	5773954	A	1998-06-30	VanHorn, David B.	
	12	5784464	A	1998-07-21	Akiyama et al.	
	13	5825876	A	1998-10-20	Peterson, Jr.	
	14	5857020	A	1999-01-05	Peterson, Jr.	
	15	5892825	A	1999-04-06	Mages et al.	
	16	5894551	A	1999-04-13	Huggins et al.	
	17	5898880	A	1999-04-27	Ryu	
	18	5928327	A	1999-07-27	Wang et al.	
	19	5991399	A	1999-11-23	Graunke et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	20	5991749	A	1999-11-23	Morrill, Jr.	
	21	6035038	A	2000-03-07	Campinos et al.	
	22	6035329	A	2000-03-07	Mages et al.	
	23	6041410	A	2000-03-21	Hsu et al.	
	24	6055314	A	2000-04-25	Spies et al.	
	25	6070796	A	2000-06-06	Sirbu	
	26	6088730	A	2000-07-11	Kato et al.	
	27	6104334	A	2000-08-15	Allport	
	28	6110041	A	2000-08-29	Walker et al.	
	29	6148142	A	2000-11-14	Anderson	
	30	6161179	A	2000-12-12	Seidel	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	31	6209089	B1	2001-03-27	Selitrennikoff et al.	
	32	6219109	B1	2001-04-17	Raynesford et al.	
	33	6247130	B1	2001-06-12	Fritsch	
	34	6266415	B1	2001-07-24	Campinos et al.	
	35	6295057	B1	2001-09-25	Rosin et al.	
	36	6336121	B1	2002-01-01	Lyson et al.	
	37	6336142	B1	2002-01-01	Kato et al.	
	38	6367019	B1	2002-04-02	Ansell et al.	
	39	6381747	B1	2002-04-30	Wonfor et al.	
	40	6385596	B1	2002-05-07	Wiser et al.	
	41	6392664	B1	2002-05-21	White et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	42	6397387	B1	2002-05-28	Rosin et al.	
	43	6401059	B1	2002-06-04	Shen et al.	
	44	6411307	B1	2002-06-25	Rosin et al.	
	45	6424715	B1	2002-07-23	Saito	
	46	6425084	B1	2002-07-23	Rallis et al.	
	47	6434535	B1	2002-08-13	Kupka et al.	
	48	6446130	B1	2002-09-03	Grapes	
	49	6463534	B1	2002-10-08	Geiger et al.	
	50	6480188	B1	2002-11-12	Horsley	
	51	6490443	B1	2002-12-03	Freeny, Jr.	
	52	6510350	B1	2003-01-21	Steen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	53	6523113	B1	2003-02-18	Wehrenberg	
	54	6529949	B1	2003-03-04	Getsin et al.	
	55	6546418	B1	2003-04-08	Schena et al.	
	56	6550011	B1	2003-04-15	Sims, III	
	57	6563805	B1	2003-05-13	Ma et al.	
	58	6564380	B1	2003-05-13	Murphy	
	59	6628302	B1	2003-09-30	White et al.	
	60	6632992	B2	2003-10-14	Hasegawa	
	61	6647417	B1	2003-11-11	Hunter et al.	
	62	6667684	B1	2003-12-23	Waggamon et al.	
	63	6683954	B1	2004-01-27	Searle	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	64	6697944	B1	2004-02-24	Jones et al.	
	65	6711464	B1	2004-03-23	Yap et al.	
	66	6775655	B1	2004-08-10	Peinado et al.	
	67	6804825	B1	2004-10-12	White et al.	
	68	6806887	B2	2004-10-19	Chernock et al.	
	69	6850147	B2	2005-02-01	Prokoski et al.	
	70	6873975	B1	2005-03-29	Hatakeyama et al.	
	71	6879567	B2	2005-04-12	Callaway et al.	
	72	6950941	B1	2005-09-27	Lee et al.	
	73	6957086	B2	2005-10-18	Bahl et al.	
	74	6973576	B2	2005-12-06	Giobbi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	75	6975202	B1	2005-12-13	Rodriguez et al.	
	76	7012503	B2	2006-03-14	Nielsen	
	77	7159765	B2	2007-01-09	Frerking, Gary	
	78	7249177	B1	2007-07-24	Miller	
	79	7305560	B2	2007-12-04	Giobbi	

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	20020007456	A1	2002-01-17	Peinado et al.	
	2	20020013772	A1	2002-01-31	Peinado	
	3	20020015494	A1	2002-02-07	Nagai et al.	
	4	20020026424	A1	2002-02-28	Akashi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	5	20020073042	A1	2002-06-13	Maritzen et al.	
	6	20020104006	A1	2002-08-01	Boate et al.	
	7	20020108049	A1	2002-08-08	Xu et al.	
	8	20020109580	A1	2002-08-15	Shreve et al.	
	9	20030055689	A1	2003-03-20	Block et al.	
	10	20030213840	A1	2003-11-20	Livingston et al.	
	11	20040129787	A1	2004-07-08	Saito et al.	
	12	20050090200	A1	2005-04-28	Karaoguz et al.	
	13	20050116020	A1	2005-06-02	Smolucha et al.	
	14	20060111955	A1	2006-05-25	Winter et al.	
	15	20060136742	A1	2006-06-22	Giobbi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	16	20060208066	A1	2006-09-21	Finn et al.	
	17	20070159994	A1	2007-07-12	Brown et al.	
	18	20070174809	A1	2007-07-26	Brown et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	WO 2000/062505	WO	A1	2000-10-19	Thomson Multimedia		☐
	2	WO 2001/022724	WO	A1	2001-03-29	Thomson Multimedia		☐
	3	WO 2001/075876	WO	A1	2001-10-11	Thomson Multimedia		☐
	4	WO 2001/077790	WO	A1	2001-10-18	Thomson Multimedia		☐
	5	WO 2005/050450	WO	A1	2005-06-02	Margent Development, LLC		☐
	6	WO 2005/086802	WO	A2	2005-09-22	Margent Development, LLC		☐

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

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.	T5
	1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pages.	☐
	2	Antonoff, Michael, "Visiting Video Valley," Sound & Vision, pp. 116 and 118-119, Nov. 2001.	☐
	3	"Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002 [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.securitymagazine.comlCDA/Articles/ Technologies/3ae61Oeaa34d801OVgnVCM100000f932a8cO-> 5 pages.	☐
	4	Article, "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, Jul. 24, 2000, 2 pages.	☐
	5	Article, "Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, Aug. 14, 2000, 2 pages.	☐
	6	Blum, Jonathan, "Digital Rights Management May Solve the Napster "Problem"," Technology Investor Industry Sector, (Oct. 2000), 24-27.	☐
	7	Brown, D, Techniques for Privacy and Authentication in Personal Communication Systems; Personal Communications, IEEE; Vol. 2, Issue: 4 Publication Year: 1995, pp. 6-10.	☐
	8	Dagan (Power over Ethernet (PoE) Midspan-The Smart Path to Providing Power for IP Telephony Author: Sharon Dagan, Product Manager, Systems Aug. 2005, PowerDsine Inc.), 28 pages.	☐
	9	Debow, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p10, Nov. 1989, 4 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	10	Dennis, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, Dec. 2, 1999, 2 pages.	☐
	11	Fasca, Chad, "The Circuit," Electronic News, 45(45) (Nov. 8, 1999), 20 pages.	☐
	12	Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, Jan. 18, 1996, 2 pages.	☐
	13	"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.biopay.comlfaqs-lowes.asp>, 5 pages.	☐
	14	Generation of keys for use with the digital signature standard (DSS) ; Nel, J.J.; Kuhn, G.J.; Communications and Signal Processing, 1993., Proceedings of the 1993 IEEE South African Symposium on Publication Year: 1993, pp. 6-11.	☐
	15	"IEEE 802.15.4-2006-Wikipedia, the free encyclopedia," Wikipedia®, Last Modified Mar. 21, 2009 [Online] [Retrieved on Apr. 30, 2009] Retrieved from the Internet <URL:http://en.wikipedia.org/wiki/IEEE_802.15.4-2006>, 4 pages.	☐
	16	Lake, Matt, "Downloading for Dollars," Sound & Vision, (Nov. 2000), pages 137-138.	☐
	17	Lewis, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, Nov. 16, 1995, 1 page.	☐
	18	McIver, R. et al., "Identification and Verification Working Together," Bioscrypt™, Aug. 27, 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.ibia.org/ membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>, 5 pages.	☐
	19	Nilsson, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise% 20Match-onCard%20for%20Java%20Cards.pdf>, 5 pages.	☐
	20	Nordin, B., "Match-On-Card Technology," Precise™ Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.ibia.org/ Membersadmin/whitepapers/pdf/17 IPrecise%20Match-onCard%20technology.pdf>, 7 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	21	Notification of the International Search Report and Written Opinion, PCT/US04/38124, Apr. 7, 2005, 10 pages.	☐
	22	Paget, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, (Dec. 1999), 4 pgs.	☐
	23	PCT International Search Report and Written Opinion, PCT/US07/11105, Oct. 20, 2008, 10 pages.	☐
	24	PCT International Search Report and Written Opinion, PCT/US07/11103, Apr. 23, 2008, 9 pages.	☐
	25	PCT International Search Report and Written Opinion, PCT/US05/43447, Feb. 22, 2007, 7 pages.	☐
	26	PCT International Search Report and Written Opinion, PCT/US05/46843, Mar. 1, 2007, 10 pages.	☐
	27	PCT International Search Report and Written Opinion, PCT/US07/00349, Mar. 19, 2008, 10 pages.	☐
	28	Personal Servers as Digital Keys; Beaufour, A.; Bonnet, P.; Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on Publication Year: 2004, pages 319-328.	☐
	29	Press Release, "Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, Jan. 8, 2002, 3 pages.	☐
	30	Press Release, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002, 2 pages.	☐
	31	Press Release, "Thompson Bets on Smart Cards for Video Encryption," www.informationweek.com. Jun. 7, 2001, 1 page.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

	32	Press Release, "Thompson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com May 30, 2001, 2 pages.	☐
	33	"SAFModule™: A Look Into Strong Authentication," saflink Corporation, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pages.	☐
	34	Sapsford, Jathon, "E-Business: Sound Waves Could Help Ease WebFraud Woes," Wall Street Journal, (Aug. 14, 2000), B1, 2 pages.	☐
	35	"Say Hello to Bluetooth," Bluetooth Web site, 5 pages [Last retrieved on March 25, 2008].	☐
	36	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>, 7 pages.	☐
	37	Van Winkle, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, (Jan. 2000), pp. 148-153.	☐
	38	Wade, W., "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, Apr. 21, 2003, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.biometricgroup.comlin_the_news/04.21.03.html>, 3 pages.	☐
	39	Wallace, Bob, "The Internet Unplugged," InformationWeek, 765(22), (Dec. 13, 1999), pp. 22-24.	☐
	40	Weber, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, (Jul. 24, 2000), B1, 2 pages.	☐
	41	Non-Final Office Action, U.S. Appl. No. 11/939,451, Dated: May 12, 2010, 12 pages.	☐
If you wish to add additional non-patent literature document citation information please click the Add button Add			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

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	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Paige Alsbury/	Date (YYYY-MM-DD)	2014-12-04
Name/Print	Paige M. Alsbury	Registration Number	72,965

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 07 APR 2005
Applicant's or agent's file reference 2012.008WO1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/38124	International filing date (*day/month/year*) 15 November 2004 (15.11.2004)
Applicant MARGENT DEVELOPMENT, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

   For **more detailed instructions**, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer for Gilberto Barron Telephone No. 571-272-3799

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

P 220

Schwegman, Lundberg
Woessner & Kluth, P.A.
APR 18 2005
CMG RECEIVED

RECEIVED
APR 11 2005
PORTFOLIO IP

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference 2012.008WO1	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/38124	International filing date (*day/month/year*) 15 November 2004 (15.11.2004)
Applicant MARGENT DEVELOPMENT, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer for Michelle L. Eason Gilberto Barron Telephone No. 571-272-3799

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PORTFOLIO I.P.
APR 1 1 2005

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 2012.008WO1	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US04/38124	International filing date (*day/month/year*) 15 November 2004 (15.11.2004)	(Earliest) Priority Date (*day/month/year*) 17 November 2003 (17.11.2003)

Applicant
MARGENT DEVELOPMENT, LLC

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

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

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
      ☐ The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

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

   D ✓ 5/7/05

6. With regard to the **drawings**,
   a. the figure of the drawings to be published with the abstract is Figure No. 2
      ☐ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☒ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/38124

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d)).

NEW ABSTRACT

A Personal Digital Key Digital Content Security System (PDK-DCSS) is used to protect computers from unauthorized use and protect the digital content (110) stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are 1) a standard hard drive device (108), with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and 2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: 1) hard drive (108) access control for providing Drive-Level and Sector-Level protection and 2) operating system-level independent file protection for providing File-Level and Network-Level protection.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/38124

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30
US CL : 713/193
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/193

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,385,596 B1 (WISER et al) 07 May 2002, fig. 1b block 106,120,130 and associated text; col.4, lines 3-13; col.3, lines 5-10; col.4, lines 12-27, 51-67; col.5, lines 11-17; fig.2 and 4,9b-13 and associated text; col.8, lines 46-56; col.18, lines 66-67; col.19, lines 1-25;col.6, lines 4-65.	1-4,7-12-14, 17-20
Y	PAGET, THE SECURITY BEHIND SECURE EXTRANETS,ENTERPRISE SYSTEM JOURNAL,14,12,74, December 1999. entire reference	1-4, 7-14 and 17-20
Y	US 6,632,992 B2 (HASEGAWA) 14 October 2003, col.3, lines 22-39.	3 and 13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	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)

ATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
CHARLES E. STEFFEY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	07 APR 2005
Applicant's or agent's file reference 2012.008WO1	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US04/38124	15 November 2004 (15.11.2004)	17 November 2003 (17.11.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): G06F 11/30 and US Cl.: 713/193

Applicant

MARGENT DEVELOPMENT, LLC

1. This opinion contains indications relating to the following items:

- [X] Box No. I — Basis of the opinion
- [ ] Box No. II — Priority
- [ ] Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- [ ] Box No. IV — Lack of unity of invention
- [X] Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI — Certain documents cited
- [ ] Box No. VII — Certain defects in the international application
- [ ] Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

06/07/05

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer for Michelle A. Cox Gilberto Barron Telephone No. 703-305-3900

Form PCT/ISA/237 (cover sheet) (January 2004)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material

      ☐ in written format

      ☐ in computer readable form

   c. time of filing/furnishing

      ☐ contained in international application as filed.

      ☐ filed together with the international application in computer readable form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-20	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	5, 6, 15 and 16	YES
	Claims	1-4, 7-14 and 17-20	NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims	NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1, 2, 4, 7-12, 14, 17-20 lacks an inventive step under PCT Article 33(3) as being obvious over Wiser et al (6, 385, 596 B1) in view of Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999).

As per claims 1, 2, 4, 7-12, 14 and 17-20 Wiser et al (6, 385, 596 B1) teach a method, system of securing a hard drive (see fig.1b, blocks 106, 120 and 130; col.4, lines 3-13) of a computer, comprising: detecting a key with a receiver/decoder circuit associated with the hard drive; validating the detected key with the receiver/decoder circuit; and permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected key is validated (see col.3, lines 5-10; col.4, lines 15-18 where the passport corresponds to Applicant's key; col.4, lines 12-27, 51-67; col.5, lines 11-17; col.8, lines 46-56 where decryption process is being done and where the decoding or decrypting circuit is inherent part of the system in order to do the decoding and decryption; Also see the entire reference for more detail);wherein the receiver/decoder circuit resides in the computer (see fig.9b-13 and associated text); wherein the validating step includes determining whether or not the detected key is associated with the hard drive (see fig 1b and associated text; col.3, lines 37-39; col.5, lines 11-17; col.18, lines 66-67 and col.19, lines 1-25); wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive in order to provide sector-level protection (see col.6, lines 4-65; fig.9b and associated text where the storing corresponds to applicant's write and retrieving media files corresponds to applicant's read); wherein the key associated with the hard drive is initially delivered with the hard drive (see fig.2-4 and associated text); wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer (see fig.1b; 2 and associated text); wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to perform the detecting, validating, and decrypting steps (see abstract; col.3-4); wherein the validating step includes determining whether or not the detected key is associated with the file (fig.1b, 2 and associated text; col.3-4). but do not explicitly disclose the key is a physical, portable key. However Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999) disclose the key is a physical portable key (see the entire reference pages with close attention to where the passport and digital certificate that contains the key are installed on a smart card on the second page where examiner considers such smart card as corresponding to Applicant's physical, portable key). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Paget's portable key such as the smart card in Wiser's secure access to on-line music files on the storage (hard disk) in order to extends extranet access and authority to users based on their roles and business privileges, while ensuring confidentiality and integrity of the data users send, receive and access
Claims 3 and 13 lacks an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hasegawa (6,632,992 B2).

As per claims 3 and 13 Wiser et al (6, 385, 596 B1) in view of Paget (The security behind Secure Extranets, Enterprise System Journal, 14, 12, 74, December 1999) teach all limitation of the method, system of claims 1, 9, 17 and 22 as applied above but do not explicitly disclose wireless communication. However Hasegawa (6,632,992 B2) wireless communication (see col.3, lines 22-39). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Hasegawa's wireless communication in Wiser's secure access to on-line music files on the storage (hard disk) in view of Paget's portable key such as the smart card in order to extends extranet access and authority to users based on their roles and business privileges, while ensuring confidentiality and integrity of the data users send, receive and access without the use of wires or cables.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/38124

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Claims 5, 6, 15 and 16 meets the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest disabling of the storage or hard-disk in case of non validation of the physical key.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 20 OCT 2008
Applicant's or agent's file reference 11744 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/11105	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	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 31 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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

A system and method provide efficient, secure, and highly reliable authentication for transaction processing and/or access control applications. A Personal Digital Key stores one or more profiles(e.g., a biometric profile) in a tamper-proof memory that is acquired in a secure trusted process. Biometric profiles comprise a representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK(102). The PDK wirelessly transmits the biometric profile over a secure wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric wireless transaction to a Reader(108) for use in a biometric authentication process. The Reader compares the received biometric profile to a biometric input(104) acquired at the point of transaction in order to determine if the transactionshould be authorized.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01);**H04L 9/32**(2006.01)

USPC: 713/182,186;726/2;380/270
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182,186; 726/2;380/270

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 7,249,177 B(MILLER) 24 July 2007 (24.07.2007), column 3 lines 28-42; column 4,lines 19-25; column 5,lines 1-17	1-42
A	US 6,070,796 A(SIRBU) 06 June 2000 (06.06.2000), column 7,lines 7-40; column 9,lines 25-55.	1-42
X	US 6,850,147 B(PROKOSKI et al) 01 February 2005 (01.02.2005), column 4,lines 39-62; column 6,lines 46-67; column 11,lines 1-22.	1-42

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2008 (30.09.2008)	20 OCT 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Hosuk Song Telephone No. 5712722100

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11105

Continuation of B. FIELDS SEARCHED Item 3:
EAST, foreign patent databse
search terms: biometric, fingerprint,iris,key, password, wireless, authentication, authorization,access,control,tamper-proof,memory,storage.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

PALM Tracking Number = 51711105

PCT

NOTIFICATION OF RECEIPT
OF SEARCH COPY

(PCT Rule 25.1)

Date of mailing *(day/month/year)*	06 Aug 2007
Applicant's or agent's file reference: 11744 PCT	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011105	07 May 2007	05 May 2006

Applicant

PROXENSE, LLC

1. Where the International Searching Authority and the receiving Office are not the same Office:
The applicant is hereby notified that the search copy of the international application was received by this International Searching Authority on the date indicated below.

Where the International Searching Authority and the receiving Office are the same Office:
The applicant is hereby notified that the search copy of the international application was received on the date indicated below.

06 Aug 2007 *(date of receipt).*

2. ☐ The search copy was accompanied by a nucleotide and/or amino acid sequence listing or tables related thereto in computer readable form.

3. Time limit for establishment of international search report and written opinion of the International Searching Authority
The applicant is informed that the time limit for establishing the international search report and the written opinion of the International Searching Authority is three months from the date of receipt indicated above or nine months from the priority date, whichever time limit expires later (Rules 42.1 and 43*bis*.1(a)).

4. A copy of this notification has been sent to the International Bureau and, where the first sentence of paragraph 1 applies, to the receiving Office.

Name and mailing address of the ISA/	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Arnessa Smith
Facsimile No. 571-273-3201	Telephone No. 703- 308-9290 EX 138

Form PCT/ISA/202 (January 2004)

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

To:

GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

PCT

NOTIFICATION CONCERNING PAYMENT OF PRESCRIBED FEES

(PCT Rules 14, 15 and 16 and Administrative Instructions, Sections 102*bis*(c), 304, 323(b), 707(b) and 803)

Date of mailing *(day/month/year)*	06 Aug 2007
Applicant's or agent's file reference: 11744 PCT	PAYMENT DUE: see item 3 for time limits

International application No.	International filing date/Date of receipt *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011105	07 May 2007	05 May 2006

Applicant: PROXENSE, LLC

1. The applicant is hereby notified that this receiving Office has received:

☒ the payment of all the prescribed fees, and ☐ an overpayment, which will be refunded in due course.

☐ no or insufficient payment of the prescribed fees and the applicant is hereby invited to pay the balance due, as summarized under item 2, within the time limit(s) indicated under item 3.

2. Fees and payment calculation:

1,950.00	–	1,950.00	=	0.00
Total fees payable		Amount paid		Balance

☐ The details of the calculation are given in the Annex.

3. Time limit(s) for payment and amount(s) payable (Rules 14.1, 15.4 and 16.1(f)):

☐ within ONE MONTH from the date of receipt of the international application (for the transmittal fee (if any), the search fee and the international filing fee). The amount payable for each fee is the amount applicable on the date of receipt of the international application.

☐ within 16 MONTHS from the priority date (only for the fee for priority document). The applicant's attention is drawn to the fact that the request made by the applicant under Rule 17.1(b) will be considered not to have been made unless the fee is paid within that time limit.

4. Additional observations *(if necessary)*:

☐ The search copy will not be transmitted to the International Searching Authority until the search fee is paid (therefore the start of the international search will be delayed) (Rule 23.1(a) and (b)).

Name and mailing address of the receiving Office	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Arnessa Smith
Facsimile No. 571-273-3201	Telephone No. 703- 308-9290 EX 138

Form PCT/RO/102 (January 2004)

ANNEX TO FORM PCT/RO/102
CALCULATION OF THE PRESCRIBED FEES

International application No.
PCT/US2007/011105

T Transmittal Fee

Prescribed amount: . . . . . 300.00 T
Amount paid: . . . . . – 300.00
Balance: . . . . . = 0.00

☒ correct amount
☐ overpayment
☐ balance due

S Search Fee

Prescribed amount: . . . . . 300.00 S
Amount paid: . . . . . – 300.00
Balance: . . . . . = 0.00

☒ correct amount
☐ overpayment
☐ balance due

I International Filing Fee

Fixed amount for first 30 sheets: 1,086.00 i1

12 (Number of sheets in excess of 30) x 12.00 (Fee per sheet) = 144.00 i2

Additional component: . . . 400 x 0.00 (Fee per sheet) = 0.00 i3

Reduction where the international application is filed *(See PCT Applicant's Guide, Volume I, General Part, for details on the availability of this reduction)*:

using the PCT-EASY software: . . . . . – 0.00 r

or

in electronic form where the text of the description, claims and abstract is not in character coded format: . . . . . – 0.00 r

or

in electronic form where the text of the description, claims and abstract is in character coded format: . . . . . – 0.00 r

Sub-total: . . . . . = 1,230.00 i1+i2+i3-r

Prescribed total amount *(The amount to be entered at I is the sub-total entered at* (i1+i2+i3-r)*, except where the applicant is (or all applicants are) entitled to a reduction of 75%, in which case the amount to be entered at I is 25% of the sub-total* (i1+i2+i3-r)*; certain applicants from certain States are entitled to a reduction of 75% of the international filing fee; see Notes to the Fee Calculation Sheet as annexed to the Request Form, PCT/RO/101, for details)*: . . . . . = 1,230.00 I

Amount paid: . . . . . – 1,230.00
Balance: . . . . . = 0.00

☒ correct amount
☐ overpayment
☐ balance due

P Fee for Priority Document

Prescribed amount: . . . . . 120.00 P
Amount paid: . . . . . – 120.00
Balance: . . . . . = 0.00

☒ correct amount
☐ overpayment
☐ balance due

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

Confirmation No: 7923

PCT

NOTIFICATION OF THE INTERNATIONAL APPLICATION NUMBER AND OF THE INTERNATIONAL FILING DATE

(PCT Rule 20.2(c))

Date of mailing *(day/month/year)*	06 Aug 2007
Applicant's or agent's file reference: 11744 PCT	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011105	07 May 2007	05 May 2006

Applicant: PROXENSE, LLC

Title of the invention: TWO-LEVEL AUTHENTICATION FOR SECURE TRANSACTIONS

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.

2. The applicant is further notified that the record copy of the international application:

☒ was transmitted to the International Bureau on 06 Aug 2007 .

☐ has not yet been transmitted to the International Bureau for the reason indicated below and a copy of this notification has been sent to the International Bureau*:

☐ because the necessary national security clearance has not yet been obtained.

☐ because *(reason to be specified)*:

* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

3. FOREIGN TRANSMITTAL LICENSE INFORMATION Completed by: AS

☐ Additional license for foreign transmittal not required. This subject matter is covered by a license already granted or the equivalent U.S. national application. Refer to that license for information concerning its scope.

☐ License for foreign transmittal not required. 37 CFR. 5.11(e)(1) or 37 CFR 5.11(e)(2). However, a license may be required for additional subject matter. See 37 CFR 5.15(b).

☒ Foreign transmittal license granted. 35 U.S.C. 184; 37 CFR 5.11 on 31 Jul 2007 (date) :

☒ 37 CFR 5.15(a) ☐ 37 CFR 5.15(b)

Name and mailing address of the receiving Office	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Arnessa Smith
Facsimile No. 571-273-3201	Telephone No. 703- 308-9290 EX 138

Form PCT/RO/105 (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

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 DEBORAH A. THOMAS PARALEGAL SPECIALIST Telephone No. 571 270 9922

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 12786 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/11103	International filing date (*day/month/year*) 07 May 2007 (07.05.2007)	(Earliest) Priority Date (*day/month/year*) 05 May 2006 (05.05.2006)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 2 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 Rule 43.6 *bis(a)*
   c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/11103

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04K 1/00**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPAT, US-PGPUB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0104006 A1 (Boate et al.) 01 August 2002 (01.08.2002), [0011], [0012], [0014], [0027], [0035], [0043].	1-20
A,E	US 7,249,177 B1 (MILLER) 24 July 2007	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 April 2008 (08.04.2008)

Date of mailing of the international search report
23 APR 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
SUMAN DEBNATH
DEBORAH A. THOMAS
PARALEGAL SPECIALIST
Telephone No. 571 270 9922

Form PCT/ISA/210 (second sheet) (April 2007)

PATENT COOPERATION TREATY

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 _____ 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)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

PALM Tracking Number = 51711103

PCT

NOTIFICATION OF RECEIPT
OF SEARCH COPY

(PCT Rule 25.1)

Date of mailing *(day/month/year)*	29 Aug 2007
Applicant's or agent's file reference: 12786 PCT	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011103	07 May 2007	05 May 2006

Applicant

PROXENSE, LLC

1. Where the International Searching Authority and the receiving Office are not the same Office:
The applicant is hereby notified that the search copy of the international application was received by this International Searching Authority on the date indicated below.

Where the International Searching Authority and the receiving Office are the same Office:
The applicant is hereby notified that the search copy of the international application was received on the date indicated below.

29 Aug 2007 *(date of receipt).*

2. ☐ The search copy was accompanied by a nucleotide and/or amino acid sequence listing or tables related thereto in computer readable form.

3. Time limit for establishment of international search report and written opinion of the International Searching Authority
The applicant is informed that the time limit for establishing the international search report and the written opinion of the International Searching Authority is three months from the date of receipt indicated above or nine months from the priority date, whichever time limit expires later (Rules 42.1 and 43*bis*.1(a)).

4. A copy of this notification has been sent to the International Bureau and, where the first sentence of paragraph 1 applies, to the receiving Office.

Name and mailing address of the ISA/	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Misty Walker
Facsimile No. 571-273-3201	Telephone No. 703-308-9290 EX 122

Form PCT/ISA/202 (January 2004)

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

To:

GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

PCT

NOTIFICATION CONCERNING PAYMENT OF PRESCRIBED FEES

(PCT Rules 14, 15 and 16 and Administrative Instructions, Sections 102*bis*(c), 304, 323(b), 707(b) and 803)

Date of mailing *(day/month/year)*	29 Aug 2007
Applicant's or agent's file reference: 12786 PCT	PAYMENT DUE: see item 3 for time limits

International application No.	International filing date/Date of receipt *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011103	07 May 2007	05 May 2006

Applicant: PROXENSE, LLC

1. The applicant is hereby notified that this receiving Office has received:

☒ the payment of all the prescribed fees, and ☐ an overpayment, which will be refunded in due course.

☐ no or insufficient payment of the prescribed fees and the applicant is hereby invited to pay the balance due, as summarized under item 2, within the time limit(s) indicated under item 3.

2. Fees and payment calculation:

2,690.00	–	2,690.00	=	0.00
Total fees payable		Amount paid		Balance

☐ The details of the calculation are given in the Annex.

3. Time limit(s) for payment and amount(s) payable (Rules 14.1, 15.4 and 16.1(f)):

☐ within ONE MONTH from the date of receipt of the international application (for the transmittal fee (if any), the search fee and the international filing fee). The amount payable for each fee is the amount applicable on the date of receipt of the international application.

☐ within 16 MONTHS from the priority date (only for the fee for priority document). The applicant's attention is drawn to the fact that the request made by the applicant under Rule 17.1(b) will be considered not to have been made unless the fee is paid within that time limit.

4. Additional observations *(if necessary)*:

☐ The search copy will not be transmitted to the International Searching Authority until the search fee is paid (therefore the start of the international search will be delayed) (Rule 23.1(a) and (b)).

Name and mailing address of the receiving Office	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Misty Walker
Facsimile No. 571-273-3201	Telephone No. 703-308-9290 EX 122

Form PCT/RO/102 (January 2004)

ANNEX TO FORM PCT/RO/102
CALCULATION OF THE PRESCRIBED FEES

International application No.
PCT/US2007/011103

T Transmittal Fee

Prescribed amount:		300.00 T	
Amount paid:	–	300.00	☒ correct amount
Balance:	=	0.00	☐ overpayment
			☐ balance due

S Search Fee

Prescribed amount:		1,000.00 S	
Amount paid:	–	1,000.00	☒ correct amount
Balance:	=	0.00	☐ overpayment
			☐ balance due

I International Filing Fee

Fixed amount for first 30 sheets:		1,086.00 i1	
17 (Number of sheets in excess of 30) x 12.00 (Fee per sheet)	=	204.00 i2	
Additional component: . . . 400 x 0.00 (Fee per sheet)	=	0.00 i3	
Reduction where the international application is filed *(See PCT Applicant's Guide, Volume I, General Part, for details on the availability of this reduction)*: using the PCT-EASY software:	–	0.00 r	
or in electronic form where the text of the description, claims and abstract is not in character coded format:	–	0.00 r	
or in electronic form where the text of the description, claims and abstract is in character coded format:	–	0.00 r	
Sub-total:	=	1,290.00 i1+i2+i3-r	
Prescribed total amount *(The amount to be entered at I is the sub-total entered at* (i1+i2+i3-r)*, except where the applicant is (or all applicants are) entitled to a reduction of 75%, in which case the amount to be entered at I is 25% of the sub-total* (i1+i2+i3-r)*; certain applicants from certain States are entitled to a reduction of 75% of the international filing fee; see Notes to the Fee Calculation Sheet as annexed to the Request Form, PCT/RO/101, for details)*:	=	1,290.00 I	
Amount paid:	–	1,290.00	☒ correct amount
Balance:	=	0.00	☐ overpayment
			☐ balance due

P Fee for Priority Document

Prescribed amount:		100.00 P	
Amount paid:	–	100.00	☒ correct amount
Balance:	=	0.00	☐ overpayment
			☐ balance due

Form PCT/RO/102 (Annex) (January 2004)

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

To:
GREG T. SUEOKA
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CALIFORNIA 94041

Confirmation No: 8406

PCT

NOTIFICATION OF THE INTERNATIONAL APPLICATION NUMBER AND OF THE INTERNATIONAL FILING DATE

(PCT Rule 20.2(c))

Date of mailing *(day/month/year)*	29 Aug 2007
Applicant's or agent's file reference: 12786 PCT	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2007/011103	07 May 2007	05 May 2006

Applicant: PROXENSE, LLC

Title of the invention: SINGLE STEP TRANSACTION AUTHENTICATION USING PROXIMITY AND BIOMETRIC INPUT

1. The applicant is hereby notified that the international application has been accorded the international application number and the international filing date indicated above.

2. The applicant is further notified that the record copy of the international application:

☒ was transmitted to the International Bureau on 29 Aug 2007 .

☐ has not yet been transmitted to the International Bureau for the reason indicated below and a copy of this notification has been sent to the International Bureau*:

☐ because the necessary national security clearance has not yet been obtained.

☐ because *(reason to be specified)*:

* The International Bureau monitors the transmittal of the record copy by the receiving Office and will notify the applicant (with Form PCT/IB/301) of its receipt. Should the record copy not have been received by the expiration of 14 months from the priority date, the International Bureau will notify the applicant (Rule 22.1(c)).

3. FOREIGN TRANSMITTAL LICENSE INFORMATION Completed by: MW

☐ Additional license for foreign transmittal not required. This subject matter is covered by a license already granted or the equivalent U.S. national application. Refer to that license for information concerning its scope.

☐ License for foreign transmittal not required. 37 CFR. 5.11(e)(1) or 37 CFR 5.11(e)(2). However, a license may be required for additional subject matter. See 37 CFR 5.15(b).

☒ Foreign transmittal license granted. 35 U.S.C. 184; 37 CFR 5.11 on 23 Aug 2007 (date) :

☒ 37 CFR 5.15(a) ☐ 37 CFR 5.15(b)

Name and mailing address of the receiving Office	Authorized officer
Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450	Misty Walker
Facsimile No. 571-273-3201	Telephone No. 703-308-9290 EX 122

Form PCT/RO/105 (April 2007)

PATENT COOPERATION TREATY

RECEIVED
FEB 26 2007
FENWICK & WEST

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

11163/PCT

	Date of mailing (*day/month/year*)
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)
Applicant PROXENSE, LLC	

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

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

   When The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. (571) 272-3600

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

M

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 22 FEB 2007
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. (571) 272-3600

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/43447	International filing date (*day/month/year*) 30 November 2005 (30.11.2005)	(Earliest) Priority Date (*day/month/year*) 01 December 2004 (01.12.2004)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 7 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/43447

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06Q 99/00**(2006.01);**H04K 1/00**(2006.01);**H04L 9/00**(2006.01)

USPC: 705/59
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0109580 A1 (SHREVE ET AL.) 15 AUGUST 2002 (15.08.2002) PARAGRAPKS 0001 TO 0007.	1-55
X	US 2002/0073042 A1 (MARIITZEN ET AL.) 13 JUNE 2002 (13.06.2002) PARAGRAPHS 0001-0005.	1-55
X	US 5,991,749 A (MORRILL, JR) 23 NOVEMBER 1999 (23.11.1999), COLUMN 1 LINE 5-58.	1-55

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 November 2006 (14.11.2006)

Date of mailing of the international search report
22 FEB 2007

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
James Trammel

Telephone No. (571) 272-3600

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

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WASIF H. QURESHI
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	22 FEB 2007
Applicant's or agent's file reference PROXE-72586	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US05/43447	30 November 2005 (30.11.2005)	01 December 2004 (01.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **G06Q 99/00**(2006.01);**H04 K 1/00;H04 L 9/ 00**

USPC: 705/59

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	15 November 2006 (15.11.2006)	James Tramme Telephone No. (571) 272-3600

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/43447

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/43447

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-55	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-55	NO
Industrial applicability (IA)	Claims 1-55	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Morrill, Jr (US 5,991,749 A). Morrill, in at least column 1, lines 25-58 discloses a system for collecting funds by passing within a proximity of a wireless computing and transactional device.

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Maritzen et al. (US 2002/0073042 A1). Maritzen, in at least paragraphs 0001-0006, discloses conducting e-commerce transactions across wireless devices.

Claims 1-55 lack novelty under PCT Article 33(2) as being anticipated by Shreve et al. (US 2002/0109580 A1). Shreve, in at least paragraphs 0001-0007 discloses remote keyless entry devices for granting access to secure domains.

RECEIVED
MAR 15 2007

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT 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*) 01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

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

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)
Applicant PROXENSE, LLC	

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

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

   For more detailed instructions, see the notes on the accompanying sheet.

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

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

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

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

4. **Reminders**

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

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

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

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

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/46843	International filing date (*day/month/year*) 20 December 2005 (20.12.2005)	(Earliest) Priority Date (*day/month/year*) 20 December 2004 (20.12.2004)
Applicant PROXENSE, LLC		

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

This international search report consists of a total of 2 sheets.

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

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/46843

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/32**(2006.01)

USPC: 713/186
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/186

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,041,410 (HSU et al), 21 March 2000, Column 4, lines 15-56, Column 5, line 1 to Column 6, line 24, and Column 6, line 42 to Column 7, line 34	1, 4-11, 15, 18 --- 2, 3, 12-14, 16, 17, 19-21
Y	US 2004/0129787 (SAITO et al) 8 July 2004, Paragraphs 40-56, 81-91, 91-101, and 164	2, 3, 12-14, 16, 17, 19-21

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2007 (18.01.2007)	01 MAR 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Emmanuel Moise Telephone No. (571)-305-3900

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

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN T. MCNELIS
FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	01 MAR 2007
Applicant's or agent's file reference 11062 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US05/46843	20 December 2005 (20.12.2005)	20 December 2004 (20.12.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/32**(2006.01)
USPC: 713/186

Applicant

PROXENSE, LLC

1. This opinion contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis(b)* that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	18 January 2007 (18.01.2007)	Emmanuel Moise Telephone No. (571)-305-3900

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 2, 3, 12-14, 16, 17, and 19-21	YES
	Claims 1, 4-11, 15, and 18	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-21	NO
Industrial applicability (IA)	Claims 1-21	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2005)

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

V. 2. Citations and Explanations:
Claims 1, 4-11, 15, and 18 lack novelty under PCT Article 33(2) as being anticipated by Hsu (US 6041410 A) 21 March 2000.

Regarding Claim 1,
Hsu discloses a method for verifying a user during authentication of an integrated device, comprising the steps of:
Persistently storing biometric data for the user in a tamper-resistant format (Column 4, lines 15-25);
Responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan (Column 4, lines 26-56);
Comparing the scan data to the biometric data to determine whether the data match (Column 4, lines 26-56); and
Wirelessly sending a code for authentication (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9).

Regarding Claim 10,
Claim 10 is a device claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 4,
Hsu discloses that the code uniquely identifies the integrated device (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 5,
Hsu discloses that the code indicates that the biometric verification was successful (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 6,
Hsu discloses that persistently storing biometric data comprises permanently storing biometric data (Column 4, lines 15-25; and Column 5, lines 1-47).

Regarding Claim 11,
Claim 11 is a device claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 7,
Hsu discloses that the biometric data and the scan data are both based on a fingerprint scan by the user (Column 4, lines 15-56).

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/46843

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Regarding Claim 8,
Hsu discloses establishing a secure communication channel prior to sending the code for authentication (Column 6, line 42 to Column 7, line 34).

Regarding Claim 9,
Hsu discloses receiving a request for the code without a request for biometric verification (Column 5, line 57 to Column 6, line 24); and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data (Column 5, line 57 to Column 6, line 24).

Regarding Claim 15,
Hsu discloses a method for authenticating a verified user, comprising:
Receiving a code associated with a biometrically verified user (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Requesting authentication of the code (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34);
Receiving an authentication result (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34); and
In response to the authentication result being positive, providing access to an application (Column 5, line 1 to Column 6, line 9; and Column 7, lines 17-34).

Regarding Claim 18,
Hsu discloses establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key (Column 6, line 42 to Column 7, line 34).

Claims 2, 3, 12-14, 16, 17, and 19-21 lack an inventive step under PCT Article 33(3) as being obvious over Hsu in view of Saito (US 20040129787 A1) 8 July 2004.

Regarding Claim 2,
Hsu does not disclose that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority.
Saito, however, discloses that the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 12,
Claim 12 is a device claim that corresponds to method claim 2 and is rejected for the same reasons.

Regarding Claim 3,
Hsu does not disclose registering an age verification for the user in association with the code.
Saito, however, discloses registering an age verification for the user in association with the code (Paragraphs 82, 83, and 164). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 13,
Claim 13 is a device claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 14,
Hsu does not disclose that the verification module comprises an LED to be activated for requesting the biometric scan.
Saito, however, discloses that the verification module comprises an LED to be activated for requesting the biometric scan (Paragraphs 40-56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 16,
Hsu does not disclose registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority.

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

Saito, however, discloses registering the code with a trusted authority, wherein requesting authentication of the code comprises providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 17,
Hsu as modified by Saito does discloses the method of claim 16, in addition, Saito discloses registering a date of birth or age with the trusted authority (Paragraphs 82, 83, and 164).

Regarding Claim 19,
Hsu discloses a system comprising:
A biometric key to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code (Column 4, lines 15-56; and Column 5, line 1 to Column 6, line 9);
An authentication module to authenticate the user for access to an application (Column 7, lines 17-34);
But does not disclose sending the code to a trusted authority for authentication.
Saito, however, discloses an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application (Paragraphs 95-101). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication procedures of Saito into the personal identification fob authentication system of Hsu in order to increase reliability and security of authentication and authorization by providing a trusted entity that can confirm that the user and device are authentic.

Regarding Claim 20,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Column 4, lines 26-56; and Column 5, line 1 to Column 6, line 9); and Saito discloses that the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data (Paragraphs 40-56; and 81-91

Regarding Claim 21,
Hsu as modified by Saito discloses the system of claim 19, in addition, Hsu discloses that if the biometric key cannot verify the scan data as being from the user, it does not send the code (Column 5, lines 1-47).

Fenwick & West LLP

MAR 21 2008

PCT 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

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

(PCT Rule 44.1)

Applicant's or agent's file reference 12194PCT	Date of mailing *(day/month/year)*
	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US07/00349	International filing date *(day/month/year)* 08 January 2007
Applicant PROXENSE, LLC	

25000-

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

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

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 1435

   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: Blaine R. Copenheaver Telephone No. 571-272-7774

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)* 19 MAR 2008
Applicant's or agent's file reference 12194PCT	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US07/00349	International filing date *(day/month/year)* 08 January 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 22 740 1435

   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: Blaine R. Copenheaver Telephone No. 571-272-7774

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 12194PCT	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US07/00349	International filing date *(day/month/year)* 08 January 2007	(Earliest) Priority Date *(day/month/year)* 06 January 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. 4

   ☒ 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/US07/00349

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Extra Sheet (page 10)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-16 and 31

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/00349

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04Q 7/20 (2008.01)
USPC - 455/41.2
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(8) - H04Q 7/20 (2008.01)
USPC - 455/41.2, 455/502

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)
Patbase, Pubwest

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2005/0090200 A1 (KARAOGUZ et al) 28 April 2005 (28.04.2005) entire document	1-6,8-9,12-16,31 --- 7, 10, 11
Y	US 6,879,567 B2 (CALLAWAY et al) 12 April 2005 (12.04.2005) entire document	7, 10, 11
A	US 6,957,086 B2 (BAHL et al) 18 October 2005 (18.10.2005) entire document	1-16, 31

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 February 2008	19 MAR 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: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US07/00349

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-16 and 31, drawn to a system and apparatus configured for communication in a wireless coverage area.
Group II, claims 17-30, 32, 33 and 102-108, drawn to a gaming system, apparatus and method for facilitating data exchange.
Group III, claims 34-59, drawn to a method, apparatus and system facilitating data exchange.
Group IV, claims 60-81, drawn to an apparatus, method and system facilitating wireless data exchange.
Group V, claims 82-101, drawn to a system, method and apparatus facilitating wireless data exchange.

The inventions listed as Groups I-V do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention is a wireless device configured to broadcast synchronization information in a wireless coverage area of a network device to coordinate a data exchange between a first wireless device and a second wireless device located in the wireless coverage area as claimed therein is not present in the invention of Groups II-V; the special technical feature of the Group II invention is arranging to wirelessly detect a presence of a portable wireless user device in proximity to a system as claimed therein is not present in the invention of Groups I and III-V; the special technical feature of the Group III invention is assigning a time slot during which a client device can receive data as claimed therein is not present in the invention of Groups I, II, IV and V; and the special technical feature of the Group IV invention is activating a wireless transceiver from a sleep mode at a beginning of a time slot as claimed therein is not present in the invention of Groups I-III and V; and the special technical feature of the Group V invention is adjusting a wireless coverage range in response to an initiation of a wireless transaction between a reader device and a client device as claimed therein is not present in the invention of Groups I-IV.

Since none of the special technical features of the Group I, II, III, IV and V inventions is found in more than one of the inventions, unity of invention is lacking.

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)*	19 MAR 2008
Applicant's or agent's file reference 12194PCT	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/00349	08 January 2007	06 January 2006

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04Q 7/20 (2008.01)
USPC - 455/41.2

Applicant PROXENSE, LLC

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	01 February 2008	Blaine Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/00349

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the appicable time limit:

   ☐ paid additional fees

   ☐ paid additional fees under protest and, where applicable, the protest fee

   ☐ paid additional fees under protest but the applicable protest fee was not paid

   ☒ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

   ☐ complied with

   ☒ not complied with for the following reasons:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-16 and 31, drawn to a system and apparatus configured for communication in a wireless coverage area.
Group II, claims 17-30, 32, 33 and 102-108, drawn to a gaming system, apparatus and method for facilitating data exchange.
Group III, claims 34-59, drawn to a method, apparatus and system facilitating data exchange.
Group IV, claims 60-81, drawn to an apparatus, method and system facilitating wireless data exchange.
Group V, claims 82-101, drawn to a system, method and apparatus facilitating wireless data exchange.

The inventions listed as Groups I-V do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention is a wireless device configured to broadcast synchronization information in a wireless coverage area of a network device to coordinate a data exchange between a first wireless device and a second wireless device located in the wireless coverage area as claimed therein is not present in the invention of Groups II-V; the special technical feature of the Group II invention is arranging to wirelessly detect a presence of a portable wireless user device in proximity to a system as claimed therein is not present in the invention of Groups I and III-V; the special technical feature of the Group III invention is assigning a time slot during which a client device can receive data as claimed therein is not present in the invention of Groups I, II, IV and V; and the special technical feature of the Group IV invention is activating a wireless transceiver from a sleep mode at a beginning of a time slot as claimed therein is not present in the invention of Groups I-III and V; and the special technical feature of the Group V invention is adjusting a wireless coverage range in response to an initiation of a wireless transaction between a reader device and a client device as claimed therein is not present in the invention of Groups I-IV.

Since none of the special technical features of the Group I, II, III, IV and V inventions is found in more than one of the inventions, unity of invention is lacking.

4. Consequently, this opinion has been established in respect of the following parts of the international application:

   ☐ all parts

   ☒ the parts relating to claims Nos. 1-16 and 31

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

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/00349

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	7, 10, 11	YES
	Claims	1-6,8-9,12-16,31	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-16,31	NO
Industrial applicability (IA)	Claims	1-16,31	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-6,8-9,12-16 and 31 lack novelty under PCT Article 33(2) as being anticipated by Karaoguz et al. (US 2005/0090200; hereinafter Karaoguz).

Referring to claim 1, Karaoguz discloses a system, comprising: a first wireless device having a first range of wireless coverage (see par. 0015, note the piconet and devices); a second wireless device having a second range of wireless coverage (see par. 0016, note the second plurality of devices); and a synchronization device having a third range of wireless coverage and configured for communication with the first wireless device and the second wireless device, wherein an operation of the first fixed wireless device (see par. 0015, note the piconet coordinator) and an operation of the second fixed wireless device are coordinated based on synchronization information wirelessly broadcast by the synchronization device (see par. 0060, note the synchronized message).

Referring to claim 2, Karaoguz (as discussed in the lack of novelty of claim 1 above) discloses wherein the first range and the second range of wireless coverage at least partially overlap (see fig. 9, also see par. 0075, note the proximity).

Referring to claim 3, Karaoguz discloses wherein an operation of a portable wireless device located in at least one of the first range and the second range is coordinated using the synchronization information (see par. 0075, note the proximity, also see par. 0076, note the piconet devices).

Referring to claim 4, Karaoguz discloses wherein one of the first fixed wireless device and the second fixed wireless device is arranged to communicate with another of the first fixed wireless device and the second fixed wireless device (see par. 0092, note the devices and the arrangement).

Referring to claim 5, Karaoguz discloses wherein at least one of the first fixed wireless device and the second fixed wireless device (see par. 0015, note the piconet and devices) comprises: a first wireless transceiver arranged to continuously monitor broadcasts by the synchronization device (see par. 0015, note the piconet coordinator); and a second wireless transceiver arranged to wirelessly communicate with a portable wireless user device in proximity to the at least one of the first fixed wireless device and the second fixed wireless device (see par. 0075, note the proximity).

Referring to claim 6, Karaoguz discloses wherein at least one of the first fixed wireless device and the second fixed wireless device (see par. 0015, note the piconet and devices) comprises: a single transceiver arranged to periodically monitor broadcasts by the synchronization device (see par. 0015, note the piconet coordinator, also see par. 0060, note the synchronized message) and further arranged to wirelessly communicate with a portable wireless user device in proximity to the at least one of the first fixed wireless device and the second fixed wireless device (see par. 0075, note the proximity).

Referring to claim 8, Karaoguz discloses a central server configured to gather information from the first fixed wireless device and the second fixed wireless device (see par. 0044, note the piconet coordinator).

Referring to claim 9, Karaoguz (as discussed in the lack of novelty of claim 8 above) discloses wherein the central server is operatively connected to at least one of the first fixed wireless device and the second fixed wireless device via a wired connection (see par. 0016, note the second plurality of devices, also see par. 0084, note the wired connection).

Referring to claim 12, Karaoguz discloses wherein at least one of the first fixed wireless device and the second fixed wireless device is arranged to simultaneously detect presence of a plurality of portable wireless user devices in proximity to the at least one of the first fixed wireless device and the second fixed wireless device (see par. 0016, note the second plurality of devices , also see par. 0075, note the proximity).

(Cont. in Supplemental Box)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/00349

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box No. V
2. Citations and explanations:

Referring to claim 13, Karaoguz (as discussed in the lack of novelty of claim 12 above) discloses wherein the at least one of the first fixed wireless device and the second fixed wireless device is further arranged to differentiate among the plurality of simultaneously detected portable wireless user devices (see par. 0087, note the grouping).

Referring to claim 14, Karaoguz wherein the at least one of the first fixed wireless device and the second fixed wireless device is further arranged to coordinate a plurality of data exchanges with the plurality of simultaneously detected portable wireless user devices (see par. 0016, note the second plurality of devices , also see par. 0075, note the proximity).

Referring to claim 15, Karaoguz (as discussed in the lack of novelty of claim 14 above) discloses discloses wherein the plurality of data exchanges is coordinated based on the synchronization information (see par. 0060, note the synchronized message).

Referring to claim 16, Karaoguz discloses wherein the synchronization device is a standalone device (see par. 0092, note the device).

Referring to claim 31, Karaoguz discloses an apparatus, comprising: a predetermined network device, wherein the network device (see par. 0015, note the piconet and devices) comprises: a wireless transmitter configured to broadcast synchronization information in a wireless coverage area of the network device to coordinate a data exchange between a first wireless device and a second wireless device located in the wireless coverage area (see par. 0015, note the piconet coordinator, also see par. 0075, note the proximity).

Claims 7, 10 and 11 lack an inventive step under PCT Article 33(3) as being obvious over Karaoguz in view of Callaway et al. (US 6,879,567 B2; hereinafter Callaway).

Referring to claim 7, Karaoguz (as discussed in the lack of novelty of claim 1 above) is silent on wherein the synchronization device is arranged to broadcast a security update. However, in disclosing nodes within a communication system, Callaway teaches wherein the synchronization device is arranged to broadcast a security update (see col. 4 lines 32-40, note the security). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein the synchronization device is arranged to broadcast a security update in the invention of Karaoguz as taught by Callaway in order to have message encryption and integrity of the communication (see col. 4 lines 32-40).

Referring to claim 10, Karaoguz (as discussed in the lack of novelty of claim 1 above) is silent on wherein a wireless communication in the system is dependent on an IEEE 802.15.4 protocol. However, in disclosing nodes within a communication system, Callaway teaches a wireless communication in the system is dependent on an IEEE 802.15.4 protocol (see col. 4 lines 14-23, note the IEEE 802.15.4 protocol). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to include a wireless communication in the system is dependent on an IEEE 802.15.4 protocol in the invention of Karaoguz as taught by Callaway in order to support low power wireless personal area network.

Referring to claim 11, Karaoguz (as discussed in the lack of novelty of claim 1 above) is silent on wherein use of a service provided by the system is accessible with a portable wireless device, wherein successful access depends at least partially on a security mechanism provided in at least one of the first fixed wireless device and the second fixed wireless device. However, in disclosing nodes within a communication system, Callaway teaches wherein use of a service provided by the system is accessible with a portable wireless device, wherein successful access depends at least partially on a security mechanism provided in at least one of the first fixed wireless device and the second fixed wireless device (see col. 4 lines 32-40, note the security). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to include wherein use of a service provided by the system is accessible with a portable wireless device, wherein successful access depends at least partially on a security mechanism provided in at least one of the first fixed wireless device and the second fixed wireless device in the invention of Karaoguz as taught by Callaway in order to have message encryption and integrity of the communication (see col. 4 lines 32-40).

Claims 1-16 and 31 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.

Personal Servers as Digital Keys

Allan Beaufour, Philippe Bonnet
Department of Computer Science
University of Copenhagen
beaufour@diku.dk, bonnet@diku.dk

Abstract

Personal servers are an attractive concept: People carry around a device that takes care of computing, storage and communication on their behalf in a pervasive computing environment. So far personal servers have mainly been considered for accessing personal information. In this paper, we consider personal servers in the context of a digital key system. Digital keys are an interesting alternative to physical keys for mail or good delivery companies whose employees access tens of private buildings every day. In this paper, we present a digital key system tailored for the current incarnation of personal servers, i.e., a Bluetooth-enabled mobile phone. We describe how to use Bluetooth for this application, we present a simple authentication protocol and we provide a detailled analysis of response time and energy consumption on the mobile phone.

1. Introduction

Intel and HP are promoting the concept of *personal server* [11, 20]. People carry around their personal server, a small device that takes care of storage, computing, and communication on their behalf in a pervasive computing environment. Mobile phones with extended functionalities or PDAs enhanced with communication capabilities are the current incarnation of the personal server. Ideally, a personal server should be small-scale so that people can carry it easily; it should avoid consuming too much energy so that it can run for several days; it should be efficient to ensure good response time and thus a nice user experience.

So far personal servers have been essentially considered as a means to access personal information in an ubiquitous manner. In this paper, we consider a natural extension of the personal server functionalities: *the personal server as a digital key*.

First, why consider digital keys? What is wrong with the good old physical keys? We use them every day to unlock doors. It is a well-known and well-tested technology. This being said, we have all experienced problems like carrying too many keys while forgetting the one key we need, or maybe having a lock replaced because we lost a single key.

The problems with physical keys are strategic for companies in the business of mail or goods delivery. These companies need access to many different private buildings – doors spread over a wide geographical area and governed by many different owners. Personnel need to carry keys for each single door on the delivery route. Carrying all these keys (literally kilograms) is a hassle in the daily use. But just as important, routes, personnel, and locks change over time, making it a resource consuming operation to assure that all personnel have the right keys at the right time.

Consider the following scenario. In the morning, a mailman downloads the route she is going to follow for the day (a mailman can be assigned various routes depending on the deliveries and on the staff available). The digital keys she needs are uploaded to her personal server. Whenever she approaches a door dur-

Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications (PERCOM'04)
0-7695-2090-1/04 $ 20.00 © 2004 IEEE

IEEE COMPUTER SOCIETY

ing her tour, the appropriate key is transfered to the lock automatically, without physical contact and without user interaction. The automatic unlocking makes it possible for the mailman to unlock the door while carrying goods, making the system very user-friendly.

Replacing the physical keys with digital keys managed by a personal server has the following advantages: A digital key can easily be distributed to users, it can be specialized for each user so each key will be unique, and it can be restricted to a given time or date range to increase security. Moreover, many such digital keys can be contained in a personal server. Several companies have expressed commercial interests in such digital key systems and it is not unreasonable to expect that most private buildings in large cities will be equipped with such systems in a near future.

We propose to use a mobile phone equipped with Bluetooth as a personal server. Mobile phones are getting very common and bringing your mobile phone with you is becoming as natural as bringing your keys. Combined with the ability to run custom applications and to perform short-range wireless communications via Bluetooth, the mobile phone is a good candidate to become a personal server. There are some unknowns however: Can the functionality of a digital key system be implemented on a Bluetooth-enabled mobile phone? If yes, is the platform efficient in terms of response time and resource usage (both in terms of storage and energy)?

In this paper, we describe how a Bluetooth-enabled mobile phone can be used as a personal server in the context of a digital key system. Specifically, we are making the following contributions:

- We present how Bluetooth can be used to establish connections in a digital key system. The major issues are (i) to devise an efficient way to use Bluetooth's device discovery protocol and (ii) to establish connections efficiently when the user enters a building.
- We present a simple, specialized, and secure authentication protocol. Existing general purpose authentication protocols, such as SSH [2], are too complex for our purpose.
- We implemented a prototype digital key system on a Sony Ericsson P800 mobile phone. We present the results of experiments to evaluate response time and energy consumption when running our prototype digital key system. Note that we calibrated energy consumption on the mobile phone under different regimes. Such performance numbers are not available from the constructor or in the litterature. They provide a reference for further studies on personal servers.

Before discussing these contributions in Section 3, Section 4 and Section 5 respectively, we precise the application context. We discuss related work in Section 6.

2. Digital Key System

Ideally, a user carrying mail or goods as her personal server running the digital key application should not have to worry about anything but pushing the door open. More specifically, the digital key system should be:

- *secure*: access to a door should be limited to authorized persons
- *easy-to-use*: access to a door should be granted without user interaction
- *efficient*: a user should not have to wait more than 5 seconds for a door to open (an arbitrary yet reasonable target)

In terms of architecture, the digital key system we consider has three components (see Figure 1):

Lock Device A fixed device, attached to the physical lock unit. The lock device is an actuator that can open the physical lock. It is equipped with storage and computation capabilities as well as a Bluetooth radio. It can thus establish local connections. The lock device is not connected to a LAN or a WAN, to simplify installation and management and to eliminate running costs. The lock device is externally powered as it is fixed and located in a building connected to the power grid. The design of a lock device is beyond the

IEEE COMPUTER SOCIETY

scope of this paper (BTNodes developed at ETH Zurich[10] are a good approximation of what lock devices could be).

Personal Server The mobile phone acting as a personal server can communicate with the lock device via Bluetooth.

External Authority A third party responsible for generating the digital keys. It can communicate with the personal server and is trusted by the lock device. No direct communication with the lock device is possible. Key distribution from the external authority to the personal servers is beyond the scope of this paper.

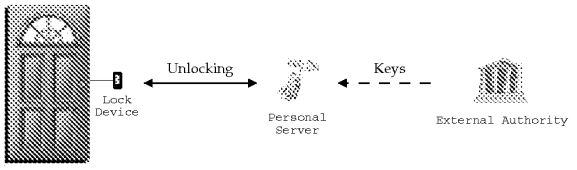


Figure 1: Digital Key System Architecture

3. Bluetooth Connections

Bluetooth requires devices to establish a connection before they can exchange data. This is a constraint from a performance point of view: devices first need to discover each other before they can establish a connection and then exchange data. This is time and energy consuming.

Bluetooth device discovery is a powerful mechanism. It allows connections to be established between devices that have no a priori knowledge of each other. In the discovery phase, one of the devices transmits search requests, *inquiry*, while the other listens for these requests, *inquiry scan*. Inquiry is an expensive operation in terms of energy consumption: an inquiring device broadcasts inquiry packets continuously during the entire inquiry period (i.e., 1.28 seconds). In contrast, a device doing inquiry scan with default parameters only listens for inquiry messages for 11.25 ms every period. This qualitative analysis is confirmed by our calibration of the mobile phone (see Section 5.2).

The Bluetooth specification recommends performing inquiry for 10.24 seconds to assure that all devices present in the vicinity are found [5, Part B, 10.7.3]. Practical experiments show that 99 percent of all discoveries are successful after approximately 6 seconds (2.3 seconds on average) [10, 12]. These numbers are large compared to our goal of five seconds for opening a door.

A first issue for our digital key system is when and how to perform inquiries. The first approach is to let the lock device perform inquiry scan. This seems like the most natural approach: the personal server moves around and discovers the lock device it needs to communicate with to unlock a door. One problem though is that performing inquiry is more energy consuming than performing inquiry scan. Another problem is that doing constant inquiries ties up the Bluetooth chip on the personal server, making it unavailable for other purposes. Letting the lock device perform inquiries solves these problems (there is no power limitation on the lock device and it does not need to serve any other purpose than connecting to personal servers). This is the design we adopt. It does however create a new problem: how does a lock device connect to the right personal server?

This is the second issue for our digital key system: when and how should the lock device stop inquiry and establish a connection. When the lock device performs an inquiry, it detects the Bluetooth devices in its vicinity. There could be plenty (given that Bluetooth radios have a range of tens of meters). The first question is when to stop inquiry: after a fixed period or as soon as one device is detected. Our goal is not to find all the devices in the vicinity of the lock device but to establish a connection with a personal server as quickly as possible. We therefore choose to stop inquiry as soon as a device is detected.

Now the problem is that the first Bluetooth device detected by the lock device might not be a personal server, even if there is one in its vicinity. The lock device must determine if the detected device is a personal server or not. The lock device keeps a history of

IEEE COMPUTER SOCIETY

the Bluetooth devices it has encountered and classifies those that are personal servers and those that are not. If the first detected device is already known as something else than a personal server then the lock device returns to its inquiry mode. If the first detected device is not known, then a connection is established. If the device is not a personal server then the lock device goes back to the inquiry mode.

Once a connection is established between lock device and personal server, the actual authentication can start. This is the topic of the next section.

4. Secure Access Control

The main problem is to design a secure protocol that allows a personal server with a valid key to unlock a door. Recall that keys are created by an external authority that cannot communicate with the lock device that handles the unlocking of the door. The solution we propose here relies on well-known and well-tested security mechanisms whenever possible and keeps the system as simple as possible (note that simplicity is also important because of ressource constraints on the personal server).

4.1. Secure Protocol

In order to unlock a door, a personal server needs (i) an *identity*, i.e., a unique identifier and (ii) a valid *access key* for the door, i.e., a simple data structure associating lock device identifiers with the personal server identity – the list of doors the personal server is authorized to open – in our digital key system, access keys are created and distributed by the external authority. The secure protocol ensures that the personal server proves its identity (*authentication*) and that the data it sends are actually received unaltered by the lock device and cannot be reused later (*integrity*) [1]. Existing protocols (e.g., TLS [7], IPSec [19] and SSH [2]) support secure and authenticated communication but do not include access control. Their complexity make them poor candidates for the constrained environment of a personal server. We thus implement our own, simple access control protocol:

1. The lock device establishes a connection and sends its identifier to the personal server.
2. The personal server looks up an access key for the door whose identifier it just received and sends that access key to the lock device together with a proof of its identity.
3. The lock device unlocks the door if the proof of the identity is correct and if the access key is valid. Success or failure is reported back to the personal server (for feedback and logging purposes).

We rely on asymmetric cryptography for authentication [2]. A personal server proves its identity by (i) sending its public key to the lock device, (ii) proving that this public key is actually associated to its identity, and (iii) proving that it possesses the corresponding private key. The personal server uses a X.509 certificate, provided (and signed) by a certificate authority trusted by all components of the digital key system, to associate its public key with its identity. In order to prove that it possesses the private key, it signs the packet containing the certificate and the access key. This signature also guarantees the integrity of the data transferred from the personal server to the lock device. We skip details of the protocol because of space limitation (see [3] for details).

Note that in this protocol, the only secret information is the information needed to prove the personal server's identity, i.e., its private key. If an attacker accesses the private key (e.g., by stealing the personal server) then the associated identity should become invalid. Using traditional *Certificate Revocation Lists* on the lock devices is unpractical because there is no direct connection between lock devices and the certificate authority. Instead we propose to limit the validity of the access keys to short time ranges. In the worst case the attacker can use the private key for the length

1 Note that denial-of-service or relay attacks cannot be avoided. Their effects can be limited but at the cost of increased software complexity.

2 Symmetric cryptography requires personal servers and lock devices to share secret information. This is neither desirable nor practical.

IEEE COMPUTER SOCIETY

of the access key validity period. Once a theft or a loss of a personal server is registered, the external authority stops producing access key for the invalid identity.

4.2. Cryptographic Algorithms

RSA [16] is a generally trusted and well-tested algorithm that has been used for years. Recently, ECDSA [14] has gained ground, and is now regarded as at least as secure as RSA (see [17]). We evaluate these protocols by comparing key size and speed of signature generation/verification.

The size of the asymmetric keys influences both the size of data packets exchanged between personal server and lock device as well as the speed of both signing and verification. The current NIST recommendations [15] recommends using 1024 bit keys for RSA/DSA, and 160 bits for ECDSA while existing certificate authorities (e.g., VeriSign) use 2048 bits RSA/DSA and 224 bits for ECDSA.

Type	System	RSA (ms)	DSA (ms)	ECDSA (ms)
Level 1				
Sign	Pager	15889	9529	1011
Verify	Pager	1008	18566	1826
Sign	PC	67	24	2
Verify	PC	4	47	4
Level 2				
Sign	Pager	111956	*n/a*	1910
Verify	Pager	3608	*n/a*	3701
Sign	PC	441	*n/a*	4
Verify	PC	13	*n/a*	8

Table 1: Algorithm timings on the Pager and the PC. From [6].

The speed of signature generation/verification is hardware dependent. There is no benchmark yet focusing on cryptographic algorithms on personal servers. The closest benchmarks we have found is in [6], where the authors implement PGP [9] on a pager (10 MHz custom Intel 386) and a PC (400 MHz Intel Pentium II). Based on the results summarized in Table 1, ECDSA appears as the best candidate. It is orders of magnitude faster for signatures, and is only a little slower than RSA for verification. Assuming that the personal server is somewhere in between the pager and the PC, we can expect that it will need well under one second to generate a signature.

In terms of storage, access keys occupy 136 bytes with ECDSA signatures and 222 bytes with RSA. This different is significant as access keys obtained with ECDSA can be sent via 1 SMS (the limit for SMS size is 140 bytes, see [**? ?**]).

In conclusion, ECDSA seems preferable to RSA, however actual implementation needs to take into account the requirements of the certificate authority and the algorithms supported by the personal server.

5. Performance Evaluation

5.1. Experiment Environment

We implemented a prototype of our digital key system using a Sony Ericsson P800 mobile phone as personal server. The phone has a 156 MHz ARM9 CPU, 16 MB RAM, and 12 MB flash. It uses Symbian OS, and is programmable in both Java and C++ (for full specifications see [8]). The prototype application was implemented on the mobile phone using standard Symbian OS libraries as well as the *RSAREF2* cryptography toolkit (implementing RSA). There was no suitable ECDSA implementation available. The lock device is simply implemented on a PC equipped with a USB Bluetooth unit.

The metrics we are interested in are response time and energy consumption. Figure 2 shows our measurement set-up. We measure response time using wall clock time. In order to measure energy consumption, we measure the voltage drop over a resistor inserted in series between the battery and the mobile phone. The voltage drop divided by the resistance gives us the current draw and thus the energy consumption (assuming a constant battery voltage). We cannot simply measure the current by inserting a multimeter in series between the batteries and the phone: the phone refuses to boot in this configuration.

IEEE COMPUTER SOCIETY

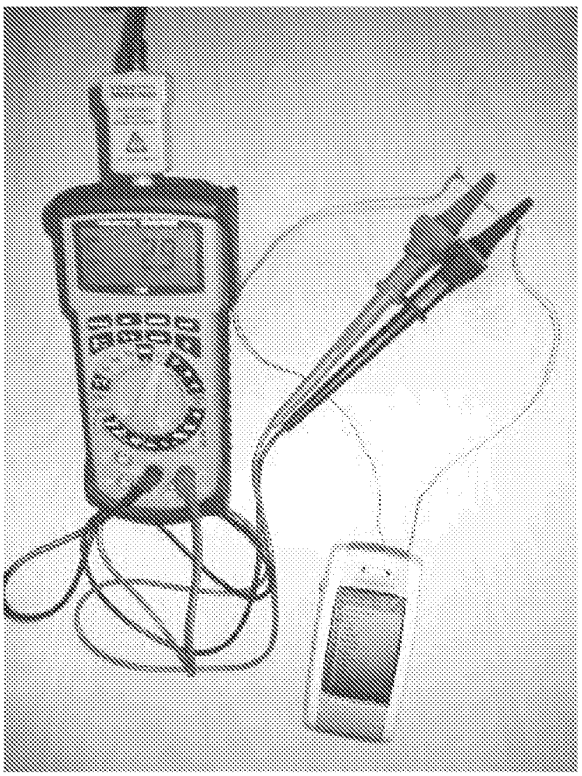


Figure 2: Setup for the measurement: We measure the voltage drop over a resistor inserted in series between the battery and the mobile phone

The precision of the measurements depends on the precision of both the resistors and the multimeter, the stability of the voltage on the battery, and the resistance of the wires connected to the resistor. The resistors have an accuracy of ±5% and the multimeter one of ±0.25%. The stability of the voltage is important because the voltage is used to calculate the energy consumption using Ohm's law. Ideally the voltage should be measured continuously, but a second multimeter for this purpose was not available during our experiments. We did some initial measurements and found that the battery deviated less than 1% from 3.6V for the first hour at least. We also tried to measure the resistance in the wires connected to the resistor and found it was negligible, so the wires will not influence measurements either. All in all, the measurements will have an inaccuracy of maximum 6–7%.

All measurements were performed a minimum of five times and for at least ten minutes.

5.2. Device Calibration

There are no public energy specifications for the mobile phone. The only available information is the voltage of the battery (3.6V), the capacity of the battery (1000 mAh), best case life time during conversations (13 hours) and standby (400 hours). From this we can deduce that the battery should have 12960 Joule, standby should consume ~9 mW and conversations ~277 mW. There is no further information available. We therefore calibrate the mobile phone in its different operating modes.

Idle Modes As a first step, we must find out how the phone behaves in idle mode. The radio can be turned off by setting the mobile device in a *flight mode*, that makes it usable in a plane or any other area where mobile phones are disallowed. The display can have the back-light turned on or off, and the phone has power-save modes that saves power by turning the display off after a specific amount of time. The power usage of the CPU can not be influenced by user-available settings.

To reveal the different power modes of the phone, measurements were made for all the possible combinations of the radio and back-light modes. It takes 150 seconds before the phone reaches its final idle mode after being booted. The lowest power consumption is ~9 mW, in flight mode with the screen turned off. The screen has four modes: On (~320 mW), dimmed back-light (~140 mW), no back light (~20 mW), and off.

To obtain a stable baseline, we want to use the mode where (i) Bluetooth is enabled and (ii) where the power consumption is as stable as possible. We use a mode where back-light and power save are off. It consumes ~33 mW. The problem is that power consumption is not really constant: it fluctuates because of the GSM radio. Fortunately, the GSM power usage comes in peaks, so as long as the functionality being tested has a stable power consumption it will be possible to disregard the GSM peaks. We have tried to find a way to have Bluetooth

IEEE COMPUTER SOCIETY

turned on with GSM turned off, but it is not supported on the phone.

Usual Functionalities In order to be able to relate the power usage of our application to the power usage of the normal functions of the phone, we have tested the following: using the GUI, having a conversation, using the camera, and playing a game.

Having a phone conversation takes around 250–300 mW, not far from the specifications. Using the GUI or the camera costs 500–600 mW, while playing a game ranges from 800 mW to 1000 mW. Compared to these numbers it was a bit surprising to see the cost of just touching the screen. Holding the pointer still at the same position on the screen costs 500 mW, no matter whether the program has a GUI or not (a console mode program). This is probably caused by the endless processing of pointer events from the screen. For a GUI application this is unavoidable, but for a console program this is not necessary, and must be considered a design flaw. Lastly, we tried to stress the phone maximally by playing a game with back-light on, full sound, a GSM connection and Bluetooth connection on at the same time – this peaked at around 1570 mW.

Cryptography For cryptography, the cost of one iteration of each operation with our implementation of RSA is the following (with idle mode cost subtracted):

Operation (bits)	Time (s)	Cost (mJ)
Sign, 1024	0.48	241.00
Verify, 1024	0.02	10.08
Sign, 512	0.08	40.32
Verify, 512	< 0.01	0.01

The device performs well. Generating a signature takes 0.5 seconds – only 7.5 times slower than the PC used in [6]. Extrapolating these results, an ECDSA signature would take 0.015 seconds for 160 bits keys and 0.030 for 224 bits keys. This would practically eliminate cryptography as a time factor for the application.

Bluetooth Experiments showed that Bluetooth costs (with idle mode cost subtracted):

Action	Cost
Being discoverable	4 mW
Being discoverable and connectable	7 mW
Answering an inquiry	< 1 mW
Doing inquiry	127 mW
Maintaining a connection or transferring data	557 mW / 532 mW[3]
Transferring data > 180 seconds	291 mW / 331 mW[3]
Slack	408–720 mJ

One of our first assumptions was that inquiry was expensive compared to inquiry scan, and it certainly is. Doing inquiry scans cost 7 mW while doing inquiry costs 127 mW. The cost of answering an inquiry was so low that it disappeared in the GSM background noise. Doing inquiries constantly would drain the battery 14 times faster than doing inquiry scans, so the choice of the lock device as the inquiring party is correct. Compared to having a conversation (250–300 mW), transferring data with Bluetooth is quite expensive – especially when adding the slack (extra energy usage after each Bluetooth activity on the phone for which we do not have an explanation – our best guess is that the Bluetooth chip power down is delayed).

5.3. The Application

Based on the measurements in the previous sections we can deduce what discovery and connection from the lock device will cost. We do not know how much time the actual data transfer takes, but with a conservative assumption of around 0.5 seconds (1 KB at 5 KB/sec plus overhead), the cost calculation is the following:

Function	Cost (mJ)
Answering inquiry	0
Signature (1024 bit)	241
Bluetooth connection (0.5 s)	278.5
Bluetooth slack	408–720
Total	928–1240

3 When phone initiates or sends.

IEEE COMPUTER SOCIETY

We obtain 1000 mJ for the cost of running the application, to which the 40 mW should be added to get the actual power usage (the idle mode baseline cost plus Bluetooth cost).

An actual application run with 1024 bit keys is shown in Figure 3. Average inquiry time was found to be 3.6 seconds (minimum 2.8 seconds, maximum 4.4 seconds), which is stable but more than one second slower than previously reported. The reason for inquiry being slower may be found in the interoperability between the specific Bluetooth devices we used, or the specific noise conditions in our office environment. It is beyond our scope to investigate this further, but the results confirm that the Bluetooth discovery process is influenced by the specific equipment and environment.

The Bluetooth connection only consumes energy after it has been established. In our application, the connection is established for around 0.7 seconds (see Figure 4). This too fast to be captured on the graph with the sampling rate of our multimeter (1 sample per second). Note that our graph shows a peak of energy consumption (at 550 mW) for 3.5 seconds after the connection is closed. This is due to a time-out in the Bluetooth stack we used on the PC, which should be optional. A way to avoid this time-out is to close down the entire Bluetooth stack on the PC when closing a connection. We thus ignore this cost in the rest of our discussion.

The average time needed to establish a connection was 1.2 seconds which was a lot faster than we expected. Even though most connects took around 1 second a few connects took over 10 seconds, the maximum being 18 seconds. The same phenomenon was experienced in [4], it is unclear why. The standard *page timeout* for a Bluetooth device is 5.12 seconds and the Bluetooth device we used was also set to this (see [5, Part H, 4.7.16]). So the connection establishment should timeout after this period. Unfortunately we do not have an explanation for this. Our conclusion is that there must be a flaw in the implementation of the connection establishment procedure.

Figure 4 shows the average time spent in different parts of the application. Apart from discovery and

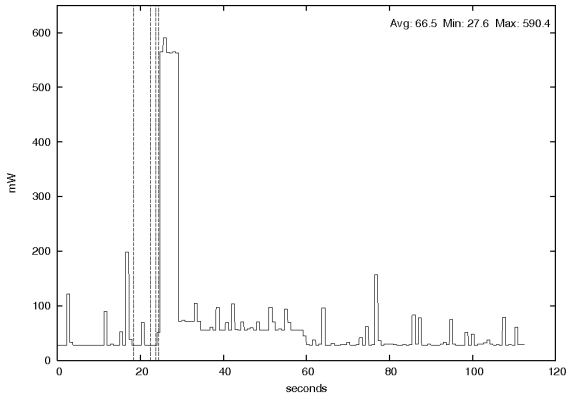


Figure 3: This graph shows the lock device connection to the mobile device, with mobile device key being 1024 bits. The vertical lines denote: Inquiry start, connection start, connection succeeded, and connection closed.

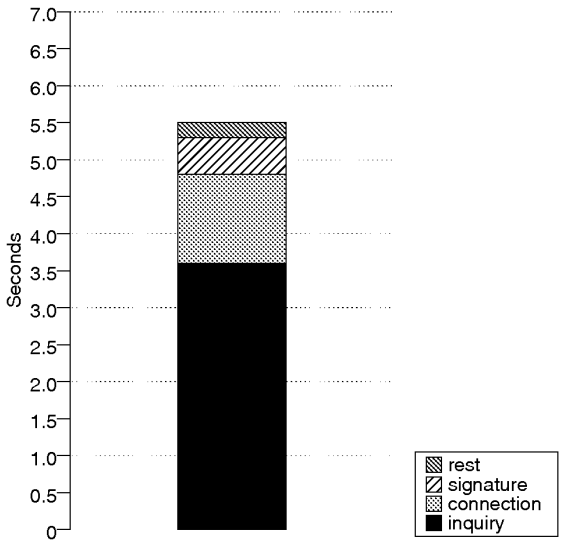


Figure 4: The average time usage of the different parts of the application.

IEEE COMPUTER SOCIETY

connection establishment the rest of the application takes 0.7 seconds on average, where 0.48 seconds are from the signature generation, so the rest of the application including communication takes around 0.2 seconds. All in all, the total average unlocking time is 5.5 seconds: Bluetooth discovery and connection establishment accounts for 87% of the total response time.

5.4. Summary

The tests confirmed our assumptions about the time and energy performance of Bluetooth and showed that our prototype implementation performed well and allows a door to be unlocked in 5.5 seconds. From an energy consumption point of view, the program cost is around 1000 mJ. This is the same cost as holding the pointer still at the screen for 2 seconds or having a phone conversation for 4 seconds. Or put differently, with a battery of 12960 J and the phone in idle mode with Bluetooth on (using 40 mW on average) it can do more than 10000 consecutive unlockings. These figures show that the application can run on the mobile phone with little influence on the lifetime of the battery.

6. Related Work

The different types of access control systems that exist to replace physical keys do not match the requirements of our scenario. Existing systems either rely on a wireless transceiver or a card. KEELOQ [13] is a solution based on a wireless transceiver. A remote keyless entry solution using KEELOQ is presented in [18]. Most cars have the possibility of remote unlocking. Some car manufactures even allow *keyless start and go* where the user simply needs to carry the key device to be able not just to open, but also start the car[4]. The problem with these kinds of solutions is that they are designed for a one-to-one situation, where one transceiver fits exactly one door.

Card-based access control systems are commonly used in large corporations and use a card equipped either with a magnetic stripe or a microchip. The latter can either be operated so that the users needs to insert the card into a reader, or *contactless* where the user just has hold the card near a reader (see [1] for an overview of the technology). Card-based microchip systems are normally passive in the sense that the card itself is activated by and receives power from the reader. It is not capable of functioning autonomously. These systems are typically meant to be used in the domain of one company, and are normally designed so that each lock device is connected to a central access control server.

We have only found one product that use Bluetooth-based mobile devices for access control purposes. XyLoc[5] is a commercial key-less authentication product that enables automatic authorization, designed for Windows-based PCs and requires connection to a central access control server. Bluetooth is an optional communication technology that can replace their normal proprietary system. We have also found a case study using Bluetooth-enabled mobile phones to control access for *gates*, which is not specified further[6]. Unfortunately only marketing information is available.

7. Conclusion

This paper presented a digital key system that allows a Bluetooth-enabled personal server to unlock a door without user interaction. The design fulfills our requirements in terms of functionalities (no user interaction is needed to open a door, lock devices are autonomous) and in terms of performance (a door can be opened in around 5 seconds without a major impact on battery lifetime).

The mobile phone we used as a personal server for our prototype provided most of the functionalities we needed. We missed some cryptographic capabilities (support for RSA and ECDSA). More importantly, Bluetooth is not ideal for such a digital key system. First, Bluetooth connections are expensive in terms of energy consumption (more expensive than a conver-

4 F.x. the Nissan Micra (`http://www.nissan-micra.com/`) or the Mercedes S-class (`http://www.mercedes-benz.com/`).

5 `http://www.ensuretech.com/`.

6 `http://www.codeisland.com/studies/studies.dvd.asp`.

IEEE COMPUTER SOCIETY

sation over GSM). Second, the device discovery procedure is slow. Bluetooth might not be the prefered standard for future generations of personal servers providing a wide range of functionalities including digital keys.

References

[1] Smart Card Allicance. Contactless technology for secure physical access: Technology and standards choices. Technical report, Smart Card Alliance, 2002. URL http://www.smartcardalliance.org/.

[2] Daniel J. Barrett and Richard Silverman. *SSH, The Secure Shell: The Definitive Guide*. O'Reilly & Associate, 1st edition, 2001.

[3] Allan Beaufour. Secure access control using mobile bluetooth devices. Master's thesis, Department of Computer Science, University of Copenhagen, 2003.

[4] Allan Beaufour, Martin Leopold, and Philippe Bonnet. Smart-tag based data dissemination. In *First ACM International Workshop on Wireless Sensor Networks and Applications WSNA02*, June 2002.

[5] *Specification of the Bluetooth System – Core*. Bluetooth SIG, 1.1 edition, February 2001.

[6] Michael Brown, Donny Cheung, Darrel Hankerson, Julio Lopez Hernandez, Michael Kirkup, and Alfred Menezes. PGP in constrained wireless devices. In *Security Symposium*. USENIX, 2000.

[7] T. Dierks and C. Allen. RFC2246 – the TLS protocol version 1.0. Technical report, RFC Editor, Januar 1999.

[8] Sony Ericsson. P800/P802 white paper. Technical report, Sony Ericsson, 2003.

[9] Simon L. Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc., 1994.

[10] O. Kasten and M. Langheinrich. First experiences with bluetooth in the smart-its distributed sensor network. In *Workshop on Ubiquitous Computing and Communications, PACT 2001*, 2001.

[11] HP Cambridge Research Lab. Personal server project. URL http://www.crl.hpl.hp.com/projects/personalser

[12] Martin Leopold. Evaluation of bluetooth communication: Simulation and experiments. Technical Report 02/03, Institute of Computer Science, University of Copenhagen, 2002.

[13] Microchip. KEELOQ authentication products, 2002. URL http://www.microchip.com/1010/pline/security/i

[14] NIST. Digital sinature standard (DSS). Technical Report fips186-2, National Institute of Standards and Technology, 2000.

[15] NIST. Recommendation for key management. part 1: General guideline. Special Publication 800-57, National Institute of Standards and Technology, January 2003. URL http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.h Draft.

[16] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978.

[17] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons Ltd., 1996.

[18] Microchip Technologies. Remote keyless entry and convenience center reference design with LIN bus interface, 2002. URL http://www.microchip.com/.

[19] R. Thayer, N.Doraswami, and R. Glenn. RFC2411 –IP security: Document roadmap. Technical report, RFC Editor, November 1998.

[20] Roy Want. New horizons for mobile computing. Keynote speech at PerCom 2003, 2003. URL http://www.percom.org/percom_2003/slides/.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :		(11) International Publication Number:
H04L 29/06, 12/28	A1	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).

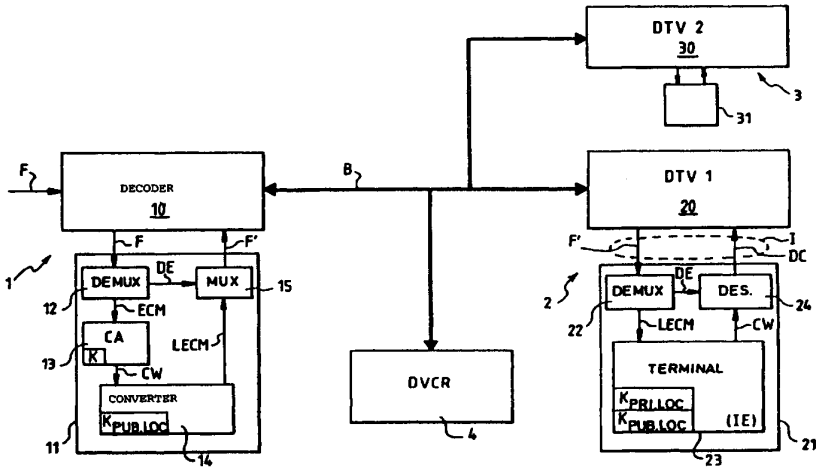
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: QUES, Florence [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR). ANDREAUX, Jean–Pierre [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR). FURON, Teddy [FR/FR]; Thomson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

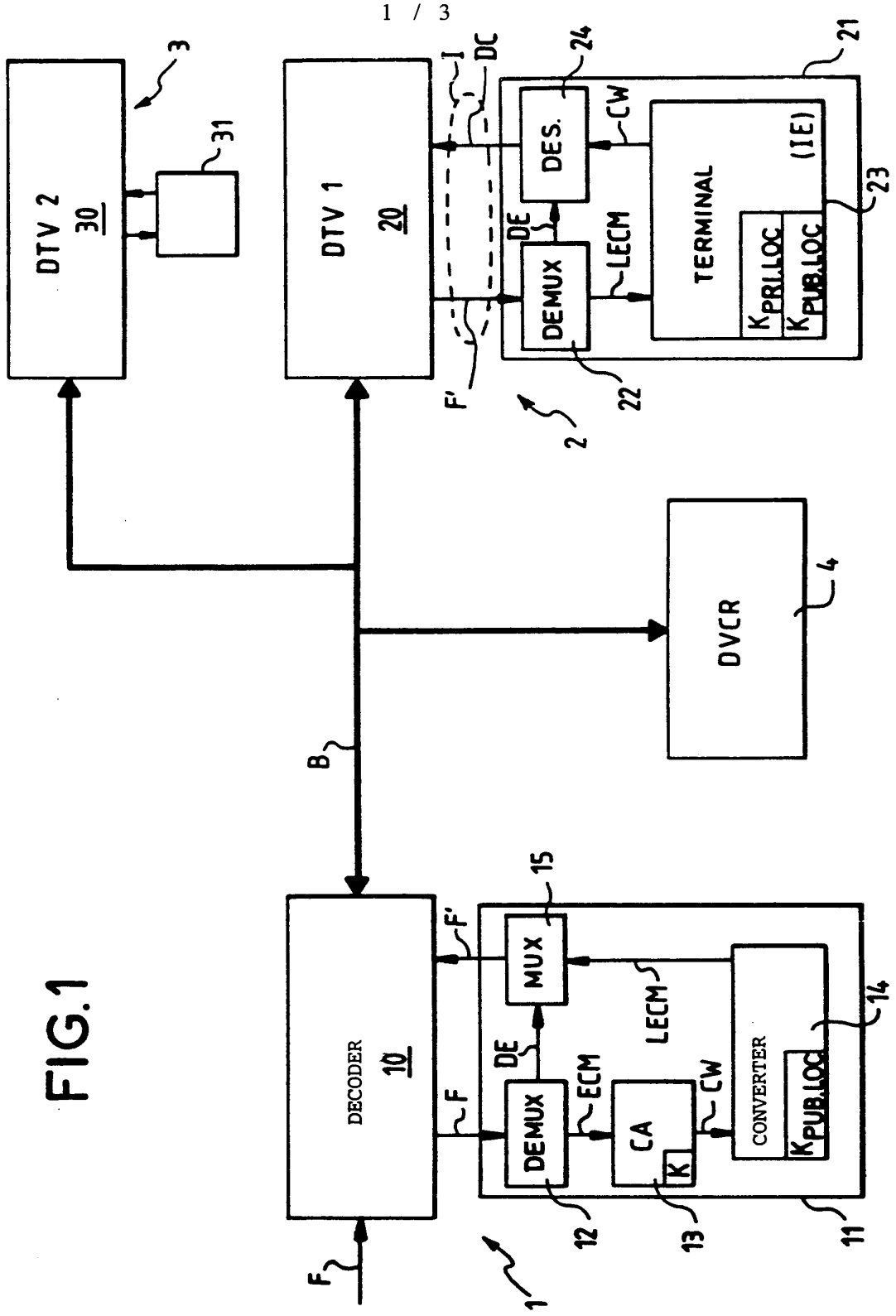

DTV 2
30
31
3
DTV 1
20
DC
24
DES.
CW
21
TERMINAL
(IE)
23
DE
DEMUX
LECM
K PRI.LOC
K PUB.LOC
F'
22
2
DVCR
4
B
DECODER
10
F'
15
MUX
DE
LECM
14
F
DEMUX
ECM
CA
K
CW
CONVERTER
K PUB.LOC
12
13
11
F
1

FIG.1

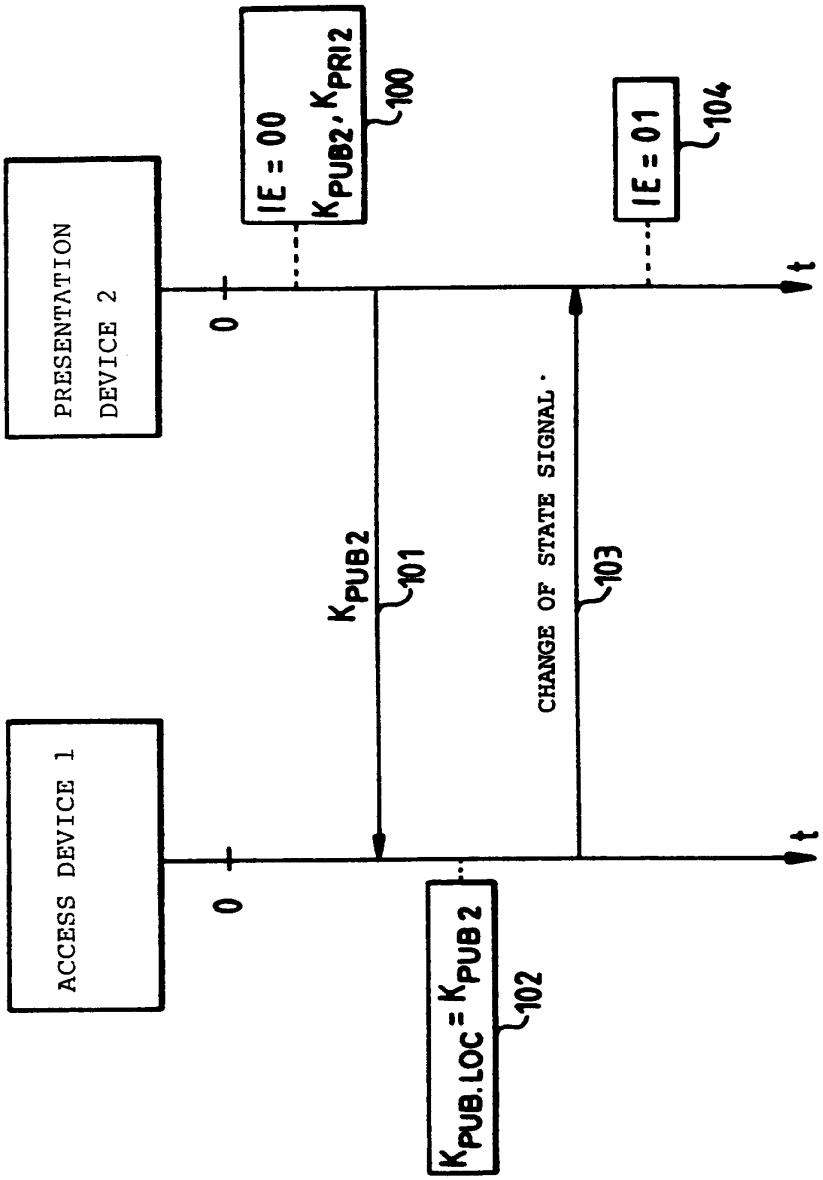

PRESENTATION DEVICE 2
ACCESS DEVICE 1
0
0
t
t
IE = 00
K_{PUB2}, K_{PRI2}
100
IE = 01
104
K_{PUB2}
101
CHANGE OF STATE SIGNAL
103
$K_{PUB.LOC} = K_{PUB2}$
102

FIG.2

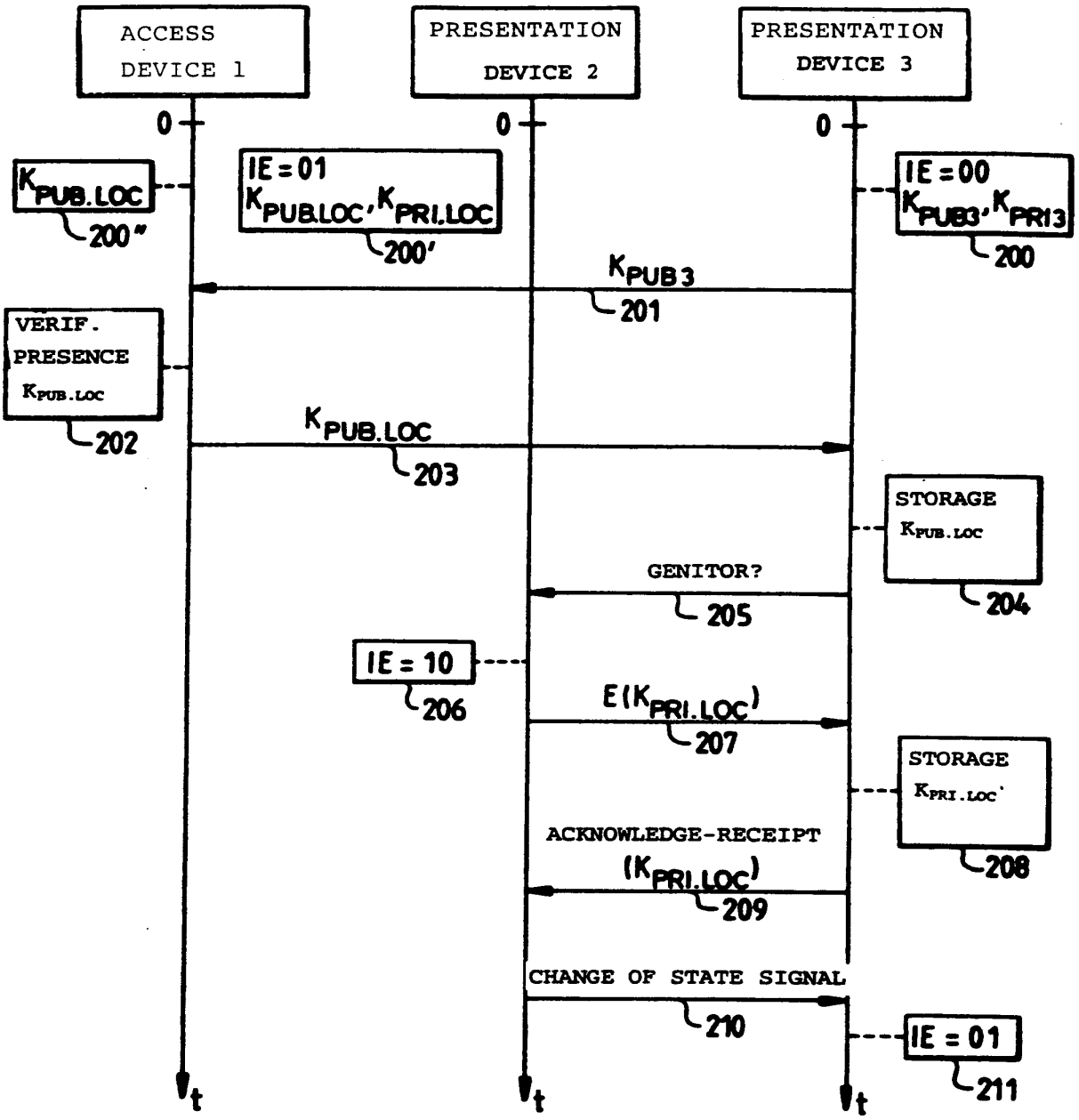

ACCESS DEVICE 1
PRESENTATION DEVICE 2
PRESENTATION DEVICE 3
0
0
0
$K_{PUB.LOC}$
200"
IE = 01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE = 00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
VERIF. PRESENCE $K_{PUB.LOC}$
202
$K_{PUB.LOC}$
203
STORAGE $K_{PUB.LOC}$
204
GENITOR?
205
IE = 10
206
$E(K_{PRI.LOC})$
207
STORAGE $K_{PRI.LOC}$
208
ACKNOWLEDGE-RECEIPT
$(K_{PRI.LOC})$
209
CHANGE OF STATE SIGNAL
210
IE = 01
211
t
t
t

FIG.3

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 00/02918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 382 296 A (N.V. PHILIPS GLOEILAMPENFABRIEKEN) 16 August 1990 (1990-08-16)	1
A	column 2, line 2-37 column 3, line 12-29 column 4, line 40-44 column 4, line 55 -column 5, line 34 column 6, line 57 -column 7, line 5 column 8, line 56 -column 9, line 42	2-14
A	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 (1995-10-25) page 2, line 22-41 page 3, line 31-34 page 3, line 47-50 page 7, line 34-57 page 9, line 46-57	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2000	21/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter ›nal Application No
PCT/EP 00/02918

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0679029 A	25-10-1995	US 5237610 A	17-08-1993
		EP 0683614 A	22-11-1995
		AT 144670 T	15-11-1996
		AT 181196 T	15-06-1999
		AT 180373 T	15-06-1999
		AU 650958 B	07-07-1994
		AU 1384092 A	01-10-1992
		BR 9201106 A	24-11-1992
		CN 1066950 A,B	09-12-1992
		DE 69214698 D	28-11-1996
		DE 69214698 T	06-03-1997
		DE 69229235 D	24-06-1999
		DE 69229235 T	23-09-1999
		DE 69229408 D	15-07-1999
		DE 69229408 T	11-11-1999
		EP 0506435 A	30-09-1992
		JP 5145923 A	11-06-1993
		SG 44801 A	19-12-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22724 A1

(51) International Patent Classification[7]: H04N 5/00, 7/16, 7/167

(21) International Application Number: PCT/EP00/08439

(22) International Filing Date: 30 August 2000 (30.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99/11901 23 September 1999 (23.09.1999) FR

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: MORCEL, Stéphane [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

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

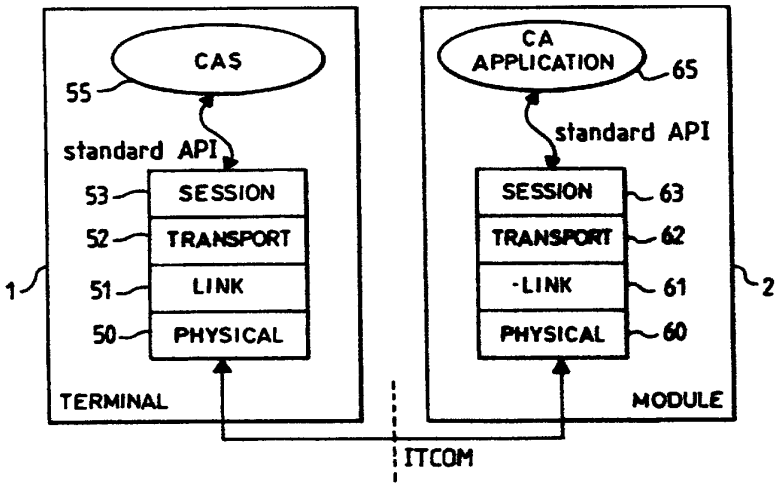
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTIMEDIA DIGITAL TERMINAL AND DETACHABLE MODULE COOPERATING WITH THE TERMINAL COMPRISING AN INTERFACE PROTECTED AGAINST COPYING



(57) Abstract: The terminal (1) receives a scrambled data stream (TS(D.EMB.)) in which the control words (CW) having served to scramble the data are transmitted in encrypted form. It transmits, via a first interface (ITTS), this stream to a detachable module (2) containing the conditional access system specific to the service provider supplying the data. The module (2) extracts from the stream and decrypts the control words (CW) before transmitting them to the terminal, via a second interface (ITCOM). These control words are used by a descrambler (16) of the terminal to descramble the data. The data stream leaving the module (TS'(D.EMB.)) contains only scrambled data, thus guaranteeing better protection against copying.

WO 01/22724 A1

Multimedia digital terminal and detachable module cooperating with the terminal comprising an interface protected against copying

The present invention relates to the field of conditional access systems for multimedia digital terminals. It relates more particularly to a multimedia digital terminal as well as to a detachable module associated with this terminal for implementing a conditional access system, in which the interface between the terminal and the module is protected against illicit copying.

The invention has been embodied within the context of the so-called DVB-CI interface (the initials standing for "Digital Video Broadcasting - Common Interface" which is described in particular in European Standard EN 50221 published by CENELEC (Comité Européen de Normalisation Electrotechnique).

This DVB-CI common interface has been defined by the DVB group so as to allow standardization of digital receiving equipment whilst allowing service providers supplying the data, (for example suppliers of Pay TV programmes) to remain proprietors of the conditional access system and of the corresponding security elements. This is because a conditional access system must be envisaged whenever it is necessary to control access to broadcast data. However, the service providers supplying the data wish to preserve a specific conditional access system. By virtue of the DVB-CI interface, the specific proprietary elements can be integrated into a module which is separate from the standardized parts of the terminal which receive and decode the digital video data or the service data. Thus, the proprietary elements can be manufactured and sold separately from the terminals, thereby making their distribution easier. The module is referred to as a "DVB-CI module" by extension.

The aforesaid European standard describes in particular the hardware and software architecture of the common interface between a server (the host) and one or more DVB-CI modules connected to the server.

We have represented this architecture in Figure 1. The host server 1 is a multimedia digital terminal such as a decoder of programmes broadcast by satellite or by cable, a video recorder or a personal computer, to which may be connected one or more modules 2. The module 2 is a detachable device which cannot operate alone but which is intended to execute certain specific tasks in association with the host server, in particular the implementation of a conditional access system or of an electronic programme guide. To do this, the module can access resources, that is to say software or hardware functional units, of the host server. The aforesaid common interface standard defines for this purpose a certain number of objects able to be exchanged between the module and the host server and allowing the module to use the resources of the host server.

Within the framework of the standards defined by the DVB group, the digital data are transmitted in the form of an information stream coded according to the MPEG 2 standard (ISO/IEC 13818-1), but naturally any other data transport standard can be used within the framework of the invention.

The digital terminal 1 of Figure 1 comprises a tuner/demodulator 10 which receives a signal S, emanating from a satellite antenna or from a cable network, and which outputs a digital data stream transmitted in the form of packets, and referred to as the TS (standing for "Transport Stream") in the aforesaid MPEG 2 standard, and containing the services supplied by providers.

The data stream TS comprises, in a known manner, packets of data supplied by various service providers and, so as to guarantee that the data reach only those users having acquired the right to receive them (for

example by means of a subscription to the service), these data are transmitted whilst being scrambled by control words CW.

In order to descramble the data, the service provider also supplies the users with the control words having served to scramble the data. So as to keep the control words secret, they are supplied after having been encrypted with an algorithm with key K. The various encrypted control words are sent to the users in control messages, commonly denoted ECMs (the abbreviation ECM standing for "Entitlement Control Message") transmitted in the data stream TS. The control words are thereafter decrypted in a secure processor containing the key K, the secure processor being included within a security element, for example a smart card, which is supplied to the users.

Returning to Figure 1, TS(D.EMB.) therefore denotes the data stream TS containing the data in scrambled form. In accordance with the principle defined in the aforesaid standard EN 50221, all the elements of the conditional access system which are specific to the service provider are contained in the detachable module 2 which receives the data stream TS(D.EMB.) from the digital terminal 1 across the DVB-CI common interface.

The module 2 comprises a microcontroller 21, in which the access control software application CA specific to the service provider is executed. It furthermore comprises a component 22 referred to as demultiplexer which receives the data stream TS(D.EMB.) so as to extract therefrom the video or audio data packets corresponding to a service which the user wishes to view or so as to extract therefrom data packets containing so-called "service" information, such as control messages ECM. The video or audio data packets are sent to a descrambler 23 contained in the module 2 whilst the messages ECM are sent to a smart card 3 which has been inserted into the module 2 and which contains, in a

secure processor 30, the key K having served to encrypt the control words. The decryption of the control words contained in the messages ECM is performed by the secure processor 30 which outputs the control words CW unenciphered to the descrambler 23 situated in the module 2. The descrambler 23 is thus in a position to descramble the video or audio data packets received from the demultiplexer 22 by virtue of the control words CW which it receives from the smart card 3. It outputs a digital data stream TS(D.DES.) in which the data packets corresponding to the service which has been selected by the user are descrambled.

The data stream TS(D.DES.) is transmitted to the digital terminal 1 via the DVB-CI common interface. It is more particularly transmitted to an MPEG decoder 14 of the terminal which supplies the audio and video outputs of the terminal which can be read directly by an apparatus such as a television.

The terminal 1 also comprises a microcontroller 11 in which the various software applications of the terminal are executed.

The DVB-CI common interface in fact comprises two logic interfaces:

- the first, the interface of the data stream ITTS, constitutes a bi-directional bus and transports the digital data packets of the TS stream in both directions between the terminal 1 and the module 2 according to the MPEG 2 transport standard. From the terminal to the module, the stream TS(D.EMB.) transmitted via the ITTS interface is a scrambled data stream whilst in the other direction stream TS(D.DES)), and on condition that the module 2 allows access to the data selected by the user (that is to say that it contains the elements of the conditional access system of the service provider which are necessary for descrambling the said data), the packets containing the selected data are returned

descrambled whilst the remainder of the TS stream remains unchanged;

- the second, the command interface ITCOM, transmits commands in both directions between the terminal 1 and the module 2 (more particularly between the microcontrollers 11 and 21) by way of the objects (or primitive functionalities) defined in the standard and which were mentioned above.

A notable drawback of the system just described is that certain data flow unenciphered at the DVB-CI common interface level (in the stream TS(D.DES.). In actual fact, data broadcasters are becoming increasingly preoccupied by illicit copies which may be made from the data which these broadcasters transmit, all the more so when these data are transmitted in digital form as is the case in the present instance, and they are asking for means of protection against copying to be set in place.

The current DVB-CI common interface cannot guarantee this protection against copying since, the module 2 being detachable, it is possible for a pirate to connect a digital recorder to a connection port across which the stream TS(D.DES.) travels and to record the data packets which flow unenciphered.

A purpose of the present invention is to solve the aforesaid problems by providing means of ensuring protection against copying at the level of the common interface between a digital terminal and a module which are linked together by an interface of the DVB-CI type.

The invention therefore relates to a multimedia digital terminal intended for receiving a stream of digital data scrambled by control words, the control words being contained in the stream in encrypted form, and intended to cooperate with a detachable module for descrambling the data stream. The terminal is able to transmit the scrambled data stream to the detachable module. According to the invention, the terminal is furthermore capable of receiving from the detachable

module the decrypted control words, and it comprises a descrambler capable of descrambling the digital data stream by using the control words received from the detachable module.

The descrambling of the data is therefore performed solely in the decoder and no data item now travels unenciphered at the level of the interface between the terminal and the detachable module. The risks of illicit copies are therefore considerably reduced by virtue of the invention.

According to a preferred embodiment of the invention, the digital terminal is furthermore able to receive from the detachable module the scrambled digital data stream, wherein the data stream received by the terminal is not modified relative to the data stream transmitted by the terminal.

According to another embodiment, the digital terminal is able to receive from the detachable module the scrambled digital data stream from which, relative to the data stream transmitted by the terminal, the data packets containing the control words have been removed.

According to another aspect of the invention, the terminal is able to transmit the scrambled data stream to the detachable module across a first interface with the detachable module, and it is furthermore capable of receiving from the detachable module the decrypted control words across a second interface with said module.

According to another particular characteristic of the invention, the terminal is furthermore able to receive from the detachable module, across the first interface, the scrambled digital data stream.

The invention also relates to a multimedia digital terminal intended for receiving a stream of digital data scrambled by control words, the stream of data containing the control words encrypted using a first key, and intended to cooperate with a detachable module for descrambling the data stream. The terminal is able to

transmit the scrambled data stream to the detachable module across a first interface with the detachable module. According to the invention, the terminal is furthermore capable of receiving from the detachable module the decrypted control words which are encrypted using a second key before being transmitted across a second interface with the module. The terminal also comprises means for decrypting the control words received from the detachable module using the second key; and a descrambler capable of descrambling the digital data stream by using the decrypted control words.

Thus, in addition to the data which travel at the level of the first interface between the module and the terminal only in scrambled form, the control words are also encrypted so as to travel at the level of the second interface, thereby further increasing the security of the assembly.

The invention also relates to a module intended for cooperating with a digital terminal as described above, this module being able to receive from the terminal a scrambled digital data stream. According to another aspect of the invention, the module is furthermore capable of extracting from the data stream the control words having served to scramble the digital data; of decrypting the control words; and of transmitting the decrypted control words (CW) to the terminal.

According to another aspect of the invention, the module is furthermore adapted for returning the scrambled digital data stream to the terminal without modifying the stream.

According to yet another aspect of the invention, the module is furthermore adapted for returning the scrambled digital data stream to the terminal by removing, relative to the data stream transmitted by the terminal, the data packets containing the control words.

According to another characteristic of the invention, the module is able to receive the digital data stream across a first interface with the terminal, and it is furthermore capable of transmitting the decrypted control words to the terminal across a second interface with the terminal.

According to a particular embodiment of the invention, the module is able to cooperate with a detachable security element for decrypting the control words, the module being capable of extracting from the digital data stream messages containing the encrypted control word; of transmitting the messages to a security element inserted into the module; of receiving from the security element the decrypted control words; and of transmitting the decrypted control words to the digital terminal with which it cooperates.

The invention also relates to a module intended for cooperating with a digital terminal as described above, the module being able to receive from the terminal a scrambled digital data stream across a first interface with the terminal. According to the invention, the module is furthermore capable of extracting from the data stream the control words having served to scramble the digital data; of decrypting the control words and encrypting the control words using a second key; and of transmitting the encrypted control words to the terminal across a second interface with said terminal.

The invention also relates to a method for descrambling a stream of digital data, scrambled by control words, which is received by a multimedia digital terminal, the control words being contained in the stream in encrypted form. The method comprises a first step consisting in transmitting the scrambled data stream to a detachable module. It furthermore comprises the steps consisting, for the detachable module, in extracting from the data stream the control words having served to scramble the digital data; in decrypting said control

words; and in transmitting the decrypted control words to the terminal.

The invention also relates to a method for descrambling a stream of digital data, scrambled by control words, which is received by a multimedia digital terminal, the stream of data containing the control words encrypted using a first key. The method comprises a first step consisting in transmitting the scrambled data stream to a detachable module. According to the invention, it furthermore comprises the steps consisting, for the detachable module, in extracting from the data stream the control words having served to scramble the digital data; in decrypting the control words; in encrypting the control words with using a second key; and in transmitting the encrypted control words to the terminal. The method furthermore comprises the steps consisting, for the terminal, in decrypting the control words using the second key; and in descrambling the digital data stream by using said decrypted control words.

The invention also relates to a method for transferring control words between a module as described above and a digital terminal also described above. This method consists essentially:

- for the module, in sending a first identification object to the terminal;
- for the terminal, in sending, in response to the first object, a second identification object indicating whether the terminal is or is not able to receive the control words from the module; and
- for the module, in the event of a positive response with the second object, in sending the control words enclosed in a third object.

Other characteristics and advantages of the invention will become apparent on reading a particular, non-limiting embodiment of the invention given with reference to Figures 1 to 4, among which:

- Figure 1, described above, represents a digital terminal into which is plugged a DVB-CI module according to the prior art;
- Figure 2 represents a digital terminal into which is plugged a module according to the principle of the invention;
- Figure 3 diagrammatically represents a part of the common interface between a digital terminal and a module such as those of Figure 2;
- Figure 4 illustrates a protocol for communication across the part of the common interface represented in Figure 3.

Represented in Figure 2 are a digital terminal 1 together with a module 2 connected to the terminal via an interface which is improved relative to the DVB-CI interface so as ensure better protection against copying at the level of this interface.

The elements which are similar to those of Figure 1 described earlier bear the same reference numbers and will not be described further.

In the embodiment of the invention illustrated in Figure 2, it will be considered that the digital terminal 1 is a decoder receiving programmes from various service providers via cable or via a satellite antenna.

A module 2 containing the specific elements of the conditional access system of a first service provider is connected to this decoder.

According to the principle of the invention, the data stream TS'(D.EMB.) leaving the module 2 via the interface ITTS contains only data in scrambled form. The module 2 extracts only the control words CW from the stream TS(D.EMB.) received so as to transmit them, once decrypted, to the decoder. The descrambling of the data is performed only in the decoder 1 by virtue of a descrambler 16 contained in the decoder. Thus, the digital data are no longer available unenciphered at the level of the ITTS interface and illicit copying is, if

not eliminated, at least made much more complex than in the prior art.

To do this, as in the prior art, the module 2 comprises a demultiplexer 22 which extracts the ECM control messages from the data stream TS(D.EMB.) received and which transmits them to a smart card 3 inserted into the module. The secure processor 30 of the smart card decrypts the control words CW contained in the ECM messages and it transmits them to the module 2.

According to a preferred embodiment of the invention, the control words CW are transmitted from the module 2 to the decoder 1 across the control interface ITCOM. The details of the transmission of the control words via the ITCOM interface will be explained later in conjunction with Figures 3 and 4.

Preferably, the data stream TS(D.EMB.) which is received by the module 2 is retransmitted as is to the decoder (link 29) without being modified (TS'(D.EMB) = TS(D.EMB.)). It is received in the decoder by a demultiplexer 15 which extracts the video or audio data packets corresponding to the programme which the user wishes to view and which transmits them to the descrambler 16 so as to be descrambled before being transmitted to the MPEG decoder 14. For this purpose the descrambler 16 receives the control words CW from the module 2 via the ITCOM interface.

According to a first variant embodiment, the module 2 extracts the ECM control messages from the data stream TS(D.EMB.) and replaces them, in the data stream TS'(D.EMB.) transmitted to the decoder, with stuffing packets. This variant is represented diagrammatically via the link 28 shown dashed.

According to a second variant embodiment, the demultiplex 22, contained in the module 2, extracts the video or audio data packets corresponding to the programme which the user wishes to view and it transmits them in the data stream TS'(D.EMB.) so that they are

received directly by the descrambler 16 of the decoder. This variant is represented diagrammatically by the link 27 shown dashed.

Also represented dashed in Figure 2 is a smart card 4 which can be inserted into the decoder 1 and which belongs to the conditional access system of a second service provider. Indeed, the decoder can comprise an integrated conditional access system for accessing the services of the second provider and furthermore comprise several connectors for modules 2 so as to access the services of several other providers.

It is for this reason that the decoder comprises a demultiplexer 15 and a descrambler 16. The access control software application CA' of the second provider is executed in the microcontroller 11. When the user selects a service of the second provider, the stream TS(D.EMB.) is transmitted directly to the demultiplexer 15 via a link 19. This demultiplexer extracts the control messages ECM' and transmits them to the secure processor 40 of the smart card 4 which, with the aid of the key K', decrypts the control words CW' contained in the messages ECM' and sends them unenciphered to the descrambler 16, so as to descramble the services selected by the user.

According to a third variant embodiment of the invention, the data stream TS(D.EMB.) is transmitted from the decoder 1 to the module 2 so that the latter extracts the control words CW and retransmits them unenciphered to the decoder, but unlike the variants mentioned earlier, the stream TS(D.EMB.) is not returned via the ITTS interface to the decoder. Only the control words are transmitted to the decoder after having been decrypted by the module. The stream TS(D.EMB.) is for its part sent directly to the demultiplexer 15 of the decoder via the link 19 inside the decoder.

According to a fourth variant embodiment of the invention, the control words CW are not transmitted unenciphered across the ITCOM interface. They are

encrypted by the microcontroller 21 of the module 2 using a second key, different from the key K used to encrypt the control words upon their transmission in the data stream TS(D.EMB.), before being transmitted over the ITCOM interface. This variant thus offers increased security since now no element travels unenciphered via the interface between the module and the decoder.

The microcontroller 11 of the decoder 1 will therefore have to decrypt, using this second key, the control words received by the ITCOM interface before transmitting them to the descrambler 16.

In a first embodiment of this variant, the module 2 and the decoder 1 generate, before a single control word travels through the ITCOM interface, a session key SSK by using the Diffie Hellman protocol, which is well known to the person skilled in the art. Thereafter, all the control words are encrypted in the module using the session key SSK, then are transmitted to the decoder in this encrypted form across the ITCOM interface before being decrypted, using the session key, in the decoder.

In this embodiment, a different session key is generated each session, that is to say each time the user selects a programme which needs to be descrambled in the module 2.

In a second embodiment of this variant, the decoder 1 and the module 2 each contain a secret key K2 which is stored in a secure area of the decoder or of the module, for example in a secure processor. This secret key is unique for each decoder and if several modules are plugged into the decoder, they all contain the secret key of the decoder.

In this embodiment, the control words are therefore encrypted with the secret key K2 in the module before being transmitted to the decoder via the ITCOM interface; they are then decrypted in the decoder using the key K2.

The principle of the invention is particularly advantageous since it makes it possible to harness the demultiplexer and the descrambler which are already contained in the decoder so as to use them even when the conditional access system of another provider, contained in a detachable module, is used.

It should be stated in this regard that the demultiplexer and the descrambler components have been standardized within the framework of the DVB digital broadcasting standard in particular. Only the conditional access system (access control software, decryption algorithm and key, smart card, etc.) remains a proprietary system of the service provider.

We shall now describe in greater detail, in conjunction with Figures 3 and 4, how the control words CW are transmitted via the command interface ITCOM.

The ITCOM interface between the terminal (decoder) 1 and the module 2 uses a communication protocol which is represented diagrammatically in Figure 3 and which comprises several layers:

- a "Physical" layer (50, 60) which comprises the physical connector and low-level software for initializing the communication;
- a "Link" layer (51, 61) which forms the link between the Physical layer which deals only with bytes (8 bits of data) and the higher layer which can deal with much larger packets of data;
- a "Transport" layer (52, 62) which optimizes the occupation of the data stream by the various session in progress and which conveys the messages from the higher layer to the "Link" layer;
- a "Session" layer (53, 63) which opens, closes and manages the sessions in which the messages of the applications using the ITCOM interface are transmitted.

Represented in Figure 3 are on the one hand the access control application CA 65 which is executed in the microcontroller 21 (cf. Fig. 2) of the module 2 and on

the other hand a software resource 55 called CAS (standing for "Conditional Access Support") of the terminal 1.

This resource CAS defines a certain number of specific objects intended for use by the access control applications of the modules connected to the terminal. It communicates with the four layers of the ITCOM interface across a " Standard API " (the abbreviation API standing for "Application Programming Interface"), the standard API defining other objects which are used by all the resources of the system.

Likewise, the access control application 65 of the module uses the objects defined by the resources of the terminal through a standard API.

It was seen earlier that, according to the principle of the invention, the control words which are decrypted in the module 2 are thereafter transmitted to the terminal 1 across the ITCOM interface. In order that the control words may "cross" the various layers of the ITCOM interface, they must be enclosed in specific objects, comprehensible both to the application CA and to the resource CAS, which will be called "CPTS_CW()" hereinafter. Of course, when the control words are transmitted encrypted with the aid of a second key (SSK or K2) as in the fourth variant set forth above, they are enclosed, in this encrypted form, in the objects CPTS_CW().

Figure 4 illustrates the protocol for communication between the access control application CA of the module and the resource CAS of the terminal which allows, according to the invention, protection against copying.

The time scale has been represented by two downward vertical arrows.

After a first session-opening phase (not represented), the application CA of the module checks that the resource CAS of the terminal does indeed support

protection against copying over the ITCOM interface. To do this, the application CA sends during a step 100 an object "CPTS_identification()" which will be defined later. The resource CAS responds by sending, in step 101, an object "CPTS_identification_answer()" which indicates whether the resource CAS does or does not support protection, against copying. In the event of a positive response, the application CA of the module then regularly sends (steps 102a, 102b, 102i) the control words enclosed in the objects "CPTS_CW()" as and when they are decrypted by the module.

Conversely, in the event of a negative response, the terminal is not considered reliable. Consequently, the control words are not sent to the terminal and the data of the stream TS(D.EMB.) are not descrambled in the terminal. Any appropriate action can be envisaged at that moment (displaying of a message destined for the user by way of the User Interface resource of the terminal for example).

As seen above, it is necessary, in order to implement the protocol of Figure 4, to define additional objects over and above those already envisaged in the existing standards.

Identification objects

The function of the identification objects is to allow an access control application CA of a module supporting protection against copying to check whether the terminal to which the module is connected also supports protection against copying. That is to say, whether the resource CAS of the terminal possesses the functionality of protection against copying.

The first object used is the following:

```
CPTS_identification() {
    CPTS_identification_tag        24 bits  uimsbf
    Length_field() = 0             8 bits   uimsbf
    }
```

The notation used here corresponds to that used in the aforesaid standard EN 50221 in which the objects are generally defined by means of a tag (here the "CPTS_identification_tag"), of a length field ("Length_field()") and of parameters which can take various values.

The CPTS_identification_tag tag is a number defined on 24 bits and the notation "uimsbf" (stemming from "unsigned integer most significant bit first") signifies that this pertains to an unsigned integer whose most significant bits (highest order bits) are always situated first.

The "Length_field()" field defines the length in terms of number of bytes of the parameters forming part of the object. Since here the object "CPTS_identification()" contains no parameter, the length field is equal to zero.

The second object used is the following:

```
CPTS_identification_answer() {
     CPTS_identification_answer_tag     24 bitsuimsbf
     Length_field() = 1
     Identification_result               8 bits  uimsbf
}
```

This "CPTS_identification_answer()" object is used to indicate whether the resource CAS of the terminal does or does not support protection against copying according to the invention. It comprises a "CPTS_identification_answer_tag()" tag and a length field which is equal to 1 since the object also comprises an "Identification_result" parameter defined on 8 bits. This parameter is for example a Boolean indicating whether or not protection against copying is supported by the resource CAS.

Other parameters can be envisaged, for example to indicate a version number of the copy protection.

Contro- word transmission objects

These objects enclose the control words which are decrypted in the module. They allow the access control application CA of the module to send them, across the various layers of the ITCOM interface, to the resource CAS of the terminal which can thereafter utilize them by transmitting them to the descrambler 16 (Fig. 2).

These objects have the following format:

```
CPTS_CW()  {
   CPTS_CW_tag                  24 bits uimsbf
   Length_field()
   MPEG2_stream_type             8 bits uimsbf
   MPEG2_pid                    16 bits uimsbf
   Odd_CW                      128 bits uimsbf
   Even_CW                     128 bits uimsbf
}
```

They comprise a "CPTS_CW_tag" tag, a length field "Length_field()" and parameters identifying:

- the type of data packet transported (video, audio or other data), in "MPEG2_stream_type" defined on 8 bits;
- the PID (standing for "Programme Identifier"), that is to say the programme identifier associated with the packet transported in "MPEG2_pid", defined on 16 bits;
- the odd ("Odd_CW") and even ("Even_CW") control words defined on 128 bits each.

Indeed, it is well known that a succession of even and odd control words is transmitted in the TS data stream, each control word being transmitted in advance relative to the data packets which are scrambled with this control word. The descrambler therefore continuously memorizes the even control word serving to descramble the

current data packet and the odd control word serving to descramble the next packet (or vice versa).

The "CPTS_CW()" object comprises, in a first embodiment, parameters making it possible to send both an even control word (in "Even_CW") and an odd control word (in "Odd_CW"). It can also comprise, in another embodiment, a parameter "CW", on 128 bits, containing the control word and a parameter "Type_CW" on 8 bits, defining the type, even or odd, of the control word transmitted.

Of course, the invention is not limited to the exemplary embodiments which are mentioned hereinabove. In particular, the person skilled in the art will be able to introduce any variant into the definition of the identification objects and control-word transmission objects by adding other parameters to these objects.

Moreover, although the invention has been described with reference to the DVB-CI standard it is not limited to the framework of this standard. The invention can in particular be advantageously applied within the framework of the American NRSS (standing for "National Renewable Security Standard") standard.

CLAIMS

1. Multimedia digital terminal (1) intended for receiving a stream (TS(D.EMB.)) of digital data scrambled by control words (CW), said control words being contained in said stream (TS(D.EMB.)) in encrypted form, and intended to cooperate with a detachable module (2) for descrambling said data stream,

said terminal being able to transmit the scrambled data stream (TS(D.EMB.)) to the detachable module,

characterized in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW), and

in that it comprises a descrambler (16) capable of descrambling the digital data stream by using the control words (CW) received from the detachable module (2).

2. Digital terminal according to Claim 1, characterized in that it is furthermore able to receive from the detachable module (2) the scrambled digital data stream (TS'(D.EMB.)), said data stream received by the terminal not being modified relative to the data stream (TS(D.EMB.)) transmitted by the terminal.

3. Digital terminal according to Claim 1, characterized in that it is furthermore able to receive from the detachable module (2) the scrambled digital data stream (TS'(D.EMB.)) from which, relative to the data stream (TS(D.EMB.)) transmitted by the terminal, the data packets containing the control words (CW) have been removed.

4. Digital terminal according to one of Claims 1 to 3, characterized in that said terminal is able to transmit the scrambled data stream (TS(D.EMB.)) to the

detachable module across a first interface (ITTS) with said detachable module, and

in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW) across a second interface (ITCOM) with said module.

5. Terminal according to Claim 4, in combination with Claims 2 and 3, characterized in that it is furthermore able to receive from the detachable module (2), across said first interface (ITTS), the scrambled digital data stream (TS'(D.EMB.)).

6. Multimedia digital terminal (1) intended for receiving a stream (TS(D.EMB.)) of digital data scrambled by control words (CW), said stream of data (TS(D.EMB.)) containing the control words encrypted using a first key (K), and intended to cooperate with a detachable module (2) for descrambling said data stream,

said terminal being able to transmit the scrambled data stream (TS(D.EMB.)) to the detachable module across a first interface (ITTS) with said detachable module,

characterized in that it is furthermore capable of receiving from said detachable module the decrypted control words (CW) which are encrypted using a second key (SSK, K2) before being transmitted across a second interface (ITCOM) with the module (2), and

in that it comprises:

- means for decrypting said control words received from the detachable module using said second key (SSK, K2); and
- a descrambler (16) capable of descrambling the digital data stream (TS(D.EMB.)) by using said decrypted control words (CW).

7. Module (2) intended for cooperating with a digital terminal according to Claim 1, said module being

able to receive from the terminal a scrambled digital data stream (TS(D.EMB.)), characterized in that said module is furthermore capable of:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- transmitting the decrypted control words (CW) to said terminal.

8. Module according to Claim 7, characterized in that it is furthermore adapted for returning the scrambled digital data stream (TS'(D.EMB.)) to the terminal without modifying said stream.

9. Module according to Claim 7, characterized in that it is furthermore adapted for returning the scrambled digital data stream (TS'(D.EMB.)) to the terminal by removing, relative to the data stream (TS(D.EMB.)) transmitted by the terminal, the data packets containing the control words.

10. Module according to one of Claims 7 to 9, characterized in that it is able to receive the digital data stream (TS(D.EMB.)) across a first interface (ITTS) with said terminal (1), and

in that it is furthermore capable of transmitting the decrypted control words to said terminal across a second interface (ITCOM) with said terminal.

11. Module according to one of Claims 7 to 10, characterized in that it is able to cooperate with a detachable security element (3) for decrypting the control words, said module being capable of:

- extracting from the digital data stream (TS(D.EMB.)) messages (ECM) containing the encrypted control words;

- transmitting said messages (ECM) to a security element (3) inserted into said module;
- receiving from said security element (3) the decrypted control words (CW); and
- transmitting the decrypted control words to the digital terminal (1) with which it cooperates.

12. Module (2) intended for cooperating with a digital terminal according to Claim 6, said module being able to receive from the terminal a scrambled digital data stream (TS(D.EMB.)) across a first interface (ITTS) with the terminal (1), characterized in that said module is furthermore capable of:
- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- encrypting said control words using the second key (SSK, K2); and
- transmitting said encrypted control words (CW) to the terminal across a second interface (ITCOM) with said terminal.

13. Module according to one of Claims 10 or 12, characterized in that it pertains to a module according to the DVB-CI standard and in that the first interface (ITTS) of the module is the interface of the transport stream according to the MPEG-2 standard and the second interface (ITCOM) is the control interface.

14. Method for descrambling a stream (TS(D.EMB.)) of digital data, scrambled by control words (CW), which is received by a multimedia digital terminal (1), said control words (CW) being contained in said stream in encrypted form, the method comprising a first step consisting in:

transmitting the scrambled data stream (TS(D.EMB.)) to a detachable module (2),

characterized in that it furthermore comprises the steps consisting, for the detachable module (2), in:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words; and
- transmitting the decrypted control words (CW) to said terminal.

15. Method for descrambling a stream (TS(D.EMB.)) of digital data, scrambled by control words (CW), which is received by a multimedia digital terminal (1), said stream of data containing said control words (CW) encrypted using a first key (K), the method comprising a first step consisting in:

transmitting the scrambled data stream (TS(D.EMB.)) to a detachable module (2),

characterized in that it furthermore comprises the steps consisting, for the detachable module (2), in:

- extracting from the data stream (TS(D.EMB.)) the control words (CW) having served to scramble the digital data;
- decrypting said control words;
- encrypting said control words using a second key (SSK, K2); and
- transmitting the encrypted control words (CW) to said terminal; and,

for the terminal (1), in:

- decrypting said control words using the second key (SSK, K2); and
- descrambling the digital data stream by using said decrypted control words.

16. Method for transferring control words (CW) between a module according to one of Claims 7 to 13 and a

digital terminal according to one of Claim 1 to 6, characterized in that it comprises the steps consisting:

- for the module (2), in sending (100) a first identification object ("CPTS_identification()") to the terminal (1);
- for the terminal (1), in sending (101), in response to said first object, a second identification object ("CPTS_identification_answer()") indicating whether the terminal is or is not able to receive the control words from the module (2); and
- for the module (2), in the event of a positive response with said second object, in sending (102a, 102b, 102i) said control words (CW) enclosed in a third object ("CPTS_CW()").

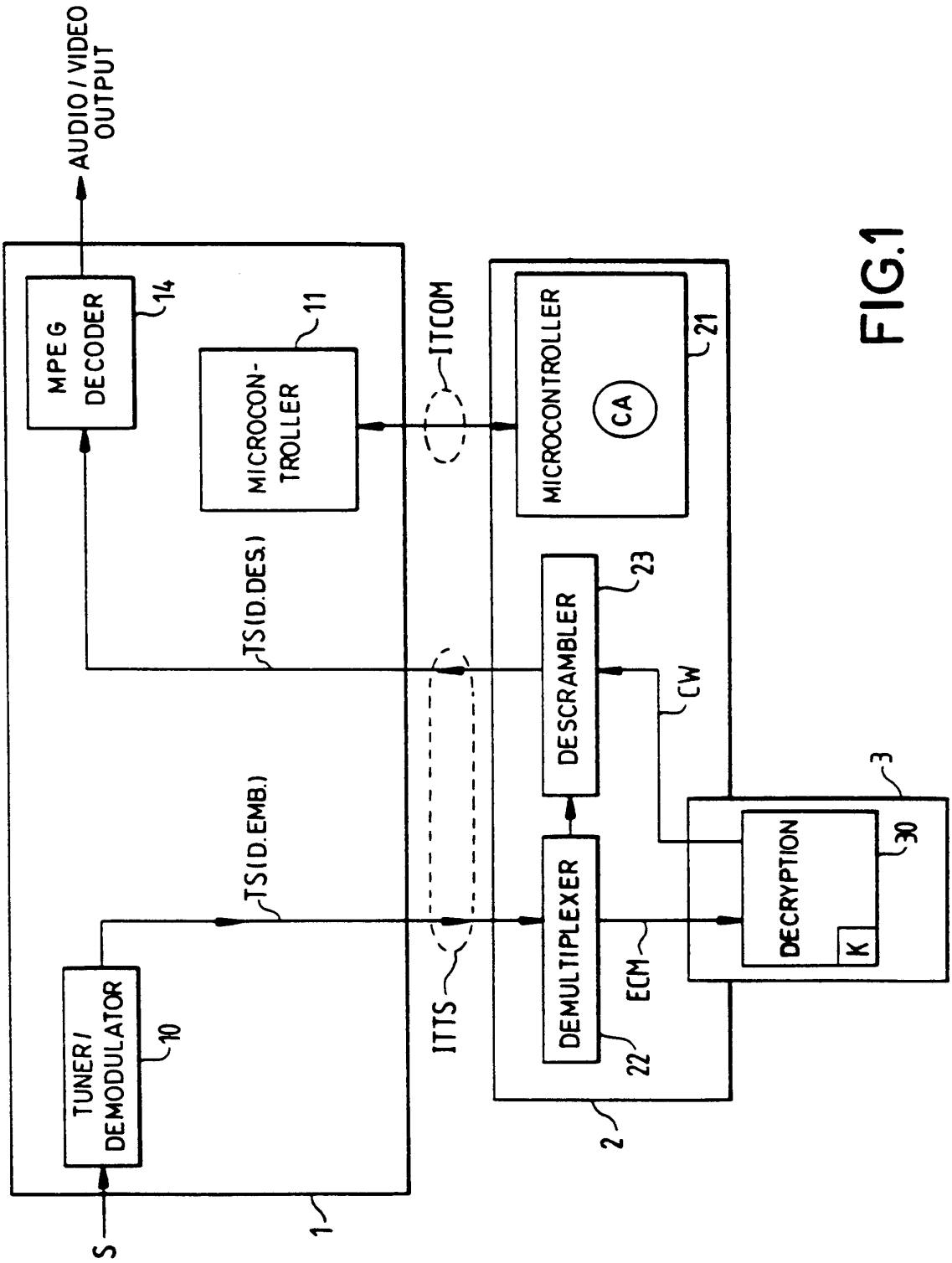

AUDIO / VIDEO OUTPUT
MPEG DECODER
14
MICROCON-TROLLER
11
ITCOM
MICROCONTROLLER
CA
21
TS(D.DES.)
DESCRAMBLER
23
CW
TS(D.EMB.)
DEMULTIPLEXER
ECM
22
DECRYPTION
K
30
3
ITTS
TUNER / DEMODULATOR
10
S
1
2

FIG.1

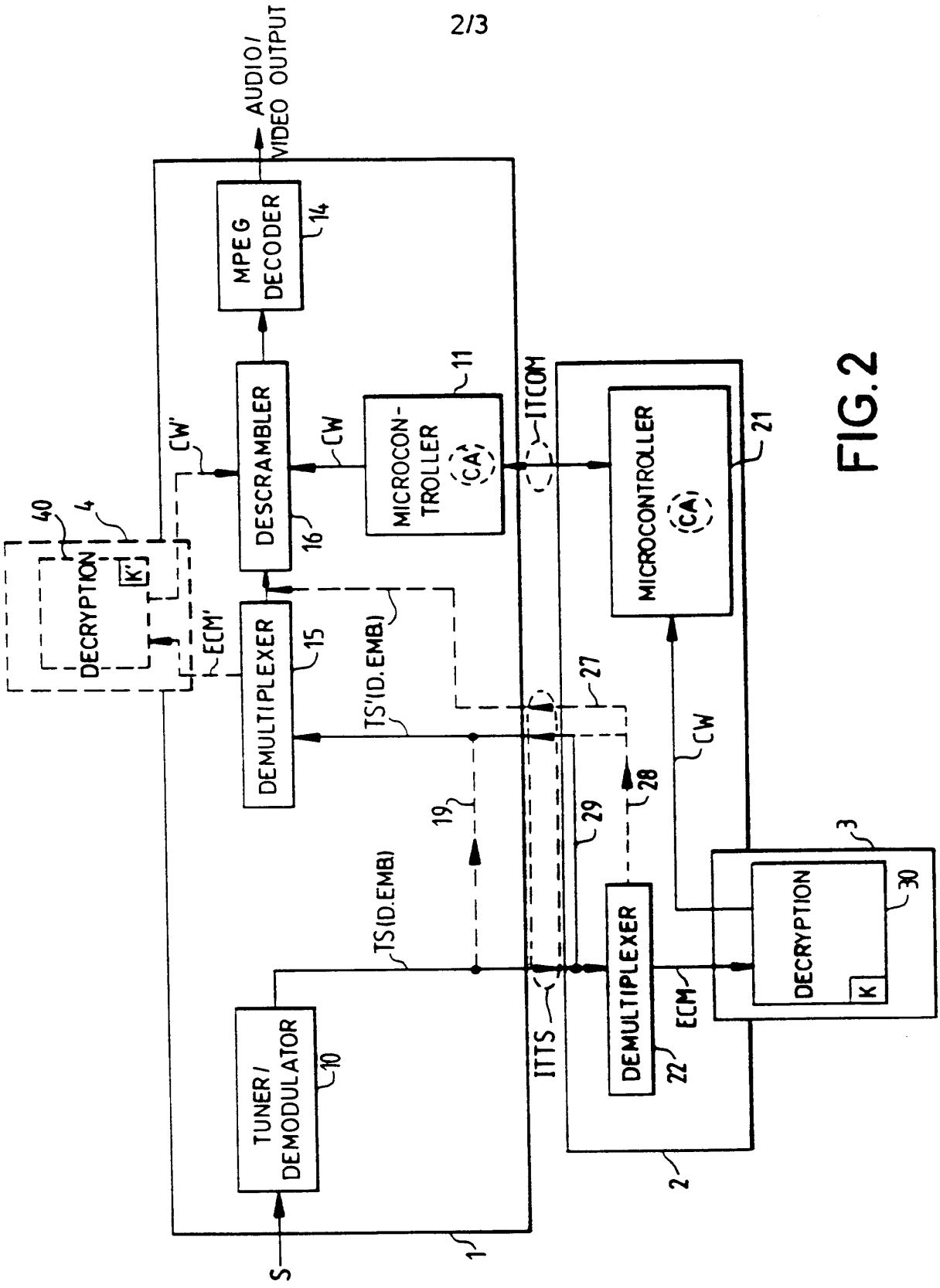

AUDIO/
VIDEO OUTPUT
MPEG
DECODER
14
DESCRAMBLER
16
CW'
CW
MICROCON-
TROLLER
(CA)
11
ITCOM
MICROCONTROLLER
(CA)
21
40
4
DECRYPTION
K'
ECM'
DEMULTIPLEXER
15
TS'(D.EMB)
27
CW
19
29
28
TS(D.EMB)
3
DECRYPTION
K
30
TUNER/
DEMODULATOR
10
ITTS
DEMULTIPLEXER
22
ECM
2
S
1

FIG.2

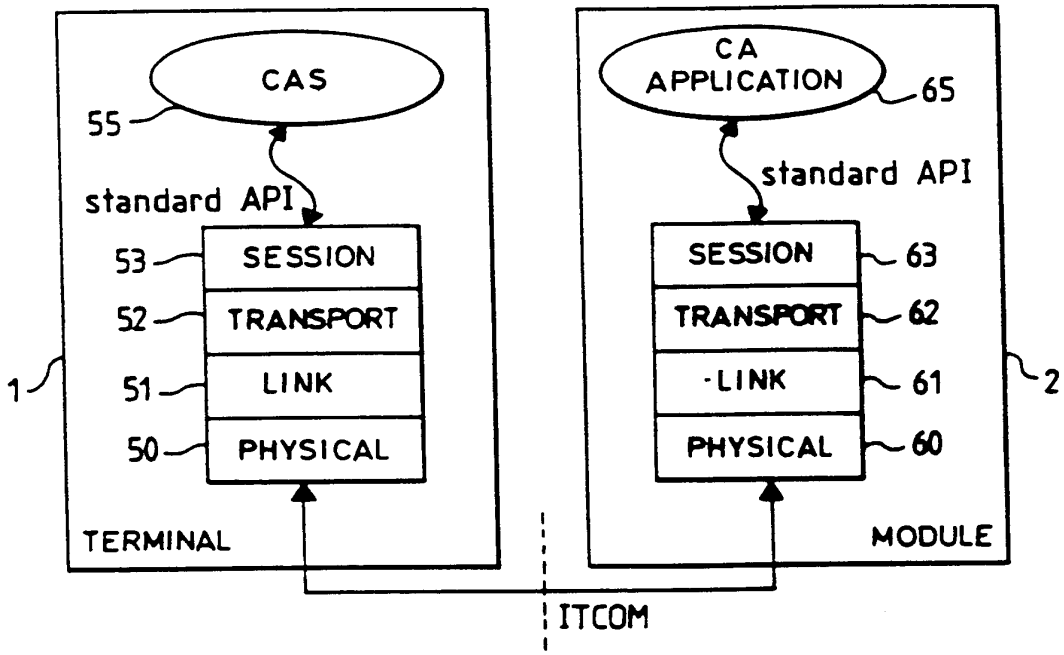

CAS
55
standard API
53
SESSION
52
TRANSPORT
1
51
LINK
50
PHYSICAL
TERMINAL
CA
APPLICATION
65
standard API
SESSION
63
TRANSPORT
62
LINK
61
2
PHYSICAL
60
MODULE
ITCOM

FIG.3

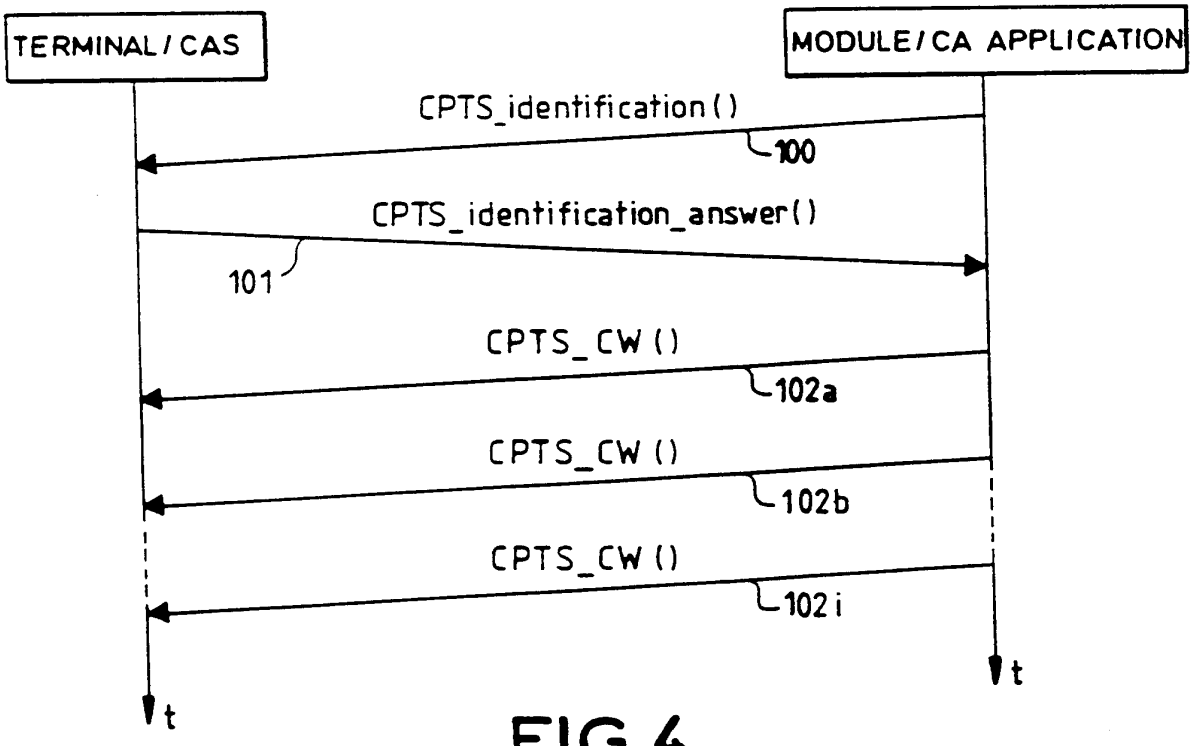

TERMINAL / CAS
MODULE / CA APPLICATION
CPTS_identification()
100
CPTS_identification_answer()
101
CPTS_CW()
102a
CPTS_CW()
102b
CPTS_CW()
102i
t
t

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	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr. 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)

APPLE Ex. 1002, Page 252

INTERNATIONAL SEARCH REPORT

information on patent family members

Interr. nal Application No
PCT/EP 00/08439

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0923245 A	16-06-1999	GB 2332345 A	16-06-1999
		JP 11331801 A	30-11-1999
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		DE 69514843 D	02-03-2000
		DE 69514843 T	18-05-2000
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		ES 2141371 T	16-03-2000
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
EP 0706291 A	10-04-1996	IL 111151 A	24-09-1998
		AU 696725 B	17-09-1998
		AU 3303695 A	18-04-1996
		CA 2159779 A	04-04-1996
		JP 8214278 A	20-08-1996
		US 5666412 A	09-09-1997
		US 5774546 A	30-06-1998
		US 5878134 A	02-03-1999

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
11 octobre 2001 (11.10.2001)

PCT

(10) Numéro de publication internationale
WO 01/75876 A1

(51) Classification internationale des brevets[7] :
G11B 20/00, H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR01/00572

(22) Date de dépôt international :
28 février 2001 (28.02.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/04222 31 mars 2000 (31.03.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THOMSON MULTIMEDIA** [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne-Billancourt (FR).

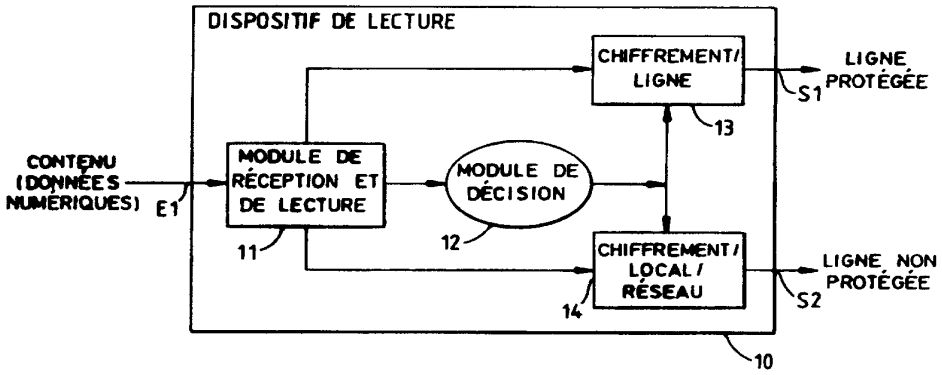
(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **DIEHL, Eric** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **ANDREAUX, Jean-Pierre** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **FURON, Teddy** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **CHEVREAU, Sylvain** [FR/FR]; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Mandataire : **KOHRS, Martin**; Thomson Multimédia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

[Suite sur la page suivante]

(54) Title: DEVICE FOR READING, RECORDING AND RESTORING DIGITAL DATA IN A COPY-PROTECTION SYSTEM FOR SAID DATA

(54) Titre : DISPOSITIFS DE LECTURE, D'ENREGISTREMENT ET DE RESTITUTION DE DONNEES NUMERIQUES DANS UN SYSTEME DE PROTECTION CONTRE LA COPIE DESDITES DONNEES



10...READING DEVICE
13...LINE ENCRYPTION
S1...PROTECTED LINE
S2...UNPROTECTED LINE
14...LOCAL NETWORK ENCRYPTION
12...DECISION MODULE
11...RECEIVING AND READING MODULE
E1...CONTENTS (DIGITAL DATA)

(57) Abstract: The invention concerns a device for reading digital data (10) receiving data representing a content designed to be connected to a digital home network. It comprises: first means for encrypting (13) data in accordance with a protection mode specific to a line whereby the device is to be connected to another digital network device, the encrypted data being in that case supplied to a first output (S1); and second means for encrypting (14) data in accordance with a mode specific to the home network, the encrypted data being in that case supplied to a second output (S2). The invention also concerns a device for recording and restoring digital data designed to be connected to said reading device (10).

[Suite sur la page suivante]

WO 01/75876 A1

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le dispositif de lecture de données numériques (10) recevant des données représentant un contenu est destiné à être raccordé à un réseau numérique domestique. Il comporte: un premier moyen de chiffrement (13) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie (S1); et un deuxième moyen de chiffrement (14) des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie (S2). L'invention concerne également un dispositif d'enregistrement et un dispositif de restitution de données numériques destinés à être raccordés à ce dispositif de lecture (10).

Dispositifs de lecture, d'enregistrement et de restitution de données numériques dans un système de protection contre la copie desdites données

Domaine de l'invention

L'invention se rapporte d'une manière générale au domaine de la protection contre la copie de données numériques, plus particulièrement dans un environnement de réseau numérique domestique.

Etat de la technique

Un réseau numérique domestique peut véhiculer des données numériques issues de différentes sources extérieures au réseau. Il peut s'agir de données stockées sur des supports détachables tels que des disques optiques, par exemple des disques DVD (de l'anglais "*Digital Versatile Disc*" signifiant littéralement "*Disque Numérique Polyvalent*"), ou des bandes magnétiques, les supports étant soit pré-enregistrés, soit enregistrables.

Il peut aussi s'agir de données diffusées puis injectées sur le réseau numérique domestique, par exemple des signaux de télévision numérique diffusés par satellite, par le câble ou encore par des réseaux numériques hertziens. Les données peuvent également être téléchargées en provenance de l'Internet.

Enfin, un réseau numérique domestique peut en outre être amené à gérer des données numériques stockées localement, par exemple dans un disque dur relié au réseau domestique.

Ces données numériques peuvent être séparées en deux grandes catégories: d'une part les données qui ne nécessitent pas de protection particulière (par exemple, celle qui relèvent d'une création personnelle de l'utilisateur du réseau domestique) et d'autre part les données qui doivent être protégées contre la copie pour garantir les intérêts de leur créateur (film, musique, jeux, etc.).

Divers mécanismes et possibilités existent actuellement pour protéger des données numériques contre une copie illégitime.

Les deux principales techniques de protection sont actuellement:

- le chiffrement des données, qui consiste à transformer des données intelligibles (ou "claires") en données chiffrées ou embrouillées à l'aide d'une clé, cette clé étant soit une clé secrète partagée par le dispositif qui chiffre les données et par celui qui est autorisé à les déchiffrer, soit dans les systèmes de cryptographie asymétrique une clé privée ou publique;

- le tatouage des données, qui consiste à insérer de manière non perceptible un tatouage (communément appelé "Watermark") attaché aux données à protéger. Le tatouage doit être non-modifiable et non effaçable même en cas de transformation des données à protéger.

Les deux techniques ci-dessus peuvent naturellement être associées en combinant le tatouage et le chiffrement des données.

Par ailleurs, les données numériques diffusées sont le plus souvent protégées dans le cadre d'un système à accès conditionnel. Dans ce type de système, les données fournies par différents prestataires de services sont transmises sous forme embrouillée par des mots de contrôle CW (de l'anglais "*Control Word*") afin de garantir que les données ne parviennent qu'aux utilisateurs ayant acquis le droit de les recevoir (par exemple moyennant un abonnement au service). Les mots de contrôle sont eux-mêmes transmis dans le flux de données diffusées après avoir été chiffrés avec un algorithme de clé K, cette clé K étant contenue dans un processeur sécurisé, par exemple inclus dans une carte à puce, qui est fournie aux utilisateurs par le prestataire de service pour leur permettre de déchiffrer les mots de contrôle et donc de désembrouiller les données.

Dans les réseaux numériques domestiques, deux grandes méthodes ont été proposées jusqu'à présent pour utiliser et combiner ces techniques de protection:

- la première méthode consiste à protéger les données qui doivent l'être en les chiffrant / embrouillant localement d'un bout à l'autre du réseau (on parle en général de "*end-to-end protection*" – signifiant littéralement "protection d'un bout à l'autre"), c'est à dire dès leur entrée en un point du réseau jusqu'au moment où elle sont restituées à l'utilisateur (affichage de vidéo sur un écran de téléviseur, diffusion de musique par un haut-parleur, etc.), tous les appareils du réseau utilisant le même type de protection, spécifique au réseau domestique. Les données ne sont donc jamais disponibles en clair dans le réseau, que ce soit sur le bus numérique reliant les appareils entre eux ou dans les appareils eux-même, sauf au moment ultime de leur restitution, généralement sous forme analogique, à l'utilisateur ;

- la seconde méthode consiste à associer une protection locale à chaque type d'appareil du réseau (un type de chiffrement particulier, un système d'accès conditionnel, etc.) avec une "protection de ligne" (ou protection "point-à-point"); dans ce type de méthode, les données sont disponibles en clair à l'intérieur des appareils mais ne sont jamais disponibles en clair sur le bus

numérique reliant les différents appareils du réseau entre eux; les données sont en effet re-chiffrées avant d'être transmises sur le bus.

Exposé de l'invention

Un but de la présente invention est de proposer un système permettant de concilier les différentes méthodes de protection qui ont été proposées jusque là.

L'invention concerne à cet effet un dispositif de lecture de données numériques destiné à être raccordé à un réseau numérique domestique et susceptible de recevoir des données représentant un contenu. Celui-ci comporte, selon l'invention :

- un premier moyen de chiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie; et

- un deuxième moyen de chiffrement des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie.

Selon une caractéristique avantageuse de l'invention, le dispositif comporte en outre un module de décision adapté à délivrer une permission ou une interdiction de copie et/ ou de lecture desdites données numériques, lesdites données numériques étant fournies au premier ou au deuxième moyen de chiffrement lorsque ledit module de décision délivre une interdiction de copie ou une permission de copie unique.

Selon une autre caractéristique avantageuse de l'invention, lesdites données numériques sont fournies directement à la première et/ou à la deuxième sortie sans être chiffrées lorsque ledit module de décision délivre une permission de copie illimitée.

Selon une autre caractéristique particulière de l'invention, le dispositif ne fournit aucune données numérique à la première ni à la deuxième sortie lorsque ledit module de décision délivre une interdiction de lecture.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une permission de copie illimitée lorsque lesdites données numériques reçues ne sont pas chiffrées.

Selon une caractéristique préférée de l'invention, le module de décision délivre une permission de copie illimitée lorsqu'en outre lesdites données numériques reçues ne sont pas tatouées.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de lecture lorsque à la fois lesdites données numériques reçues ne sont pas chiffrées et sont tatouées.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de copie lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type enregistrable; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de lecture lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type enregistrable; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une permission de copie unique lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type non-enregistrable ou que ce sont des données diffusées ou téléchargées; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

Selon une autre caractéristique particulière de l'invention, le module de décision délivre une interdiction de copie lorsque lesdites données numériques reçues sont chiffrées; qu'elles sont stockées sur un support de type non-enregistrable ou que ce sont des données diffusées ou téléchargées; et que des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

Selon encore une autre caractéristique avantageuse de l'invention, les informations de permission ou d'interdiction de copie et/ ou de lecture desdites données numériques délivrées par le module de décision sont attachées aux données fournies à la première ou à la deuxième sortie.

Selon un mode de réalisation particulier de l'invention, la première et la deuxième sortie sont reliées respectivement à un unique connecteur pour raccorder le dispositif à un bus numérique du réseau domestique, ledit bus fonctionnant dans un premier mode protégé lorsque les données sont issues de la première sortie et dans un second mode non protégé lorsque les données sont issues de la deuxième sortie.

Avantageusement, le choix de la première ou de la deuxième sortie pour fournir les données est déterminé par le dispositif raccordé au réseau

numérique domestique destiné à recevoir lesdites données émises par le dispositif de lecture sur le réseau domestique.

L'invention concerne également un dispositif d'enregistrement de données numériques destiné à être raccordé à un dispositif de lecture tel que ci-dessus par l'intermédiaire d'un réseau numérique domestique. Selon l'invention, ce dispositif d'enregistrement comporte :

- une première entrée destinée à recevoir des données qui ont été fournies à la première sortie du dispositif de lecture; et
- une seconde entrée destinée à recevoir des données qui ont été fournies à la deuxième sortie du dispositif de lecture.

Selon une caractéristique particulière de l'invention, le dispositif d'enregistrement comporte un moyen de déchiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture, ledit moyen de déchiffrement étant relié à la première entrée du dispositif d'enregistrement.

Selon une autre caractéristique particulière de l'invention, le dispositif d'enregistrement comporte en outre un module de décision adapté à analyser les informations de permission ou d'interdiction de copie et/ou de lecture attachées aux données à enregistrer. Le dispositif d'enregistrement délivre les données à enregistrer à une sortie lorsque le module de décision détecte une permission de copie. Par contre, le dispositif d'enregistrement ne délivre aucune donnée à enregistrer à ladite sortie lorsque le module de décision détecte une interdiction de copie.

L'invention concerne aussi un dispositif de restitution de données numériques destinés à être raccordés à un dispositif de lecture tel que ci-dessus par l'intermédiaire d'un réseau numérique domestique. Selon l'invention, ce dispositif comporte :

- une première entrée destinée à recevoir des données qui ont été fournies à la première sortie du dispositif de lecture et qui est reliée à un premier moyen de déchiffrement des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture ; et
- une seconde entrée destinée à recevoir des données qui ont été fournies à la deuxième sortie dudit dispositif de lecture et qui est reliée à un deuxième moyen de déchiffrement des données selon un mode de protection spécifique au réseau domestique.

Brève description des dessins

L'invention sera mieux comprise à la lecture de la description suivante d'un mode de réalisation particulier, non limitatif, de celle-ci faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente un réseau numérique domestique servant à illustrer le principe de l'invention ;
- la figure 2 représente un dispositif de lecture de données numériques selon l'invention destiné à être raccordé à un réseau domestique;
- la figure 3 représente un dispositif d'enregistrement de données numériques selon l'invention destiné à être raccordé à un réseau domestique;
- la figure 4 représente un dispositif de restitution de données numériques destiné à être raccordé à un réseau domestique;
- la figure 5 illustre un procédé mis en œuvre dans le dispositif de la figure 2 ; et
- la figure 6 illustre un procédé mis en œuvre dans le dispositif de la figure 3.

Description détaillée de modes de réalisation de l'invention

Sur la figure 1, on a représenté un exemple de réseau numérique domestique. Celui-ci se compose d'un certain nombre de dispositifs reliés entre eux par un bus numérique B, par exemple un bus selon la norme IEEE 1394. Ces dispositifs peuvent être divisés en trois catégories :

- les dispositifs de lecture qui sont capables de recevoir des données numériques en provenance de différentes sources de données; sur la figure 1, deux exemples de ces dispositifs sont représentés: le décodeur 1 recevant des données d'une antenne satellite 6, notamment des programmes de télévision numérique, et le lecteur DVD 2 capable de lire des disques DVD 5 ;
- les dispositifs d'enregistrement de données, tel le dispositif 3, qui sont capables d'enregistrer le contenu des données lues par les dispositifs de lecture sur des supports d'enregistrement persistants ; et
- les dispositifs de restitution, tel le téléviseur numérique 4 de la figure 1, qui sont prévus pour restituer le contenu de données lues par un dispositif de lecture.

Bien entendu, cette séparation entre les trois catégories de dispositifs est faite pour les besoins de simplification de l'explication et un appareil d'électronique grand public réel peut très bien regrouper deux catégories de dispositifs décrits ci-dessus, voire les trois. Par exemple, un

téléviseur numérique peut contenir aussi le dispositif de lecture des émissions diffusées sous forme numérique ou bien un lecteur de DVD peut aussi contenir un dispositif d'enregistrement.

Sur la figure 2, on a représenté un dispositif de lecture 10 selon l'invention. Celui-ci reçoit sur son entrée E1 des données numériques représentant un contenu. Ce contenu peut être un contenu pré-enregistré, un contenu enregistré dans le réseau, un contenu diffusé ou un contenu téléchargé. Les données numériques sont reçues par un module de réception et de lecture 11 qui est capable d'interpréter le format des données reçues. En fait ce module est différent selon le type d'appareil appartenant à la première catégorie. Ce module a des fonctions dédiées selon le type de contenu qu'il reçoit: ainsi, si le dispositif de lecture est un lecteur de DVD Vidéo, le module 11 reconnaîtra le format de données embrouillées selon le système CSS (de l'anglais "*Content Scramble System*" signifiant littéralement "*Système d'Embrouillage de Contenu*") utilisé habituellement pour protéger le contenu des disques DVD et sera capable de désembrouiller les données; si le dispositif de lecture est un décodeur numérique, le module 11 reconnaîtra le format de flux de données diffusées protégées par un système d'accès conditionnel et sera capable de désembrouiller les données si l'utilisateur possède les droits nécessaires.

Le dispositif de lecture comprend en outre un module de décision 12 qui effectue un contrôle sur la lecture des données, c'est à dire qu'il détermine si les données lues en entrée peuvent être copiées librement (statut "*Copy-Free*"), ne peuvent être copiées qu'une seule fois (statut "*Copy-Once*"), ne peuvent plus être copiées (statut "*Copy-No-More*"), ne peuvent jamais être copiées (statut "*Copy-Never*") ou bien si ces données lues représentent une copie illégale et ne doivent donc pas être restituées sur un dispositif de restitution. Pour déterminer ces différents statuts, le module de décision utilise un procédé qui sera décrit plus bas en liaison avec la figure 5, à partir, soit de l'ensemble du flux de données qu'il reçoit du module de réception et de lecture 11, soit de seulement certaines informations extraites de ce flux de données, selon le type d'implémentation choisie par l'homme du métier.

Il génère en sortie des informations de gestion de génération de copie, par exemple des informations au format CGMS (de l'anglais "*Copy Generation Management Status*" signifiant littéralement "*Statut pour la Gestion des Générations de Copies*"), qui sont ensuite utilisées par les dispositifs d'enregistrement ou de restitution pour déterminer si les données peuvent être enregistrées ou copiées.

En pratique, ces informations sont transmises à deux modules de chiffrement de sortie 13 et 14 qui, en fonction des informations de gestion de génération de copie reçues, fournissent les données respectivement aux sorties S1 ou S2 sous forme protégée ou non, les informations concernant le statut des données étant également transmises en sortie dans le flux de données.

Si l'information de gestion de génération de copie indique que les données lues représentent une copie illégale, les modules de chiffrement 13 ou 14 ne fourniront aucune donnée en sortie. Il ne sera ainsi pas possible de visualiser le contenu, par exemple s'il s'agit d'un film, ou de l'enregistrer.

Si ces informations indiquent que les données ont un statut "*Copy-Free*", c'est à dire qu'elles peuvent être copiées librement, les données seront transmises sur l'une ou l'autre des sorties S1 ou S2 ou sur les deux sans être chiffrées.

Par contre si ces information indiquent que les données ont un statut "*Copy-No-More*" ou "*Copy-Never*" ou "*Copy-Once*", elles seront transmises aux sorties S1 ou S2 sous forme chiffrée.

Selon l'invention, le dispositif de lecture comprend deux modules de chiffrement de sortie différents. Les sorties S1 et S2 du dispositif sont des sorties numériques, c'est à dire qu'elles sont destinées à être reliées à un bus numérique. Par contre, elles utilisent chacune un mode de protection différent.

Pour la sortie S1, les données sont protégées au niveau de la ligne, par exemple selon la proposition de protection "DTCP" pour un bus numérique selon la norme IEEE 1394 ("DTCP" est un acronyme de "*Digital Transmission Content Protection*", aussi connu sous le nom de "5C", pour laquelle on pourra se référer pour plus de détails à la publication *"5C Digital Transmission Content Protection White Paper", Rev. 1.0, 14 juillet 1998*, disponible à l'adresse Internet suivante *http://www.dtcp.com/*). Lorsque cette sortie est utilisée, les données sont chiffrées par le module de chiffrement 13 de manière spécifique pour la ligne.

La sortie S2 conduit quant à elle à une ligne non protégée. Dans ce cas, les données sont chiffrées selon un mode de protection local du réseau domestique, de manière à ce que le contenu soit protégé. On pourra notamment utiliser le mode de chiffrement local des données conforme à la proposition XCA (acronyme de "eXtended Conditional Access", pour laquelle on pourra se référer pour plus de détails à la publication "*XCA, A Global Copy Protection System for Home Networks, White Paper v. 1.2*" publiée le 6 janvier 2000). Dans le cas où cette sortie S2 est utilisée, les données sont chiffrées par le module de chiffrement local 14.

Les sorties S1 et S2 du dispositif de lecture ont été représentées de manière séparée à la figure 1 mais il peut en réalité s'agir d'un seul connecteur de sortie permettant de connecter le dispositif au bus B du réseau domestique. Dans ce cas, le bus numérique pourra comporter deux modes distincts de fonctionnement: le mode protégé dans lequel les données sont chiffrées pour une liaison spécifique entre deux appareils du réseau et le mode non protégé dans lequel les données sont chiffrées de manière globale au niveau du réseau.

Le choix du type de sortie dépend en fait de l'appareil destiné à recevoir les données lues par le dispositif de lecture. En effet, le dispositif de lecture de l'invention est destiné à pouvoir être utilisé en liaison avec d'autres dispositifs qui ne supportent qu'un seul mode de protection: soit celui au niveau de la ligne, soit celui au niveau du réseau local. Entre le dispositif qui reçoit les données et celui qui les émet sur le bus à son intention, il existe de manière connue un échange lors duquel le dispositif de lecture connaît le type de protection supporté par l'appareil destinataire et peut ainsi déterminer quelle sortie S1 ou S2 sera choisie pour transmettre les données. Si l'appareil destiné à recevoir les données supporte les deux modes de protection tout comme le dispositif de lecture, le choix de la sortie S1 ou S2 sera prédéterminé selon l'implémentation choisie par l'homme du métier. Il est également possible dans ce cas d'utiliser les deux sorties, c'est à dire de transmettre les données à la fois sur la ligne protégée et sur la ligne non protégée, si celles-ci sont physiquement séparées.

En liaison avec la figure 5, nous allons maintenant décrire le procédé mis en œuvre par le module de décision 12 pour déterminer le statut des données pour la gestion de génération de copie.

Le premier test 100 consiste à vérifier si les données reçues sont chiffrées. Si ce n'est pas le cas (sortie "*N*"), cela signifie que l'on a affaire à un contenu qui est une création de l'utilisateur ou bien à un contenu qui a été piraté. C'est pourquoi un test supplémentaire 101 peut être effectué de manière préférentielle mais non obligatoire, pour déterminer si le contenu est tatoué. Si la réponse est positive (sortie "*O*"), cela signifie que le contenu a été piraté et le dispositif de lecture doit refuser de le lire (sortie "*STOP!*"). Si par contre, le contenu n'est pas tatoué (sortie "*N*" au test 101), alors le contenu est effectivement libre de copie et le statut "*Copy-Free*" lui est attribué.

Si la réponse au premier test 100 est positive (sortie "*O*"), c'est à dire si les données reçues sont chiffrées, le test suivant 102 consiste à détecter le type de support du contenu. Ceci s'applique en particulier pour les supports

détachables tels que les DVD qui peuvent être du type "*Enregistrable*" (par exemple les formats DVD-RAM, DVD-RW, DVD-R) ou du type "*Non enregistrable*" (par exemple DVD-ROM ou DVD vidéo pré-enregistré). Les données diffusées ou téléchargées seront par convention du type "*Non enregistrable*".

Si le support du contenu est du type "*Enregistrable*", le test suivant 103 consiste à détecter si le fournisseur du contenu a donné le droit d'effectuer une copie unique (statut "*Copy-Once*") ou aucune copie (statut "*Copy-Never*") de son contenu. Ces informations de contrôle de la copie communément notées CCI (acronyme de l'anglais "*Copy Control Information*") ou encore CGMS (acronyme de l'anglais "*Copy Generation Management System*" signifiant "système de gestion de la génération de copie") sont présentes dans les données sous une forme déterminée par le fournisseur du contenu et qui est bien connue de l'homme du métier. Si un support du type "*Enregistrable*" a un statut "*Copy-Once*", cela signifie que le support est lui-même la copie unique et qu'il ne doit plus être autorisé de copie. Par conséquent le statut de sortie sera "*Copy-No-More*". Par contre, si celui-ci a un statut "*Copy-Never*", cela signifie qu'il s'agit d'une copie pirate et celle-ci ne doit pas être lue par le dispositif de lecture (sortie "*STOP!*").

Il est à noter que le statut "*Copy-No-More*" signifie qu'il est interdit d'effectuer une génération supplémentaire de copie des données reçues. Ce statut signifie également, dans le cas où nous avons une protection locale au niveau du réseau (par exemple selon la proposition XCA), qu'il est possible d'effectuer une copie locale des données, cette copie n'étant lisible par aucun autre dispositif que ceux du réseau dans lequel elle a été copiée, ou en d'autres termes qu'il n'est pas possible d'effectuer une génération supplémentaire de copie pour un autre réseau domestique.

Si le support du contenu est du type "*Non-enregistrable*" ou si les données reçues sont des données diffusées ou téléchargées, le même test que le test 103 est effectué (test 104) et le statut détecté ("*Copy-Once*" ou "*Copy-Never*") correspond au statut de sortie attribué aux données.

Le statut "*Copy-Once*" autorise également la copie locale au niveau du réseau domestique lorsque nous avons un mode de protection local au réseau.

Nous allons maintenant décrire un dispositif d'enregistrement 20 selon l'invention tel que représenté schématiquement à la figure 3.

Celui-ci comporte deux entrées numériques E2 et E3, la première E2 recevant les données par une ligne protégée et la seconde E3 par une ligne non protégée. Comme on l'a vu plus haut, il peut s'agir en réalité d'une seule connexion physique avec un bus numérique capable de fonctionner dans un mode "protégé" ou dans un mode "non protégé". Le choix de l'entrée dépend du type d'appareil avec lequel le dispositif d'enregistrement est relié et des modes de protection supportés par cet appareil.

Dans le cas où les données sont reçues sur l'entrée E2, elles sont transmises à un module de déchiffrement 21 qui effectue un déchiffrement en utilisant une clé spécifique de la ligne, qui a par exemple été échangée avec le dispositif de lecture ayant envoyé les données sur la ligne.

Les informations concernant le statut des données, c'est à dire les informations de gestion de génération de copie des données, sont extraites du flux de données et analysées par un module de décision 22 selon le procédé qui sera décrit en liaison avec la figure 6 ci-dessous. Celui-ci effectue le contrôle de la copie au niveau du dispositif d'enregistrement.

Si le statut détecté est du type "*Copy-No-More*" ou "*Copy-Never*", l'enregistrement est stoppé et le module de décision 22 donne l'instruction au module de mise en forme pour l'enregistrement 23 de ne transmettre aucune donnée en sortie pour l'enregistrement.

Si en revanche le statut détecté est du type "*Copy-Once*", le module de décision 22 donne l'instruction au module 23 d'effectuer une mise en forme pour l'enregistrement de manière à ce que les données ne soient pas enregistrées en clair. Il peut s'agir par exemple d'un chiffrement selon la proposition CPRM (acronyme de "*Content Protection for Recordable Media*" signifiant littéralement "*Protection de Copie pour Support Enregistrable*" pour laquelle on pourra trouver plus de détails à l'adresse Internet suivante : *http://www.4centity.com/4centity/tech/cprm/*). Les données mises en forme sont ensuite transmises en sortie S3 pour être stockées sur un support d'enregistrement 24.

Lorsque le statut détecté par le module de décision 22 est du type "*Copy-Free*", l'enregistrement des données peut être effectué en clair, c'est à dire sans que les données ne soient mises en forme par le module 23.

Dans le cas où les données sont reçues sur l'entrée E3, elles sont déjà protégées par un chiffrement local au niveau du réseau. Dans ce cas, le dispositif d'enregistrement n'effectue aucun traitement et se contente d'enregistrer les données sous forme chiffrée.

En liaison avec la figure 6, nous allons maintenant décrire le procédé mis en œuvre dans le module de décision 22 du dispositif d'enregistrement.

Le module 22 a deux sources d'informations pour connaître le statut des données vis à vis de la gestion des générations de copie: les informations définies par le système de protection au niveau de la ligne – ces informations étant analysées à l'étape 110 – et les informations intégrées dans le contenu même des données transmises sur la ligne non protégée – informations analysées à l'étape 111. En principe, les deux sources doivent fournir les mêmes statuts de données mais, de manière préférentielle, et pour améliorer la sécurité du système, un test supplémentaire 112 est effectué pour définir le statut le plus restrictif parmi les informations reçues.

L'ordre de restriction parmi les statuts est le suivant:

"*Copy-Never*" = "*Copy-No-More*" > "*Copy-Once*" > "*Copy-Free*" ;

">" signifiant "est plus restrictif que".

Par exemple, si une information analysée à l'étape 110 indique un statut "*Copy-Once*" tandis que celle analysée à l'étape 111 indique un statut "*Copy-Free*", le statut retenu à l'étape 112 sera "*Copy-Once*".

Ensuite, selon le statut défini à l'étape 112, le module de décision 22 du dispositif d'enregistrement autorisera l'enregistrement (statuts "*Copy-Free*" ou "*Copy-Once*") ou bien n'autorisera pas l'enregistrement (statuts "*Copy-No-More*" ou "*Copy-Never*").

Il est à noter que les données reçues sur la ligne non protégée pourront toujours être enregistrées puisque celles-ci bénéficient déjà d'une protection spécifique au réseau local, c'est à dire qu'elles sont chiffrées de telle sorte qu'elles ne peuvent être lues (et restituées) que par un appareil du réseau.

Nous allons maintenant décrire un dispositif de restitution de données 30 selon l'invention tel que représenté à la figure 4.

Celui-ci comporte, comme le dispositif d'enregistrement 20, deux entrées numériques E4 et E5, reliées respectivement à une ligne protégée et à une ligne non protégée. Lorsque les données sont reçues sur l'entrée E4, celles-ci sont déchiffrées par le module de déchiffrement 31 spécifique à la ligne. Elles sont ensuite transmises en sortie S4 pour être restituées. Par exemple, s'il s'agit d'un téléviseur numérique, les données sont transmises au moyen d'affichage (tube cathodique, écran plasma, etc.) pour être visualisées.

Lorsque les données sont reçues sur l'entrée E5, elles sont transmises à un module de déchiffrement local 32 spécifique au réseau dans

lequel se trouve le dispositif. Ce module constitue la fin de la protection "d'un bout à l'autre" du réseau puisque les données ne sont déchiffrées, dans ce mode de protection, que pour être restituées en sortie S4 du dispositif.

Les dispositifs de lecture, d'enregistrement et de restitution de l'invention sont ainsi compatibles avec les différents modes de protection existants dans les réseaux numériques domestiques et permettent ainsi une meilleure interopérabilité des systèmes de protection contre la copie illicite.

Il est à noter que le terme "ligne" tel qu'employé dans toute la description s'entend de tout canal de communication dans un réseau numérique, que ce canal soit constitué par une ligne physique ou par une voie de communication dite "sans fil".

REVENDICATIONS

1. Dispositif de lecture de données numériques (1, 2, 10) destiné à être raccordé à un réseau numérique domestique et susceptible de recevoir des données représentant un contenu, caractérisé en ce qu'il comporte :

- un premier moyen de chiffrement (13) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé à un autre dispositif du réseau numérique, les données chiffrées étant dans ce cas fournies à une première sortie (S1) ; et
- un deuxième moyen de chiffrement (14) des données selon un mode de protection spécifique au réseau domestique, les données chiffrées étant dans ce cas fournies à une deuxième sortie (S2).

2. Dispositif selon la revendication 1, caractérisé en ce qu'il comporte en outre un module de décision (12) adapté à délivrer une permission ou une interdiction de copie et/ ou de lecture desdites données numériques,

lesdites données numériques étant fournies au premier (13) ou au deuxième (14) moyen de chiffrement lorsque ledit module de décision (12) délivre une interdiction de copie ("Copy-Never"; "Copy-No-More") ou une permission de copie unique ("Copy-Once").

3. Dispositif selon la revendication 2, caractérisé en ce que lesdites données numériques sont fournies directement à la première (S1) et/ou à la deuxième (S2) sortie sans être chiffrées lorsque ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free").

4. Dispositif selon l'une des revendications 2 ou 3, caractérisé en ce qu'il ne fournit aucune données numérique à la première (S1) ni à la deuxième (S2) sortie lorsque ledit module de décision (12) délivre une interdiction de lecture ("STOP!").

5. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free") lorsque lesdites données numériques reçues ne sont pas chiffrées.

6. Dispositif selon la revendication 5, caractérisé en ce que ledit module de décision (12) délivre une permission de copie illimitée ("Copy-Free") lorsqu'en outre lesdites données numériques reçues ne sont pas tatouées.

7. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de lecture ("STOP!") lorsque:

- lesdites données numériques reçues ne sont pas chiffrées ; et
- lesdites données numériques reçues sont tatouées.

8. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de copie ("Copy-No-More") lorsque :

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type enregistrable; et
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

9. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de lecture ("STOP!") lorsque:

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type enregistrable; et
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

10. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une permission de copie unique ("Copy-Once") lorsque:

- lesdites données numériques reçues sont chiffrées; et
- lesdites données numériques reçues sont stockées sur un support de type non-enregistrable ou sont des données diffusées ou téléchargées;
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'une copie unique est autorisée.

11. Dispositif selon l'une des revendications 2 à 4, caractérisé en ce que ledit module de décision (12) délivre une interdiction de copie ("Copy-Never") lorsque :

- lesdites données numériques reçues sont chiffrées;
- lesdites données numériques reçues sont stockées sur un support de type non-enregistrable ou sont des données diffusées ou téléchargées;
- des informations de contrôle de la copie contenues dans lesdites données indiquent qu'aucune copie n'est autorisée.

12. Dispositif selon l'une des revendications précédentes, caractérisé en ce que les informations de permission ou d'interdiction de copie et/ ou de lecture desdites données numériques délivrées par le module de décision (12) sont attachées aux données fournies à la première (S1) ou à la deuxième (S2) sortie.

13. Dispositif selon l'une des revendications précédentes, caractérisé en ce que la première (S1) et la deuxième (S2) sortie sont reliées respectivement à un unique connecteur pour raccorder ledit dispositif à un bus numérique (B) du réseau domestique, ledit bus fonctionnant dans un premier mode protégé lorsque les données sont issues de la première sortie (S1) et dans un second mode non protégé lorsque les données sont issues de la deuxième sortie (S2).

14. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le choix de la première (S1) ou de la deuxième (S2) sortie pour fournir les données est déterminé par le dispositif raccordé audit réseau numérique domestique destiné à recevoir lesdites données émises par ledit dispositif de lecture sur ledit réseau domestique.

15. Dispositif d'enregistrement de données numériques (3, 20) destiné à être raccordé à un dispositif de lecture (1, 2, 10) selon l'une des revendications 1 à 14 par l'intermédiaire d'un réseau numérique domestique, caractérisé en ce qu'il comporte :

- une première entrée (E2) destinée à recevoir des données qui ont été fournies à la première sortie (S1) dudit dispositif de lecture (10); et
- une seconde entrée (E3) destinée à recevoir des données qui ont été fournies à la deuxième sortie (S2) dudit dispositif de lecture (10).

16. Dispositif selon la revendication 15, caractérisé en ce qu'il comporte un moyen de déchiffrement (21) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture, ledit moyen de déchiffrement (21) étant relié à la première entrée (E2) dudit dispositif d'enregistrement.

17. Dispositif selon l'une des revendications 15 ou 16 prises dans leur dépendance de la revendication 12, caractérisé en ce qu'il comporte en outre un module de décision (22) adapté à analyser les informations de permission ou d'interdiction de copie et/ou de lecture attachées aux données à enregistrer,

ledit dispositif d'enregistrement délivrant lesdites données à enregistrer à une sortie (S3) lorsque ledit module de décision (22) détecte une permission de copie ("Copy-Once"; "Copy-free") ;

ledit dispositif d'enregistrement ne délivrant aucune donnée à enregistrer à ladite sortie (S3) lorsque ledit module de décision (22) détecte une interdiction de copie ("Copy-No-More"; "Copy-Never").

18. Dispositif de restitution de données numériques (4, 30) destiné à être raccordé à un dispositif de lecture (1, 2, 10) selon l'une des revendications 1 à 14 par l'intermédiaire d'un réseau numérique domestique, caractérisé en ce qu'il comporte:

- une première entrée (E4) destinée à recevoir des données qui ont été fournies à la première sortie (S1) dudit dispositif de lecture (10) et qui est reliée à un premier moyen de déchiffrement (31) des données selon un mode de protection spécifique à une ligne avec laquelle le dispositif est destiné à être raccordé au dispositif de lecture ;

- une seconde entrée (E5) destinée à recevoir des données qui ont été fournies à la deuxième sortie (S2) dudit dispositif de lecture (10) et qui est reliée à un deuxième moyen de déchiffrement (32) des données selon un mode de protection spécifique au réseau domestique ; et

- une sortie (S4) pour la restitution des données, reliée au premier et au deuxième moyen de déchiffrement.

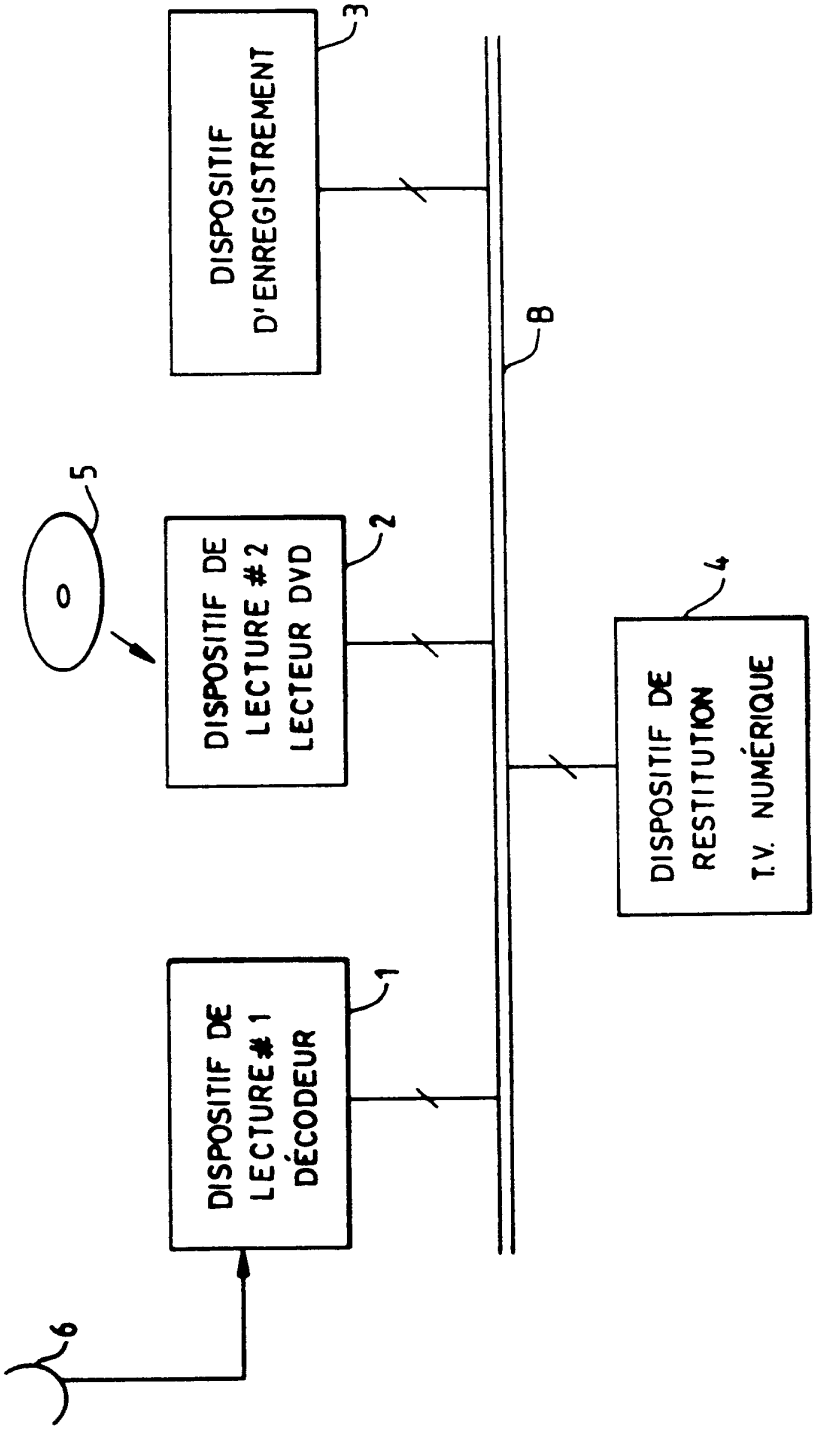

DISPOSITIF D'ENREGISTREMENT
3
8
5
DISPOSITIF DE LECTURE #2 LECTEUR DVD
2
4
DISPOSITIF DE RESTITUTION T.V. NUMÉRIQUE
DISPOSITIF DE LECTURE # 1 DÉCODEUR
1
6

FIG.1

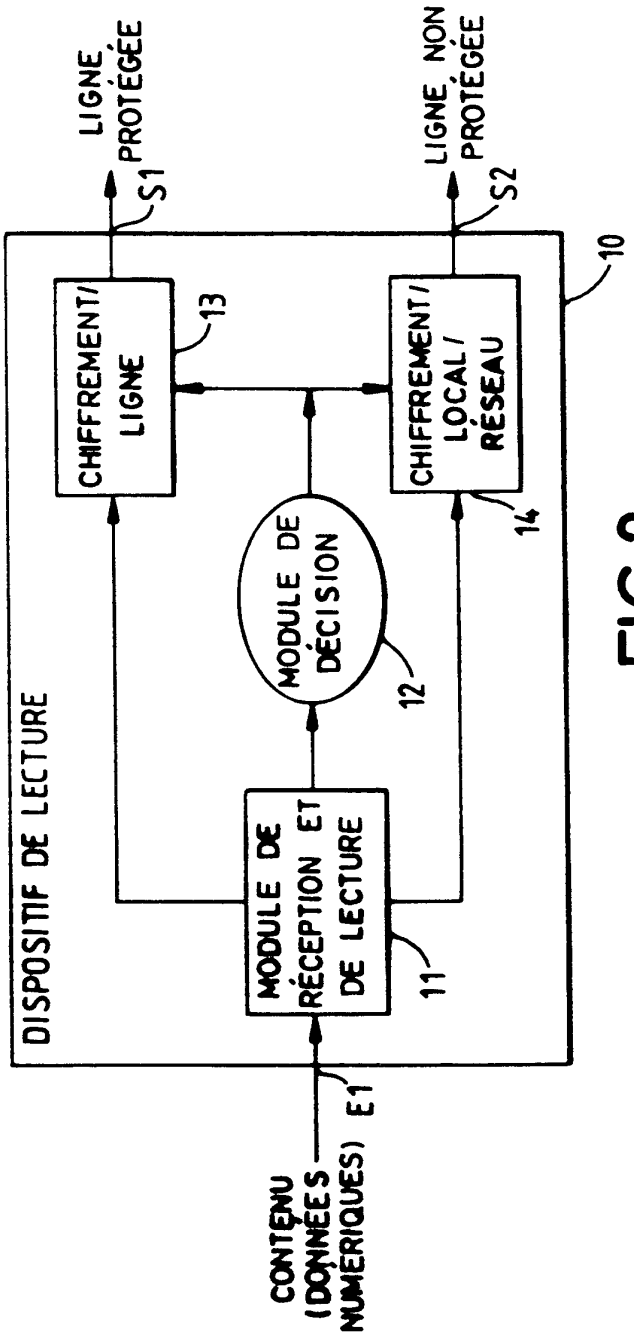

LIGNE PROTÉGÉE
S1
LIGNE NON PROTÉGÉE
S2
10
CHIFFREMENT/ LIGNE
13
CHIFFREMENT/ LOCAL/ RÉSEAU
14
MODULE DE DÉCISION
12
MODULE DE RÉCEPTION ET DE LECTURE
11
DISPOSITIF DE LECTURE
E1
CONTENU (DONNÉES NUMÉRIQUES)

FIG.2

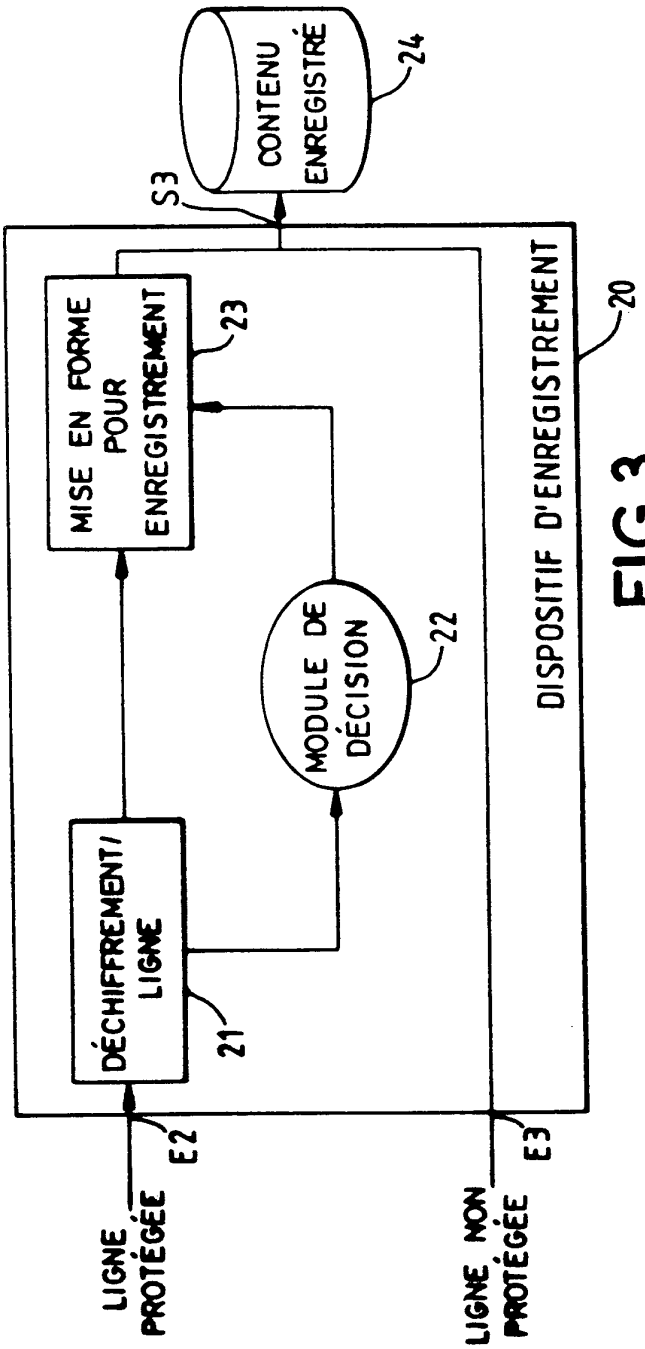

CONTENU ENREGISTRÉ
24
S3
MISE EN FORME POUR ENREGISTREMENT
23
MODULE DE DÉCISION
22
DÉCHIFFREMENT/ LIGNE
21
DISPOSITIF D'ENREGISTREMENT
20
E2
E3
LIGNE PROTÉGÉE
LIGNE NON PROTÉGÉE

FIG.3

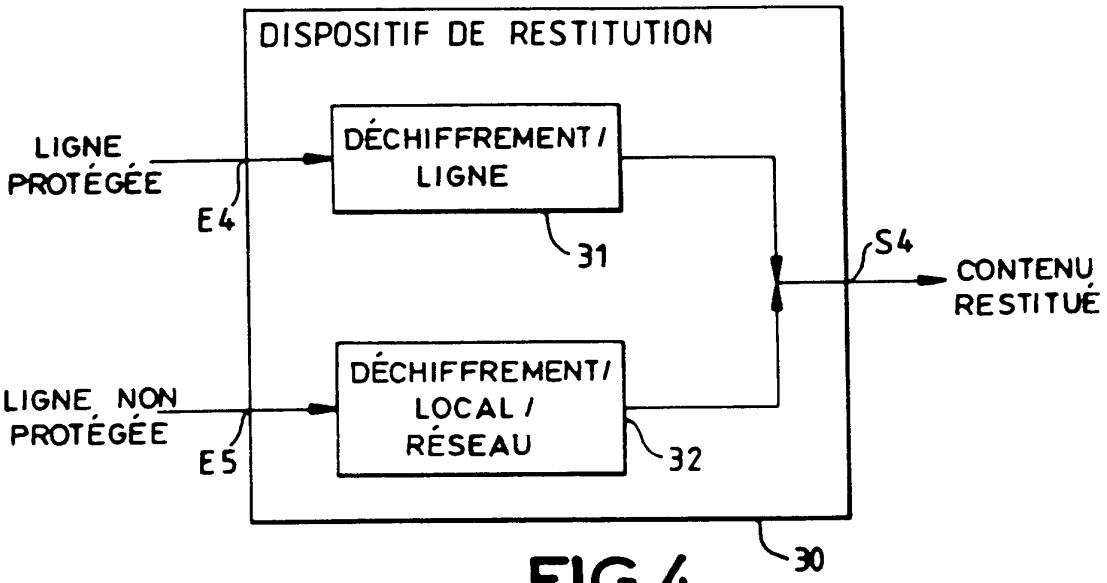

DISPOSITIF DE RESTITUTION
LIGNE PROTÉGÉE
E4
DÉCHIFFREMENT / LIGNE
31
S4
CONTENU RESTITUÉ
LIGNE NON PROTÉGÉE
E5
DÉCHIFFREMENT / LOCAL / RÉSEAU
32
30

FIG.4

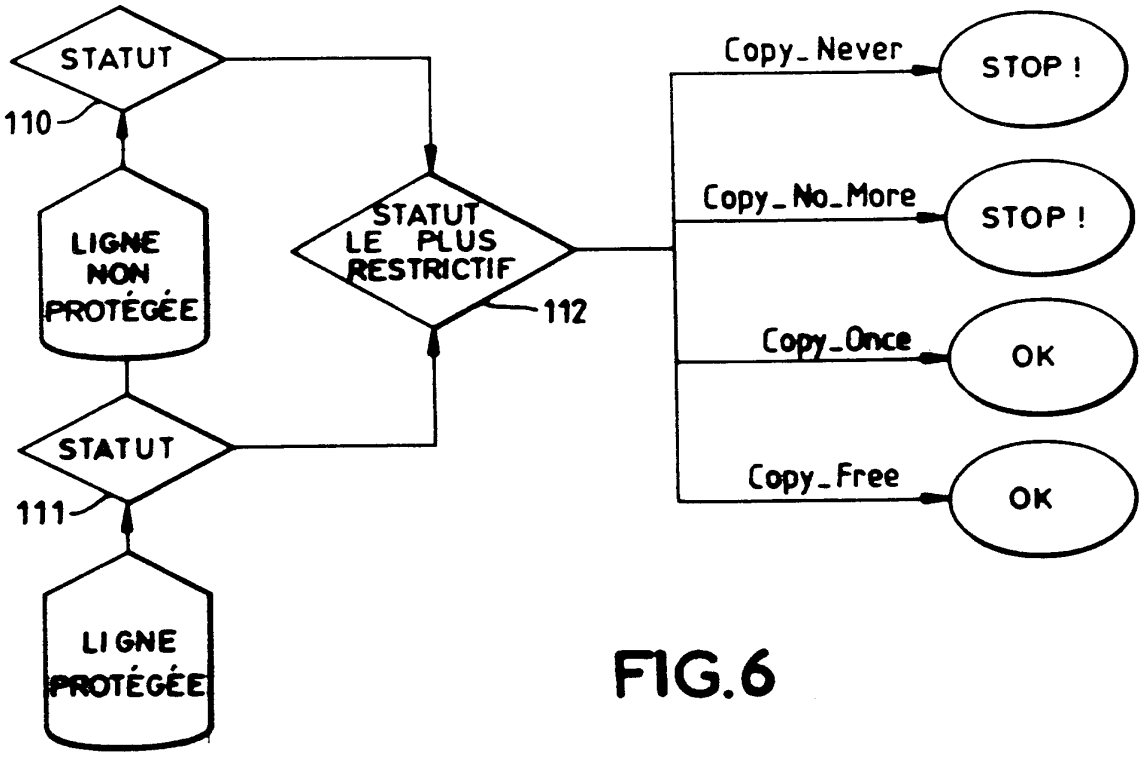

STATUT
110
LIGNE NON PROTÉGÉE
STATUT
111
LIGNE PROTÉGÉE
STATUT LE PLUS RESTRICTIF
112
Copy_Never
STOP !
Copy_No_More
STOP !
Copy_Once
OK
Copy_Free
OK

FIG.6

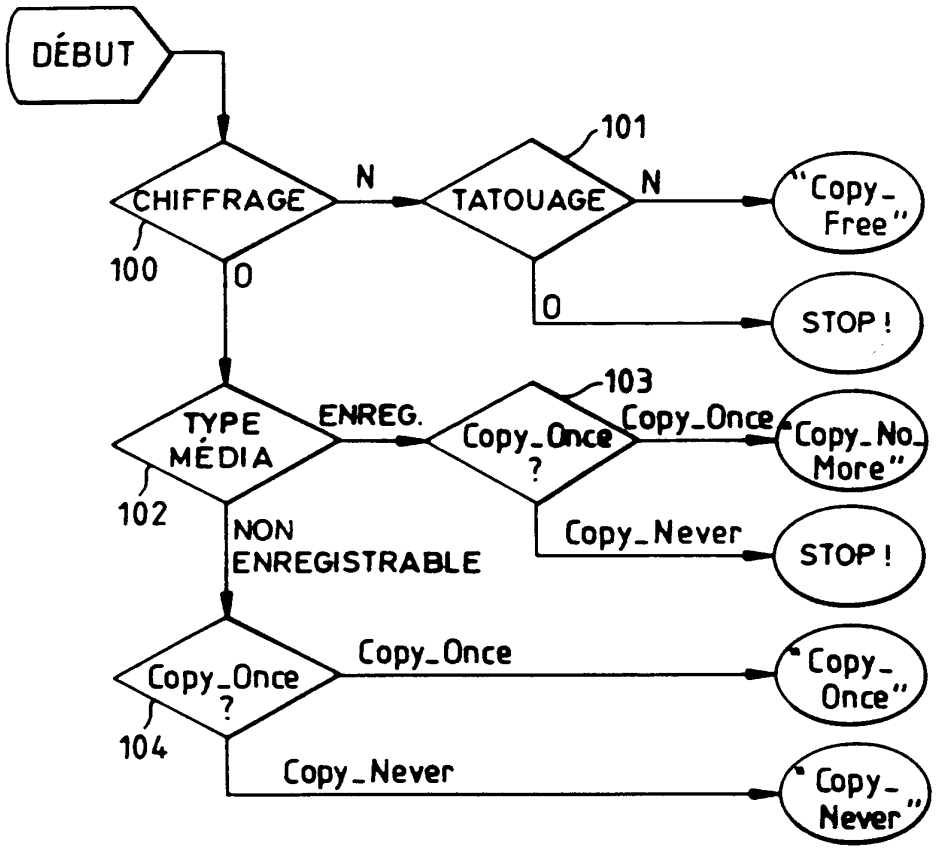

DÉBUT
CHIFFRAGE
100
N
0
101
TATOUAGE
N
0
"Copy_Free"
STOP !
TYPE MÉDIA
102
ENREG.
NON ENREGISTRABLE
103
Copy_Once ?
Copy_Once
"Copy_No_More"
Copy_Never
STOP !
Copy_Once ?
104
Copy_Once
"Copy_Once"
Copy_Never
"Copy_Never"

FIG.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/00572

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 382 296 A (PHILIPS NV) 16 August 1990 (1990-08-16) the whole document ---	1
A	EP 0 969 463 A (PIONEER ELECTRONIC CORP) 5 January 2000 (2000-01-05) the whole document ---	1-12,15, 17
A	HITACHI LTD ET AL: "5C Digital Transmission Content Protection White Paper - Revision 1.0" DTCP, 'Online! 14 July 1998 (1998-07-14), XP002134182 Retrieved from the Internet: <URL:http://www.dtcp.com/wp_spec.pdf> 'retrieved on 1999-10-15! cited in the application the whole document -----	1,12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 May 2001	29/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ogor, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR 01/00572

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0969463 A	05-01-2000	JP 2000023089 A	21-01-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Int[illegible]tionale No
PCT/FR 01/00572

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (systeme de classification suivi des symboles de classement)
CIB 7 G11B H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure ou ces documents relevent des domaines sur lesquels a porté la recherche

Base de donnees electronique consultee au cours de la recherche internationale (nom de la base de donnees, et si realisable, termes de recherche utilises)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie °	Identification des documents cites, avec, le cas echeant, 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 indiques en annexe

° Catégories speciales 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 speciale (telle qu'indiquee)

"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 priorite 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 theorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considerée comme nouvelle ou comme impliquant une activité inventive par rapport au document consideré isolement

"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 ete effectivement achevee	Date d'expedition du present rapport de recherche internationale
21 mai 2001	29/05/2001

Nom et adresse postale de l'administration chargee de la recherche internationale	Fonctionnaire autorisé
Office Europeen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Ogor, M

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux mer. s de familles de brevets

Demande Int' nationale No
PCT/FR 01/00572

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0382296 A	16-08-1990	NL 8900307 A	03-09-1990
		AU 620298 B	13-02-1992
		AU 4911190 A	16-08-1990
		CA 2009290 A	08-08-1990
		CN 1045317 A,B	12-09-1990
		DE 69011543 D	22-09-1994
		DE 69011543 T	02-03-1995
		JP 2250439 A	08-10-1990
		KR 155373 B	16-11-1998
		US 4980912 A	25-12-1990
		US 5144662 A	01-09-1992
EP 0969463 A	05-01-2000	JP 2000023089 A	21-01-2000

Formulaire PCT/ISA/210 (annexe familles de brevets) (juillet 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/77790 A1

(51) International Patent Classification[7]: G06F 1/00, G07F 17/16

(21) International Application Number: PCT/EP01/04088

(22) International Filing Date: 10 April 2001 (10.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00401007.0 11 April 2000 (11.04.2000) EP

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

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **DIEHL, Eric** [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). **FISCHER, Pierre** [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Agent: **BONNANS, Arnaud**; Thomson multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

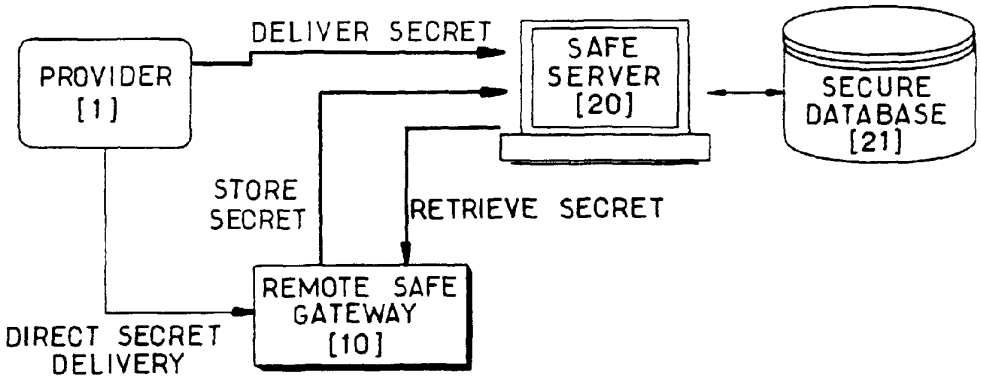
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT



(57) Abstract: A system for securely storing secret information comprises an apparatus (10; 1) containing the secret information, a device meant to use said secret information to decrypt a digital content and a remote server (20). The apparatus can send the secret information to the server (20) that has means for storing the secret information. A process with the following steps is proposed: initiating a remote communication between the apparatus (10; 1) and the remote server (20); sending the secret information from the apparatus (10; 1) to the server (20); storing the secret information on the server (20). A method for distribution of a digital content is also described.

WO 01/77790 A1

SYSTEM AND PROCESS FOR STORING SECURELY SECRET INFORMATION, APPARATUS AND SERVER TO BE USED IN SUCH A SYSTEM AND METHOD FOR DISTRIBUTION OF A DIGITAL CONTENT

Field of the invention

The invention relates generally to secure storage of secret information and more particularly to a system and a process for securely storing secret information and to an apparatus and a server to be used in said system. The invention also relates to a method for distribution of a digital content.

Background art

With the advent of digital TV, and copy protection, the access to content will be protected by rights. These rights may have many forms like entitlements, or dedicated decryption keys. The notion of rights might be extended to any secret information. All these type of data have in common that they need to be stored in a safe place.

Today none of the consumer devices has such tamper proof place. The price would be prohibitive. Only smart cards offer sufficient security. Unfortunately the size of memory of smart cards, and thus their storage capability, is limited. Furthermore a smart card can break down, or be lost. So today, once the user mislays his secret data, he will have no simple way to retrieve them. If these data represent user's rights acquired on digital content (for example the right to view a film or to listen to music) it may be prejudicial to the user if he loses these rights he has paid for.

Summary of the invention

The present invention is therefore directed to the problem of finding a way of safely and securely storing secret data to be used by a single device or by a device in a network. Another problem to be solved by the invention is to find a way of retrieving these secret data if the device or the network has lost them.

The invention relates to a system for securely storing secret information to be used by a device wherein said secret information is stored in a remote server. The device may be part of a home network and preferably the secret information is used by said device to access to a digital content.

Therefore, the remote server acts as a bank which maintains in a safe place digital secrets.

The invention proposes an apparatus containing secret information to be used by a device to decrypt a digital content and having means for sending

said secret information to a remote server in order to store said information in said remote server, said server being remote from said device.

The invention also proposes a system for securely storing secret information comprising an apparatus containing said secret information, a device meant to use said secret information to decrypt a digital content and a server remote from said apparatus and from said device, wherein said apparatus comprises means for sending said secret information to said server and wherein said server comprises means for storing said secret information.

The apparatus may be part of said device, or may belong to the same home network as said device. In such cases, the apparatus is thereafter called the remote safe gateway. The apparatus may alternatively belong to a local network generating said secret information (*i.e.* belong to the secret provider).

According to another aspect of the invention, a server for securely storing secret information to be used by a device remote from said server to decrypt a digital content has means for receiving said secret information through a remote communication

A process is proposed for securely storing secret information to be used by a device to decrypt a digital content : this process comprises the steps of :

- initiating a remote communication between an apparatus containing said secret information and a server remote from said device ;
- sending said secret information from said apparatus to said server ;
- storing said secret information on said server.

The invention also relates to a method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server remote from said device for storing said secret information on said server ;
- providing means for said device to retrieve said secret information from said server and to decrypt the encrypted digital content with said secret information.

Brief description of the drawings

Fig. 1 illustrates the general architecture of a system according to the invention.

Fig. 2 illustrates the architecture of a device used in the system of Fig. 1.

Fig. 3 illustrates a process for storing secret information according to a first embodiment of the invention.

Fig. 4 illustrates a process for retrieving a secret information stored according to the process illustrated in Fig. 3.

Fig. 5 illustrates a second embodiment of the invention.

Fig. 6 illustrates a process for storing a secret information in the second embodiment of the invention.

Description of the preferred embodiments

In Fig. 1, we have illustrated a first embodiment of a system according to the invention. In this embodiment, the user has a Set Top Box device 10 (STB) with a return channel such as a PSTN (for "Public Switched Telephone Network") modem or a cable modem.

We assume that all the information to store securely can be carried to this STB. For instance, we can envisage that a complete home network can benefit from the remote safe facility. In this case, preferably, a unique device of the network will be able to store and retrieve secret information according to the invention. This unique dedicated STB is used as an apparatus called the remote safe gateway. Obviously it could be another type of device, for example a computer.

Through its return channel, each remote safe gateway interacts with a remote server 20 called the remote safe server. The remote server has direct access to its own secure database 21. The secure database will store safely and securely the secret information.

In a preferred embodiment of the system, the secure database will be duplicated at least once in different locations. This will avoid loss of data due to natural or malicious crashes. Nevertheless, only one occurrence of the secure database will be considered in the following in order to simplify the presentation of the invention.

The user receives his secrets from a secret provider 1 which is consider here as having generated the secret information. It may be for example a content provider which provides, with an encrypted content, a secret to decrypt this content.

The secret provider 1 provides the information directly to the remote safe gateway 10. The user may receive information from many secret providers.

The characteristics of the system are as follows :

- A user must be identified uniquely. It must not be possible to impersonate him.

- A user must be able to transfer the secret digital information stored in his home system to the safe server 20. No information must leak from this transfer. For that purpose, the remote safe gateway 10 is used to make this transfer.

- The user must be able to retrieve one, part, or all the information stored in his remote safe. No information must leak from this transaction. For that purpose, the remote safe gateway 10 is also used for this transaction.

- There must be no constraint on the format of the stored information.

We will now describe how the system is working.

A first stage of the process consists in the registration of the user. Prior to use the remote safe, the user must sign on the remote safe server's operator. For that purpose, he provides a set of personal information. The definition of these data depends on the operator and is out of the scope of this invention. In return the operator returns a set of secret user identity information (SI_{user}) used in the next stages. Among this set of information is the unique identifier (ID_{user}) that thoroughly defines a given user.

The channel used for this communication can be different from the return channel of the remote safe gateway. In any case the transfer of the secret user identity information (SI_{user}) needs to be secured. There are several possible ways: mailing of a smart card, encrypted information sent through the return channel, ... In the last case, the decryption key is transferred through a secure separate channel such as phone or post mail.

A second stage of the process consists in the storage of secret information in the safe. This requires several steps.

In a first step, the remote safe gateway authenticates the remote safe server using known authentication methods. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the storage operation fails.

In a third step, they define a common session key $K_{session}$. This means a remote communication is initiated between the remote safe server and the remote safe gateway.

Then, in a fourth step, the remote safe server creates a unique identifier, $InfID_{user\_i}$ for the information i to be stored. InfIDuser_i is unique for each information stored by the user. Its choice is fully under the control of the

remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule *f*, so that $f(InfID_{user\_i}, ID_{user})=true$.

In a fifth step, the remote safe gateway sends the information i to store to the remote safe server. The information i is encrypted using the session key Ksession before being sent. In an optional step, the remote safe gateway encrypts the information i using a secret key of the remote safe gateway before using the session key. Thus, with this optional step, the remote safe server will not have access to the plain text information.

Then, in the last step, the remote safe server decrypts the received information using the session key Ksession and stores it into its secure database.

The transfer may be secured against transmission errors, or message tampering. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

A third stage of the process consists in the retrieval of the secret information from the remote safe server. This operation requires the following steps.

In a first step, the remote safe server authenticates the remote safe gateway. If the authentication fails, then the retrieval operation fails.

In a second step, they define a common session key Ksession.

Then, in a third step, the remote safe gateway provides the remote safe server with the unique identifier of the information to retrieve InfIDuser_i.

In a fourth step, the remote safe server checks the validity of InfIDuser_i. It checks if the corresponding information exists in the database and if this is the case, the remote safe server sends back the requested information to the requesting remote safe gateway in a fifth step. The information is encrypted using the session key Ksession before being sent to the remote safe gateway.

Then, in a last step, the remote safe gateway decrypts the received message using the session key Ksession.

Preferably, the transfer is secured against transmission errors, or message tampering. In that case, the remote safe gateway checks the integrity of the decrypted message before using it.

According to one preferred aspect of the invention, all the operations, except the registration phase, should be transparent to the user. In other words, the retrieval of the stored secrets should be automatic and should not request any interaction from the user.

Fig. 2 illustrates a possible architecture for the remote safe gateway. In this figure, only the elements which are necessary for the understanding of the invention have been represented.

The remote safe gateway has a Central Processing Unit (CPU) 100. It is assumed that the CPU has its own volatile memory and non-volatile memory where its program is stored. In addition, the remote safe gateway has a non-volatile memory space 101 called the identifiers' memory. The CPU 100 can read and write the content of this space.

The remote safe gateway has also a secure processor 102. This secure processor is a tamper proof device that has at least a dedicated CPU 110, a non volatile memory 111 (ROM – Read Only Memory) to store program and persistent data, a volatile memory 112 (RAM – Random Access Memory), and a dedicated non-volatile memory area 113, called the secret cache memory. The secure processor 102 is, in a preferred embodiment, a smart card.

The CPU 100 never handles actual secrets. It handles only information identifiers InfIDuser_i. It maintains a list of the secret information through a list of their corresponding InfIDuser_i. This list is stored in the identifiers' memory. This space needs not to be tamper-proofed. Therefore it is not costly. The size of the identifiers' memory should be chosen to be large enough to store the expected amount of information identifiers.

The secure processor's CPU 110 handles the actual secrets. It stores them in its secret cache memory 113. Unfortunately this space is limited in size due to cost. Therefore it will employ memory-caching techniques that optimize the use of the space. It will store the most recently used secrets and some of the most frequently used secrets.

If the remote safe gateway needs a secret information which is not readily available in the secret cache memory 113, then the secure processor's CPU 110 requests it to the remote safe server.

In one embodiment of the invention, the remote safe gateway is part of a digital home network where other devices are connected. Some of these devices can also handle secrets. In that case they may reproduce the architecture of Fig. 2. Nevertheless, only the remote safe gateway is able to communicate with the remote safe server. The other devices exchange, through secure communication, with the remote safe gateway their secrets to store or to retrieve.

We will now enter into more details of this first embodiment.

Registration of the user.

When signing on, the user receives the secret user identity information as follows:

- A unique identifier IDuser.
- A pair of public (PUB_{user}) and private (PRI_{user}) keys; the remote safe server encrypts with a public key cryptosystem that we will call CS1. RSA (Rivest-Shamir-Adleman public key cryptosystem) could be such a system.
- A public key certificate $CERT_{user}$ signed by the remote safe server using its private signature key PRI_{safe_sign}. The remote safe server signs with a public key cryptosystem that we will call CS2. RSA could be such a system. CS2 can be identical to CS1.
- The public key of the remote safe server PUB_{safe_enc} using cryptosystem CS1.

These data must be transferred safely to the user. It is especially important that his private key, $PRI_{user,}$ is kept secret. He may for example receive these data in a smart card sent to him via mail.

Storage of the secret information.

The format of the message to store is preferably defined as follows:

```
Info_To_Store = {
     InfIDuser_i
     Length_clear_text
     Clear_Text
     Length_secret
     for I=0 to Length_secret-1
          Secret_data[i]
     Checksum
}
```

where :

- InfIDuser_i is a unique identifier of the information stored by the user. This identifier is unique to the user and delivered by the safe server ;
- Clear_Text is an ASCII text that describes the stored secret information. Its content is user defined. It could be envisaged that the secret provider delivers a default value for this secret ;
- Length_clear_text defines the length in bytes of Clear_Text ;
- Secret_data is the secret to store in the remote safe ;
- Length_secret defines the length in bytes of Secret_data ;
- Checksum is the sum of all previous bytes of the packet.

The process for storing a secret information is illustrated in Fig. 3 and explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe server defines a new value for the information identifier, InfIDuser_i. It sends it to the remote safe gateway.

The remote safe gateway builds the message Info_To_Store with its secret data and InfIDuser_i. It encrypts it with the Triple DES algorithm using the common session key Ksession. It sends the encrypted message to the remote safe server that decrypts it using the common key Ksession.

The remote safe server checks the validity of Checksum. If the received message is valid, the remote safe server sends it to the secure database. If the operation was successful, the remote safe server returns an acknowledgement to the remote safe gateway, else it returns a non-acknowledgement.

Retrieving the secret information.

The process for retrieving a secret information stored in the remote safe server is illustrated by Fig. 4 and will be explained in the following.

The mutual authentication and key exchange uses the Authenticated DIFFIE HELLMAN Key Exchange Protocol. The protocol generates a common key K_{com}.

The common session key Ksession is the set of the 112 lower bits of the hash of K_{com} through the Secure Hash Algorithm (SHA-1).

The remote safe gateway sends the reference of the data to retrieve: InfIDuser_i.

On receipt of the information identifier InfIDuser_i, the remote safe server passes it to the secure database.

The secure database checks if the message exists, i.e., if there is an information, own by the user, that has the right identification. If it is the case, then it returns the requested information Info_To_Retrieve to the remote safe server. The remote safe server encrypts the received data using Triple DES with the session key Ksession and It sends the encrypted message to the remote safe gateway.

The remote safe gateway decrypts the received message using the session key Ksession. It checks the validity of Checksum and if it is valid, the remote safe gateway uses the retrieved secret information Info_To_Retrieve.

We will now describe a second embodiment of the invention which is illustrated in Fig. 5.

In this embodiment, the secret provider can provide the information directly to the remote safe gateway or by an indirect way using the remote safe server. The user may receive information from many secret providers.

The additional characteristics of the system are as follows:

- A third party, known as the secret provider, can deposit a secret to the remote safe server on behalf of a user. No information must leak from this transaction.

- It is not possible to impersonate a secret provider.

- Once a secret as been deposited by a secret provider, the secret provider has no possible access to it.

- A secret provider cannot retrieve any information stored on the account of a user.

- Only an authorized secret provider can deposit a secret onto the account of a user.

In this embodiment, the process for the secret provider has two stages :

The first stage consists in the registration of the secret provider. As for the remote safe gateway, the secret provider needs to sign on the remote safe server. He signs on as secret provider. In return, it receives a set of information known as secret provider identity information (SI_{prov}).

The second stage consists in the storage of a secret information on behalf of a user. This stage requires several steps.

In a first step, the secret provider, through an apparatus of a local network of its own, authenticates the remote safe server. If the authentication fails, then the storage operation fails.

In a second step, the remote safe server authenticates the secret provider. If the authentication fails, then the storage operation fails.

In a third step, the remote safe server and the secret provider's apparatus define a common session key $K_{session.}$

Then, in a fourth step, the secret provider provides the identity of the user that he is acting for: ID_{user}.

In a fifth step, the remote safe server creates a unique identifier, InfIDuser_i for the information to be stored. InfIDuser_i is unique for each information stored by the user identified by IDuser. Its choice is fully under the control of the remote safe server. It can be either a "random" number, or a number dedicated to the user, following a given rule.

In a sixth step, the secret provider sends the information to store to the remote safe server. The sent information is encrypted using the session key $K_{session}$.

In a last step, the remote safe server decrypts the received information using the session key $K_{session}$ and stores it into its secure database. The transfer may be secured against transmission errors, or message tampering using known techniques. In that case, the remote safe server checks the integrity of the decrypted message before its eventual storage.

Once the operation was successfully ended, then the secret provider sends the information identifier InfIDuser_i to the corresponding remote safe gateway. The secret provider does not keep any copy of it. Therefore, it is impossible for the secret provider to access any more to the secret information to retrieve it or to modify it.

Details of this second embodiment are explained bellow:

Registration of the secret provider

When signing on, the secret provider receives the following secret provider identity information:

- A unique identifier ID_{prov}.
- A pair of public (PUB_{prov}) and private (PRI_{prov}) keys; the remote safe server encrypts with the public key cryptosystem CS1.
- A public key certificate $CERT_{prov}$ signed by the remote safe server using its private signature key $PRI_{safe\_sign\_2}$; the safe server signs with the public key cryptosystem CS2.
- The public key of the remote safe server PUB_{safe_enc}.

These information must be transferred safely to the secret provider. It is especially important that his private key is kept secret

Storage of an information on behalf of a user.

This process, which is illustrated in Fig. 6, is similar to the process described previously in view of Fig. 3. The main differences are:

- Prior to exchange the secret information, the secret provider has to identify the user to whom is it depositing. The identification uses the user's unique identifier IDuser.

- Once the secret provider successfully stored the information, it sends the reference of the information to the user, that is to its remote safe gateway.

The system if the invention may be applied to a new distribution model. For example, a content provider wants to distribute in a controlled manner a content. This content can be any digital content such as video, MP3 files, software, etc. For that purpose it distributes the content encrypted with an encryption key $K_{enc\_cont\_i}$. To read this encrypted content, the user must have access to the decryption key $K_{dec\_cont\_i}$. The decryption key may be equal to the encryption if we use a symmetric cryptosystem. The user contacts the content provider and buys the right to access the content. Acting as a secret provider, the content provider deposits the decryption key in the user's remote safe. In return the user receives the information identifier of the decryption key.

Another possible application of the system of the invention is a small footprint backup of a jukebox. The jukebox will be a future new type of consumer device. It will probably be successful. Nevertheless with the jukebox, a major risk is introduced: loss of all the contents stored in the jukebox. Currently it is envisaged to use hard disks as storage units. In the field of software, it is well known that regular backup of the hard disk is a safe practice. But it is not reasonable to expect the same feature in a consumer device.

The system of the invention will provide a backup facility based on the remote safe as a new service. For each legally delivered content, the content provider will provide an additional information called a digital purchase proof. The digital purchase proof is the result of a one way cryptographic function using as input parameter a unique identifier of the owned content, and the user identifier ID_{user}. Instead of backing up all his contents, the user stores in his remote safe all his digital purchase proofs. If he loses one content, the user returns to the content provider the corresponding digital proof. The content provider checks if the digital proof is consistent with the claimed content and the identity of the user. If it is the case, then the content provider sends back to the user a copy of the content.

In conclusion, the invention offers the following advantages:

- the possibility to handle in a safe and secure manner a large quantity of secret data without requesting an in-house large tamper-proof space;

- a simple new model of distribution of digital content that could fit for IP streaming, or even prerecorded contents;

- a small size backup of large library of digital contents.

CLAIMS

1. Apparatus containing secret information to be used by a device to decrypt a digital content,

characterised by means for sending said secret information to a remote server (20) in order to store said information in said remote server (20), said server (20) being remote from said device.

2. Apparatus according to claim 1, being part of said device.

3. Apparatus according to claim 1, belonging to the same home network as said device.

4. Apparatus according to claim 1, belonging to a local network (1) generating said secret information.

5. System for securely storing secret information comprising :

- an apparatus (10 ; 1) containing said secret information ;
- a device meant to use said secret information to decrypt a digital content ;
- a server (20) remote from said apparatus and from said device,

wherein said apparatus (10 ; 1) comprises means for sending said secret information to said server (20) and wherein said server (20) comprises means for storing said secret information.

6. System according to claim 5, wherein said apparatus (10) is part of said device.

7. System according to claim 5, wherein said apparatus (10) and said device are connected to a common home network.

8. System according to claim 5, wherein said apparatus (1) belongs to a local network generating said secret information.

9. Server (20) for securely storing secret information to be used by a device to decrypt a digital content, said device being remote from said server (20),

characterised by means for receiving said secret information through a remote communication.

10. Process for securely storing secret information to be used by a device to decrypt a digital content comprising the steps of :

- initiating a remote communication between an apparatus (10 ; 1) containing said secret information and a server (20) remote from said device ;
- sending said secret information from said apparatus (10 ; 1) to said server (20) ;
- storing said secret information on said server (20).

11. Method for distribution of a digital content to be used by a device comprising the steps of :

- encrypting the digital content to thereby generate an encrypted digital content and secret information meant to later decrypt the encrypted digital content ;
- sending said secret information to a server (20) remote from said device for storing said secret information on said server (20) ;
- providing means (10) for said device to retrieve said secret information from said server (20) and to decrypt the encrypted digital content with said secret information.

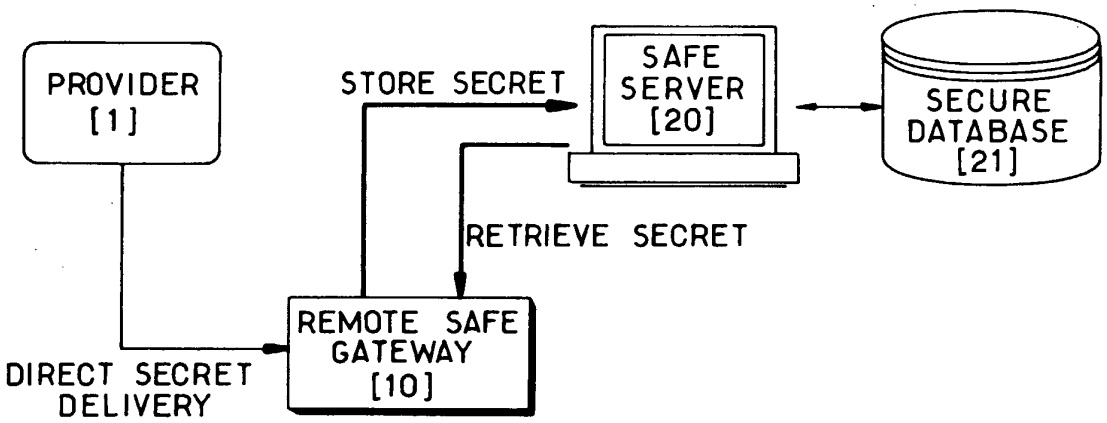

PROVIDER
[1]
STORE SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.1

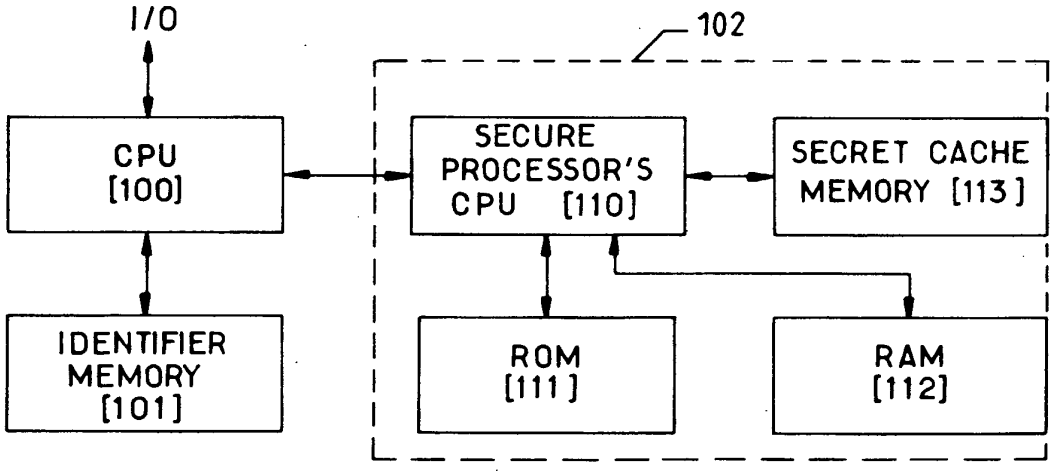

I/O
102
CPU
[100]
SECURE
PROCESSOR'S
CPU [110]
SECRET CACHE
MEMORY [113]
IDENTIFIER
MEMORY
[101]
ROM
[111]
RAM
[112]

FIG.2

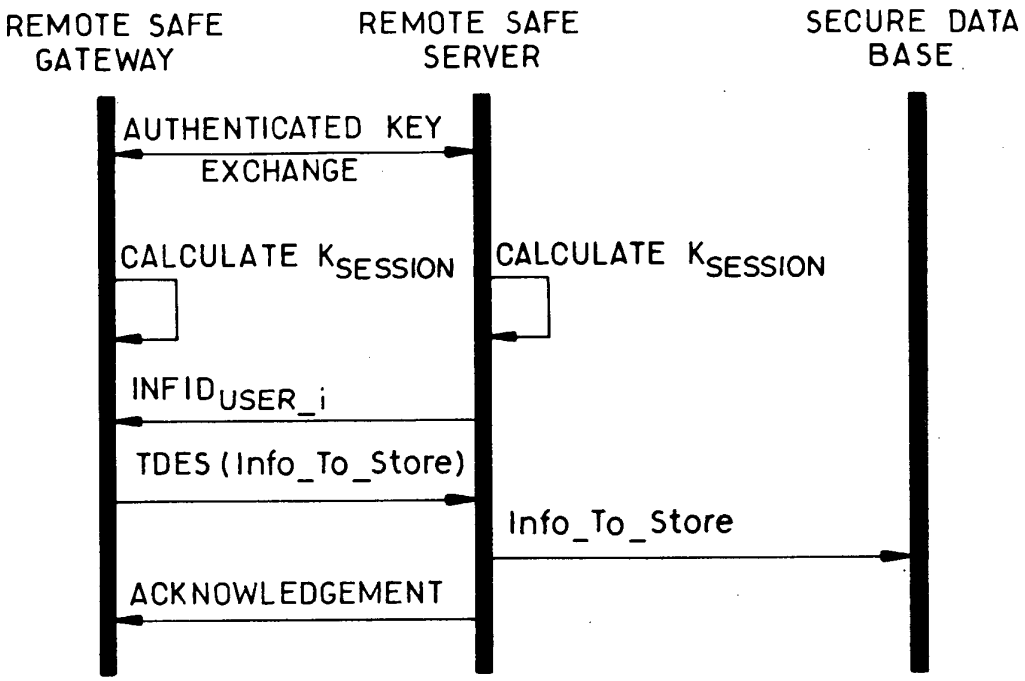

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
TDES (Info_To_Store)
Info_To_Store
ACKNOWLEDGEMENT

FIG.3

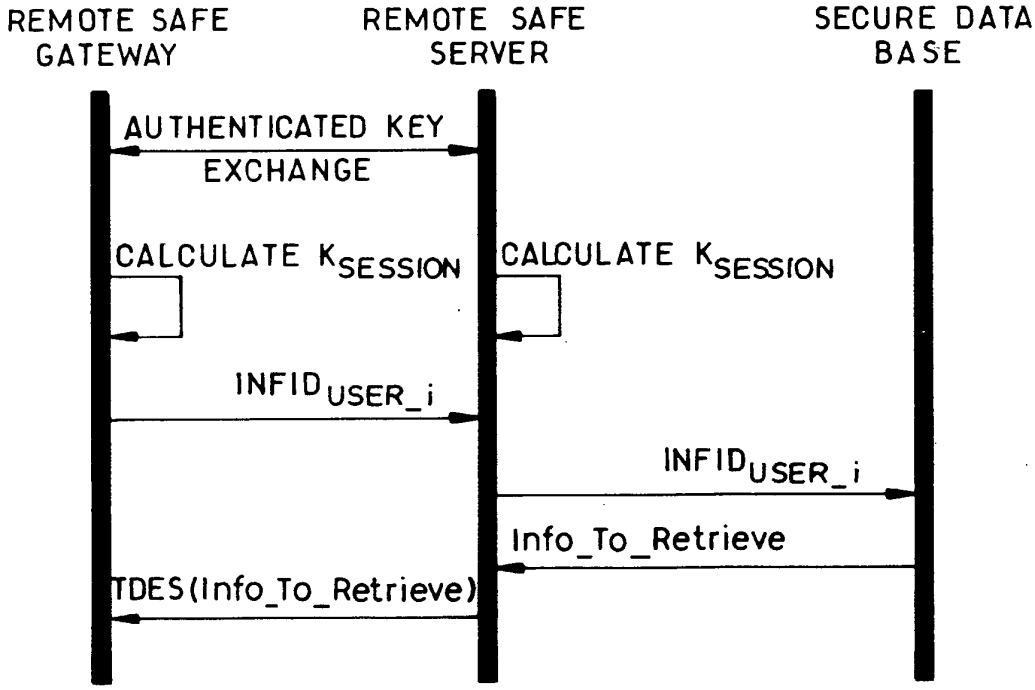

REMOTE SAFE GATEWAY
REMOTE SAFE SERVER
SECURE DATA BASE
AUTHENTICATED KEY EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
$INFID_{USER\_i}$
$INFID_{USER\_i}$
Info_To_Retrieve
TDES(Info_To_Retrieve)

FIG.4

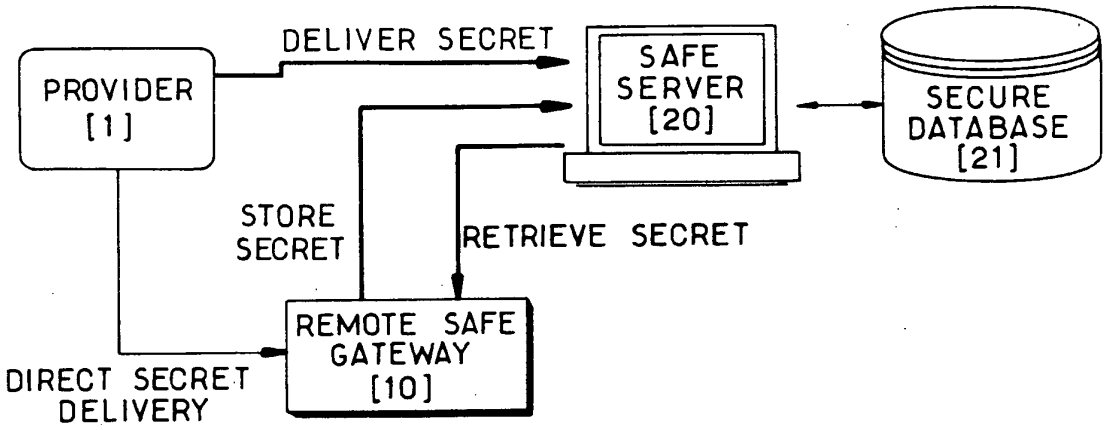

PROVIDER
[1]
DELIVER SECRET
SAFE
SERVER
[20]
SECURE
DATABASE
[21]
STORE
SECRET
RETRIEVE SECRET
REMOTE SAFE
GATEWAY
[10]
DIRECT SECRET
DELIVERY

FIG.5

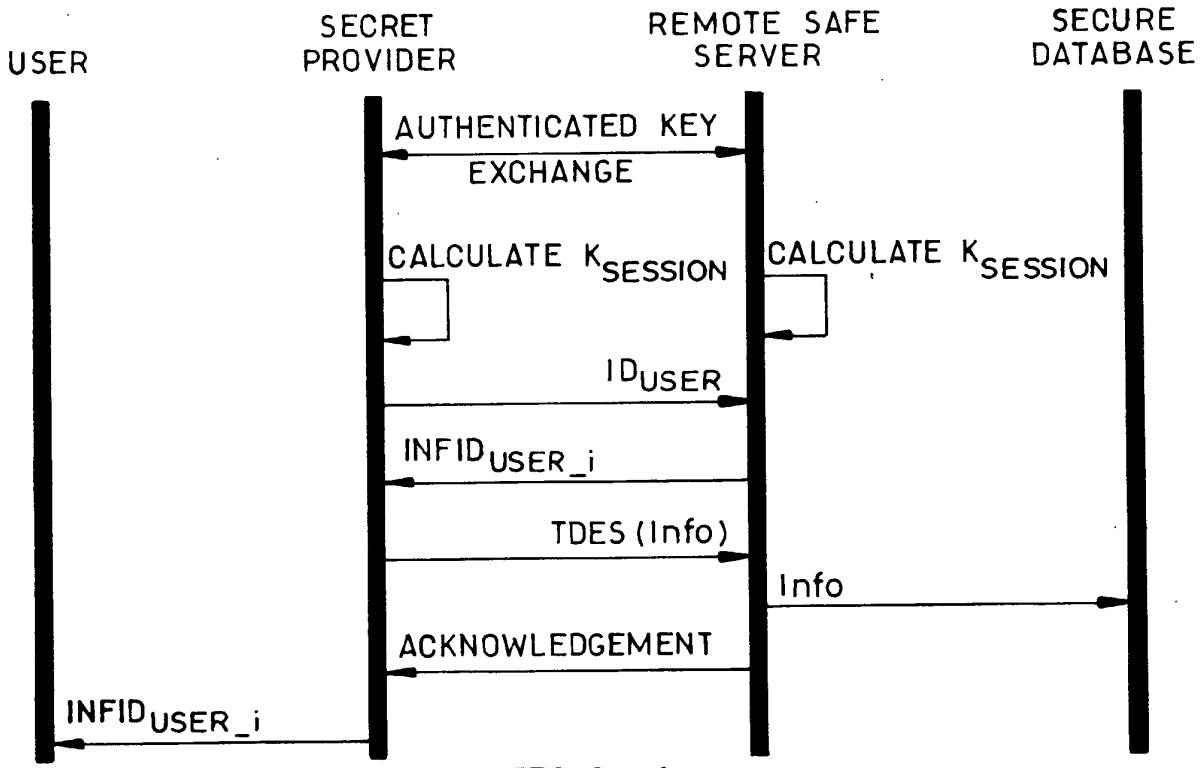

USER
SECRET
PROVIDER
REMOTE SAFE
SERVER
SECURE
DATABASE
AUTHENTICATED KEY
EXCHANGE
CALCULATE $K_{SESSION}$
CALCULATE $K_{SESSION}$
ID_{USER}
$INFID_{USER\_i}$
TDES (Info)
Info
ACKNOWLEDGEMENT
$INFID_{USER\_i}$

FIG.6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 01/04088

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F17/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 337 357 A (CHOU WAYNE W ET AL) 9 August 1994 (1994-08-09) figure 1 column 3, line 26 -column 4, line 37	1-11
X	EP 0 843 449 A (SUNHAWK CORP INC) 20 May 1998 (1998-05-20) column 5, line 8 -column 8, line 19 figures 2-5	1-11
X	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) page 10, line 7 -page 11, line 29 figures 1,5,6,9	1-11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 August 2001	14/08/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Papastefanou, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 01/04088

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5337357 A	09-08-1994	CA 2120816 A	18-12-1994
		EP 0636962 A	01-02-1995
EP 0843449 A	20-05-1998	US 5889860 A	30-03-1999
		CA 2220457 A	08-05-1998
		JP 10301904 A	13-11-1998
WO 9842098 A	24-09-1998	AU 6759198 A	12-10-1998
		EP 0968585 A	05-01-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 June 2005 (02.06.2005)

PCT

(10) International Publication Number
WO 2005/050450 A1

(51) International Patent Classification[7]: G06F 11/30

(21) International Application Number:
PCT/US2004/038124

(22) International Filing Date:
15 November 2004 (15.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/715,035 17 November 2003 (17.11.2003) US
10/, 17 May 2004 (17.05.2004) US

(71) Applicant *(for all designated States except US)*: **MARGENT DEVELOPMENT, LLC** [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

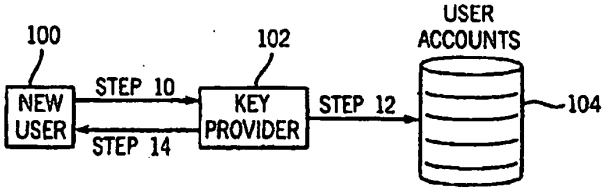
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DIGITAL CONTENT SECURITY SYSTEM



(57) Abstract: A Personal Digital Key Digital Content Security System (PDK-DCSS) is used to protect computers from unauthorized use and protect the digital content (110) stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are 1) a standard hard drive device (108), with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and 2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: 1) hard drive (108) access control for providing Drive-Level and Sector-Level protection and 2) operating system-level independent file protection for providing File-Level and Network-Level protection.

WO 2005/050450 A1

DIGITAL CONTENT SECURITY SYSTEM

REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. patent application Serial No. 10/xxx,xxx filed May 17, 2004, which is a continuation-in-part of U.S. patent application Serial No. 10/715,035 filed November 17, 2003, which is a continuation-in-part of U.S. patent application Serial No. 10/153,979 filed May 23, 2002, which is a continuation-in-part of U.S. patent application Serial No. 09/750,487 filed December 27, 2000 and Serial No. 10/016,857 filed December 14, 2001, all of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to digital content security systems and, more particularly, to a digital content security system and method that provides different levels of protection of a computer or other storage device and the digital content stored thereon.

BACKGROUND OF THE INVENTION

The market for downloading digital content online is rapidly climbing because distribution of such content is inexpensive, fast, and easy and the quality of the content itself is acceptable. The market, however, remains disorganized due to competing standards, competing companies, discontented artists and producers, and outright theft of digital content.

Digital rights management (DRM) companies seek to solve the foregoing problems by delivering the digital content from the real producers to the right customers and ensuring that everyone who should be paid in fact is paid. DRM seeks to get everyone paid by managing the multiple steps for distributing digital content (music, video, software) online: watermarking, encryption, transaction management, and rights management. Some DRM companies perform all these steps, while other DRM companies specialize in one or two steps of the process.

First, watermarking stamps each piece of digital content with a digital mark so it can be tracked wherever it goes. Digital watermarks are just like paper watermarks, except they cannot be seen or heard. Special software is required to read a digital watermark.

Second, encryption scrambles watermarked digital content and stores it inside a digital safe for shipment around the Internet. The safe protects the content during shipping by allowing only those with the right software key to the safe to decrypt and use the content.

Third, transaction management handles actual payments for the digital content using credit card techniques found elsewhere in e-commerce. An order is placed, a credit card number is taken, account status is checked, and the exchange is authorized.

Finally, rights management manages the information about the digital content itself: what it is, who gets it, how it is delivered, how many times it may be used, how long the rights last, who gets paid, how much they get paid, and how. This information travels with the digital content in something called a digital permit. The permits rests on top of the digital content as it travels the Internet and allows legal users to enjoy the digital content for as long as the rights last.

The primary objective of DRM companies is to deploy technologies that protect digital content as it is distributed online. Some of these proposed technologies and DRM in general are discussed in the article "Digital Rights Management May Solve the Napster 'Problem'," *Technology Investor*, October 2000, pp. 24-27. Although such technologies should reduce the amount of digital theft, they generally favor the content provider at the expense of the consumer or favor the consumer at the expense of the content provider. That is, the rights of either the content provider or the consumer are compromised. For example, some technologies severely limit the consumer's ability to make extra copies of digital content even when the digital content is solely for personal use. Other technologies facilitate the making of copies of digital content which can be used by different

consumers without the content provider being compensated by each consumer. The present inventor has discovered an improved DRM system and method that effectively balances and protects the rights of both the consumer and the content provider. In addition, the present inventor has discovered an associated digital content security system for protecting computers and other storage devices from unauthorized use and protecting the digital content stored on computers and other storage devices from being wrongfully accessed, copied, and/or distributed.

SUMMARY OF THE INVENTION

In accordance with the foregoing, there is disclosed a Personal Digital Key Digital Content Security System (PDK-DCSS) for protecting computers from unauthorized use and protecting the digital content stored on computers from being wrongfully accessed, copied, and/or distributed. The basic components of the PDK-DCSS are (1) a standard hard drive device, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) optionally integrated into the hard drive's controller, and (2) a PDK-Key associated with the PDK-RDC. The PDK-Key and RDC technology is utilized to provide two categories of protection: (1) hard drive access control for providing Drive-Level and Sector-Level protection and (2) operating system-level independent file protection for providing File-Level and Network-Level protection. A number of alternative embodiments are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a flow chart of a method of managing digital rights in accordance with the present invention;

FIGS. 2, 3, and 4 are block diagrams of portions of a DRM system for implementing the method in FIG. 1;

FIG. 5 is a conceptual model of core options for acquiring digital content that can be encoded to produce key-secured content and core options for playing back the key-secured content;

FIG. 6 is a block diagram for implementing a core acquisition option of downloaded content;

FIG. 7 is a block diagram for implementing a core acquisition option of store-bought content;

FIG. 8 is a block diagram for implementing a core acquisition option of broadcast content;

FIGS. 9a and 9b are block diagrams for implementing a core playback option of stand-alone devices;

FIG. 10 is a block diagram for implementing a core playback option of networked devices;

FIG. 11 is a block diagram of a standard computer hard drive incorporating an integrated PDK-RDC (receiver/decoder circuit) for the purpose of enabling multiple methods of securing digital content;

FIG. 12 is a block diagram for implementing Drive-Level protection and Sector-Level protection in connection with the computer hard drive;

FIG. 13 is a flow chart of the logic executed by the PDK-RDC for implementing Drive-Level protection and Sector-Level protection;

FIG. 14 is a block diagram for implementing File-Level protection in connection with the computer hard drive; and

FIG. 15 is a block diagram for implementing Network-Level protection by expanding File-Level protection to a network environment.

While the invention is susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and will be described in detail herein. However, it should be understood that the invention is not intended to be limited to the particular forms disclosed. Rather, the

invention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DESCRIPTION OF SPECIFIC EMBODIMENTS

Turning now to the drawings and referring initially to FIG. 1, there is depicted a method of managing digital rights in accordance with the present invention. First, a new user requests a physical electronic key or data unit from a key provider (step 10). The key provider may offer a web site on the Internet, a toll free telephone number, and/or retail outlet where the key may be acquired. In addition, the key provider may allow a key to be requested in writing, preferably using a form designed by the key provider. In one model the user may acquire as many keys as desired, while in another model each user is only entitled to a single key.

Second, in response to the user's request for a physical key, the key provider establishes a new secure account for that new user in a secure user account database (step 12). The new account may include the following data fields: account number, password, software encryption key, user label, number of users (linked to account), address, telephone number, e-mail address, and custom fields. The custom fields may, for example, include demographic information such as the user's age, gender, marital status, income level, interests, hobbies, etc. The physical key may include the following data fields: user label, account number, software decryption key, and a custom storage area. The user label and the account number serve as a first activation code (or key code) for the acquired physical key. All data fields on the physical key, except for the user label, are preferably encrypted. To allow the user to view his or her account in the future, the user is preferably assigned a login name and the above-noted password.

Third, the key provider ships the physical electronic key to the new user via a package courier such as the U.S. Postal Service, United Parcel Service, or Federal Express (step 14). In one pricing model the physical key is sent to the user at no charge, while in another pricing model the physical key must be purchased by the

user. If the physical key must be purchased by the user, either the user must provide credit/debit card information to the key provider in step 10 to pay with a credit/debit card, or the key provider includes an invoice with the shipped key in step 14.

FIG. 2 is a block diagram of a system for implementing steps 10, 12, and 14 of the method of managing digital rights. The system includes the new user 100, the key provider's web site 102, and the user account database 104.

Referring back to FIG. 1, fourth, the user transmits his or her activation code in the physical key to a digital content provider, who may have a cooperative relationship with the key provider, and requests to purchase digital content (music, video, or software) from that content provider (step 16). The content provider may offer a web site on the Internet containing a listing of digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.

Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As

used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.

Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital content either by providing credit/debit card information to the content provider in step 16 or by paying off of an invoice included with delivered digital content. If the digital content is delivered online, the user is preferably required to provide the credit/debit card information and have such information approved as a prerequisite to delivery of the digital content. If the user possesses more than one physical electronic key and would like the acquired digital content to function with each of the user's keys, all of the

activation codes are applied to the digital content. The content provider charges the user based on the number of keys with which the user would like the digital content to function. For example, the user may be charged the same amount for each activation code, or may be charged a larger amount for one activation code and lesser amounts (e.g., surcharges) for additional activation codes.

FIG. 3 is a block diagram of a system for implementing steps 16, 18, 20, 22, and 24 of the method of managing digital rights. The system includes the new user 100, the content provider 106, the key provider's web site 102, the digital content database 108, and the acquired digital content 110.

Returning to FIG. 1, ninth, the user enters the encrypted digital content into a playing device of a type suitable for playing the digital content (step 26). The device may, for example, be an MP3 player, a personal computer, a DVD player, a CD player, a cellular phone, or other portable device. In one embodiment, the device contains a wireless transceiver adapted to receive a radio frequency signal transmitted by a corresponding wireless transceiver in the user's physical electronic key. The wireless transceiver in the device is optionally tracked and "secured" for audit purposes by permanently including a unique identifier assigned by the device manufacturer in the transceiver.

Tenth, with the user's physical electronic key within a short range (e.g., few meters) of the playing device, the playing device reads (1) the first activation code carried in a secure radio frequency signal transmitted by the transceiver in the physical key to the transceiver in the device and (2) the second activation code marked on the encrypted digital content (step 28). The device contains decryption software or hardware for decrypting the encrypted digital content to the extent necessary to read any encrypted portion of the second activation code.

Eleventh, the playing device compares the first activation code and the second activation code and determines whether the first activation code is associated with the second activation code (step 30). Steps 29 and 30 may be performed, for example, when the user presses a "play" button on the playing device or when the

user first enters the encrypted digital content into the playing device. If the first activation code is associated with the second activation code, the device decrypts and plays the digital content. If the first activation code is not associated with the second activation code, the device does not play the digital content. If the second activation code is simply the same as the first activation code, then the foregoing comparison determines whether there is a match between the first activation code and the second activation code. In a preferred embodiment, the device continues to play the digital content only while the physical key is sufficiently close to the device to communicate the first activation code to the device and allow the device to compare the first activation code to the second activation code at least partially encrypted with the digital content even while the digital content is being played. If the physical key is moved out of range, the device is no longer enabled to decrypt and play the digital content. In an alternative embodiment, once the device is initially enabled to decrypt and play the digital content, the device remains enabled until either the "play" function is stopped, a play track/song ends, or the digital content is removed from the device, even if the physical key is moved out of range such that the key can no longer communicate the first activation code to the device.

FIG. 4 is a block diagram of a system for implementing steps 26, 28, and 30 of the method of managing digital rights. The system includes the encrypted digital content 110, the key-enabled playing devices 112, and the user's physical electronic key 114.

As stated above, the user's physical electronic key and the key-enabled playing device contain respective wireless transceivers to communicate the activation code in the key to the device. In a preferred embodiment, the transceivers are small, inexpensive *Bluetooth* radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are plugged into electronic devices, which can then communicate over short distances and through obstacles by means of radio waves. *Bluetooth* is a term used to describe the

protocol of a short range (e.g., about 10 meters) frequency-hopping radio link between devices containing the radio chips. These devices are then termed "*Bluetooth*-enabled." The secure radio link replaces a cable that would otherwise be used to connect the devices. Further details concerning *Bluetooth* wireless technology may be obtained from www.bluetooth.com.

Wireless technologies other than *Bluetooth* may be used to communicate the activation code from the user's physical electronic key to the playing device. One example of an alternative wireless technology is known by a trade term "Wi-Fi," which is short for wireless fidelity and is another name for IEEE 802.11 b. Products certified as Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA) are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

In other alternative embodiments, the communication between the user's physical electronic key and the playing device is not wireless. Rather, in one alternative embodiment, the user's physical electronic key communicates the activation code to the playing device via a transmission line such as a serial cable that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

The above-described DRM method and system for implementing the method are advantageous in that they afford the key holder with tremendous versatility in copying and using encrypted digital content for personal use. At the same time, the rights of the content provider are protected because only the key holder with a key-enabled device can use the encrypted digital content. The key holder can copy the encrypted digital content as many times as desired, but can only play the encrypted digital content on a key-enabled device that is enabled with the physical electronic key coded to decrypt the encrypted digital content. Thus, the digital content, even

when copied, remains personal to the key holder. Individuals other than the key holder cannot use the encrypted digital content, even if they copy it, because both the original and copies of the encrypted digital content are still encrypted and the individuals do not hold the physical electronic key coded to decrypt the digital content.

A core element of the present invention is the concept of a portable, physical electronic key that is personal to a particular user. The physical key represents a DRM solution that fully addresses the needs of both consumers and publishers of digital content. The physical key is permanently associated with a user's digital content library. At the time of content acquisition, the physical key becomes permanently associated with the newly acquired content. The user is now "linked" to that acquired content. A user (e.g., individual or family) may own as many physical keys as desired, but every piece of encrypted digital content purchased is tied to one specific key. The user may duplicate or transfer the acquired content to any media or device for playback as many times as desired, as long as the associated physical key is present. Thus, the present invention guarantees that the acquired content is played only by the user who has legitimately paid for it. The present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to FIG. 5, the present invention fully supports the use of "key-secured" digital content 125 with all core content acquisition options and all core playback options. The key-secured digital content 125 is encoded with a second activation code associated with a first activation code stored on the user's physical electronic key. The core acquisition options include downloaded content 120, store-bought content 122, and broadcast content 124. The core playback options include stand-alone devices 126 and networked devices 128. Each of these options are described in further detail below.

Referring to FIG. 6 generally, as already noted in FIGS. 1 through 4, a primary application of the present invention is its use in the downloading of digital

content from the Internet. A consumer shops a content distributor's website and selects a piece of content they wish to purchase (music, movies, software, E-books, etc.). The consumer then provides the web site with standard on-line purchase information including the selection's title and method of payment, as well as their physical electronic key information. Transparent to the consumer, the distributor's web site links to the key provider's web site and transmits the physical key information for validation. The key provider's web site then provides the distributor's web site with the information required to prepare the acquired content for secure shipment to the consumer (or notification that the physical key was invalid). The key provider's web site records the transaction for later billing. Finally, the distributor's web site retrieves a copy of the digital content from its library, permanently links it to the consumer's physical key (by using the key's information to encrypt it), and transmits the secured content to the consumer. The consumer is now free to duplicate the content as often as desired, and to play the content on any key-enabled playback device.

Referring to the specifics of FIG. 6, the process of implementing the core acquisition option of downloaded digital content 120 (see FIG. 5) proceeds as follows. At step 130, a receiver/decoder circuit 140 retrieves an account number from a consumer's physical key (transponder) 142 over a secure RF link. At step 131, the consumer enters such data as a password, purchase selection, and method of payment via the consumer's personal computer 144. The data is transmitted to a content distributor's web site 146 from the consumer's personal computer 144. At step 132, the content distributor's web site 146 transmits the account number and password to a key provider's web site 148. At step 133, the key provider's web site 148 authenticates all data against its database 150 and, if authentic, returns such information as the account number, user label, number of users, and software encryption key to the distributor's web site 146. If the data is not valid, the key provider's web site 148 sends a message to the distributor's web site 146 indicating the same. A counter, used for the key provider's billing purposes, is incremented. At

step 134, the distributor's web site 146 pulls the purchased content file from its database 152, encrypts it with the software encryption key it received in step 133, and builds a final key-secured content file that is then transmitted to the consumer's personal computer 144. Charges are assessed based on the number of users, etc. and billed to the consumer according to the method of payment. At step 135, invoices 154 are generated and sent to content distributors by the key provider's web site 148 on a regular cycle.

Optionally, to enable content providers to offer sample content (e.g., limiting playback to the device on which the content was originally downloaded, for a specified period of time) a special "enhanced" version of a receiver/decoder circuit 140 can be produced. These enhanced receiver/decoder circuits (primarily for PC's) would each include a unique identification number and additional functionality enabling them to "talk" to a key provider's web site 148 to acquire secured timing information. Sample content files may include the following information (in their encrypted header section):

- identification number of enhanced receiver/decoder circuit used for downloading and transmitted by the receiver/decoder circuit to the key provider's web site at the time of content purchase;
- hour stamp (i.e., the hour in which the content was downloaded; and
- life hours (i.e., number of hours content remains valid, such as perpetual, one hour, 24 hours, 48 hours, etc.).

The above information is used by an "enhanced" receiver/decoder circuit during playback to determine whether a content file has "expired" or is attempting to play on an unauthorized device (i.e., any device except the device on which the content was originally downloaded). This capability allows content distributor web sites to distribute limited-use samples with associated tiered-pricing models.

Referring to FIG. 7 generally, the present invention can be extended to store-bought content. To fully integrate store-bought content into the present invention, traditional store-bought content is modified in two ways. First, the content is

distributed in a copy protected format (e.g., using any valid copy protection technology). Second, the content contains a unique content serial code. The content serial code may be contained either directly in the digital content or as a physical label. Each content serial code is designated by a content distributor during manufacturing and stored in the key provider's database. This database is later used to validate that each content serial code is unique and used only a prescribed number of times. To a consumer, a content serial code on their newly purchased store-bought content represents a download of a key-secured version of that content for free or a prescribed price. This key-secured copy provides the consumer with exactly the same advantages and freedoms as any other key-secured content. From the consumer's standpoint, the download process occurs exactly as any other standard key-secured content download with the exception of how the payment is handled. The "payment" is the content serial code. By providing all of the advantages of the present invention to consumers of legacy-capable store-bought content (by way of "content serial code downloads"), the scheme provides the industry with the first complete DRM solution.

Referring to the specifics of FIG. 7, the process of implementing the core acquisition option of store-bought digital content 122 (see FIG. 5) proceeds as follows. At step 160, a receiver/decoder circuit 170 retrieves an account number from a consumer's physical key (transponder) 172 over a secure RF link, and the consumer's personal computer 174 reads a content serial code from the store-bought content 122. The store-bought content 122 contains the content serial code that uniquely identifies the content. The format of the content serial code may, for example, be PPPP.FFF.0123456789 where PPPP is a provider identification, FFF is a facility identification, and the numbers represent a sequence number. The store-bought content 122 incorporates a copy protection scheme such as Macrovision™, key2audio™, or SafeAudio™. Disc "copy flags" (specified in SDMI standards) may also be set to further inhibit duplication efforts.

At step 161, the consumer enters such data as a password and purchase selection via the consumer's personal computer 174. The previously-read content serial code specifies that the method of payment is to a "content serial code-credit" (i.e., there is typically no charge for this download because the content serial code confirms that the download in process is of content that the consumer has already legitimately purchased). The data is transmitted to a content distributor's web site 176 from the consumer's personal computer 174. At step 162, the distributor's web site 176 transmits the content serial code, account number, and password to a key provider's web site 178. At step 163, the key provider's web site 178 authenticates all data against its databases 180 and 182 and, if authentic, returns such information as the account number, user label, number of users, software encryption key, and paid-flag (indicating the content serial code has been validated) to the distributor's web site 176. The key provider's web site 178 now sets the paid-flag to disable any further downloads and records the account number field in the content serial code database 182 for auditing purposes. If the data is not valid, the key provider's web site 178 sends a message to the distributor's web site 176 indicating the same. A counter, used for the key provider's billing purposes, is incremented. Each entry in the content serial code database 182 may include the following data fields: CDC #, paid-flag, and account number. At step 164, the distributor's web site 176 pulls the content file from its database 184, encrypts it with the software encryption key it received in step 163, and builds a final key-secured file that is then transmitted to the consumer's personal computer 174. No charge is typically assessed because a valid content serial code serves as "payment" for the download. At step 165, invoices 186 are generated and sent to content distributors by the key provider's web site 178 on a regular cycle.

Referring to FIG. 8 generally, the present invention can be extended to broadcast content. To fully integrate broadcast content into the present invention, traditional broadcast content is only minimally modified. The modification is that the broadcast content is transmitted in a copy protected format (such as the DVD

standard known as Content Scramble System (CSS)). The remainder of the process is described below. A key-enabled recording device, incorporating a unique identifier, receives copy-protected broadcast content. If only playback of the broadcast content is desired, basic decoding (e.g., CSS) is performed and the broadcast content is sent on for playback. If the consumer wishes to record the broadcast content, however, the recording device performs additional steps prior to sending the broadcast content on for playback. The recording device connects to the key provider's web site to validate the recording device's internal identifier and the consumer's physical key. If both are valid, the recording device translates the broadcast content into a key-secured format by encoding it with the consumer's activation code, and then stores the key-secured content file, with its identifier permanently embedded within, for later use. The end result is key-secured broadcast content that provides the owner of the associated physical key all the freedoms and advantages of the present invention. Although the content was originally broadcast, it cannot be illegally copied or distributed. The present invention can be applied to pay per view offerings, as well as standard broadcast material.

Referring to the specifics of FIG. 8, the process of implementing the core acquisition option of broadcast digital content 124 (see FIG. 5) proceeds as follows. At step 180, a receiver/translator/recording device 190 receives digitally broadcast content in copy-protected format from a source 192 such as satellite, cable, Internet, or over-air. The broadcast content may be copy-protected using a copy-protection technology such as an enhanced CSS scheme. If a consumer wishes to only play (not record) the broadcast content, basic decoding (e.g., CSS decoding) is performed and the broadcast content is passed through to presentation device 194 for playback. The remaining steps below may be skipped.

If, however, the consumer wishes to record the broadcast content, the following additional steps are performed prior to sending the broadcast content on for playback. At step 181, the receiver/translator/recording device 190 retrieves an

account number from the consumer's physical key (transponder) 196 over a secure RF link. At step 182, the receiver/translator/recording device 190 transmits the account number and its recorder serial code to a key provider's web site 198. Each device 190 contains a recorder serial code that uniquely identifies the device. The format of the recorder serial code may, for example, be MMMM.FFF.0123456789 where MMMM is a manufacturer identification, FFF is a facility identification, and the numbers represent a sequence number. At step 183, the key provider's web site 198 authenticates the data against its databases 200 and 202 and returns an "approved" or "rejected" response. A counter, used for the key provider's billing purposes, is incremented. At step 184, if a "rejected" response is received, the broadcast content cannot be recorded. If an "approved" response is received, the receiver/translator/recording device 190 translates the decoded content into a key-secured format by encoding it with the consumer's activation code, and records the key-secured content, with the recorder serial code permanently embedded within, to a storage device (that can optionally be an external device). The broadcast content can now be copied to and played back on any key-enabled playback device. At step 185, invoices 199 are generated and sent to content distributors by the key provider's web site 198 on a regular cycle. While providing excellent additional security and protections, steps 182 and 183 are not mandatory for the present invention to function with broadcast content. It may be desirable, for cost purposes, to produce receiver/translator/recording devices 190 not capable of communicating with the key provider's web site 198.

Referring to FIGS. 9a and 9b generally, having acquired key-secured digital content and produced copies for playback on various devices such as a portable CD player, personal computer, home theater, etc., a consumer is now ready to use the digital content. Playback of key-secured content occurs as follows. A key-enabled playback device transparently reads information from a consumer's physical key and from the content file the consumer has requested to play. The pieces of information are then compared to validate that the physical key "matches" the content to be

played. If the elements match, the device begins playback of the content. If the elements do not match, the device will not play the content and, depending upon the device's capabilities, may display an "invalid content" message. From a consumer's point of view, when used with legitimately-acquired content, the process is entirely transparent, effortless, and non-intrusive. The consumer is free to use their content on any key-enabled playback device, with the only restriction being that the content can be played only when the associated physical key is present. As noted above, the present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to the specifics of FIGS. 9a and 9b, the process of implementing the core playback option of stand-alone devices 126 (see FIG. 5) proceeds as follows. At step 210, a consumer requests playback of a key-secured content file via a playback device 220. The playback device 220 may, for example, be the consumer's personal computer (FIG. 9a) or a stereo amplifier (FIG. 9b) with integrated compact disc reader/player. At step 211, a receiver/decoder circuit 222 searches for a physical key (transponder) 224. The circuit 222 may be a separate component from the playback device 220 as in FIG. 9a or integrated into the playback device 220 as in FIG. 9b. If the physical key is not found, the playback device 220 displays an "invalid content" message. If the physical key is found, the receiver/decoder circuit 222 retrieves all available information from the physical key 224 over a secure RF link. At step 212, the user labels in the physical key 224 and the key-secured content file are compared. If the user labels do not match, the playback device 220 displays an "invalid" message. If the user labels do match, the receiver/decoder circuit 222 retrieves the software decryption key from the physical key 224 over the secure RF link between the physical key 224 and the playback device 220 and begins decryption of the encrypted portion of key-secured file. When the account number is decrypted, it is matched against the account number retrieved from the physical key 224. If the account numbers do not match, the playback device 220 displays an "invalid content" message. If the account numbers

do match, the software decryption key is used by the playback device 220 to decrypt remaining data in the key-secured file for playback. The user label and the account number in the physical key serve as a first activation code, and the user label and the account number in the content file serve as a second activation code. These activation codes must match (or have some other predetermined association) in order for playback to proceed.

Referring to FIG. 10 generally, while stand-alone playback devices (e.g., CD players, PCs, DVD players, etc.) are currently the norm, the convergence of these devices and the Internet will lead to an environment where centralized digital distribution systems proliferate. Security of content in these environments is critical yet challenging to accomplish without imposing great restrictions. The present invention can provide security to a centralized digital distribution system and, in addition, offers many important enhancements that greatly increase the convenience and usability of such a system. These enhancements include integration of the physical key into a portable handheld computer which then doubles as the system remote. In addition to controlling all networked components, the remote is used for tasks such as purchasing content from the Internet, and tracking the movement of a user throughout a facility to provide automatic "content following" (i.e., where content playback follows the user from room to room). The centralized nature of the digital content distribution system means that only one storage device is required to maintain a consumer's entire digital content library (e.g., music, movies, software, E-books, etc.) and to feed that content to any networked playback device.

Referring to the specifics of FIG. 10, there is shown a centralized digital content distribution system for implementing the core playback option of networked devices 128 (see FIG. 5). The system is used in an establishment such as a residence or entertainment facility. The system includes a digital content server 310, a distribution hub 312, a plurality of remote clients 314, and a portable remote control 316. The digital content server 310 stores digital content acquired from a source 318 such as satellite, cable, Internet, or over-air. In addition, the digital

content server 310 may store digital content uploaded from a standard component 324. The plurality of remote clients 314 are located in different rooms of the establishment and linked to the digital content server 310 via the distribution hub 312 or switch. The remote clients 314 are linked to the distribution hub 312 by a backbone transmission network 315. The backbone transmission network 315 may be wireless or wired with fiber optic cables, coaxial cables, or twisted pair cables, may employ a networking protocol such as Ethernet, Wi-Fi, Arcnet, or ATM (Asynchronous Transfer Mode), and may employ a communications protocol such as TCP/IP. Each remote client 314 includes a network interface card (NIC) for interfacing with the backbone transmission network 315.

The remote control 316 is adapted to communicate with each of the remote clients 314 and select the digital content stored in the digital content server 310. The remote control 316 is essentially a personal digital assistant (i.e., hand-held computer) including a display and added remote control circuitry. The display may, for example, be a liquid crystal display (LCD). The added remote control circuitry includes "system remote" circuitry and "universal remote" circuitry.

The "system remote" circuitry in the remote control 316 is for establishing a first wireless transmission link 320 with each of the remote clients 314. The first wireless transmission link 320 may be a secure radio link (RF) as shown or an infrared link (IR). Upon establishing the first wireless transmission link 320 with one of the remote clients 314, the remote control 316 serves as a system remote capable of (1) displaying, scanning, and selecting the digital content available on the digital content server 310 and downloading the selected digital content from the digital content server 310 to the linked remote client 314 and (2) controlling the digital content server 310 to acquire or download digital content from a source 318 such as satellite, cable, Internet, or over-air. As used herein, the term "download" and similar variations thereof (e.g., downloaded, downloading, etc.) is intended to cover the transfer of content from one device to a receiving device whether the content is stored on the receiving device or merely "streamed" to the receiving

device for immediate playback. The remote control 316 preferably includes a display for displaying the digital content. The display may, for example, be a liquid crystal display (LCD). As a user holding the remote control 316 moves from room to room of the establishment, the remote control 316 successively establishes wireless transmission links 320 with the remote clients 314 in the respective rooms. In this way, the digital content available on the digital content server 310 follows the user's movement from room to room.

In a preferred embodiment, the first wireless transmission link 320 is a secure radio link established by matching transceivers in the remote control 316 and each remote client 314. The matching transceivers are preferably small, inexpensive Bluetooth™ radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are integrated into the respective remote control 316 and each remote client 314, which can then communicate over short distances and through obstacles by means of radio waves. Wireless technologies other than Bluetooth, such as Wi-Fi, may be used to communicate remote control signals between the remote control 316 and each remote client 314.

The "universal remote" circuitry in the remote control 316 is for establishing a second wireless transmission link 322 with standard components 324 connected to the remote clients 314. The second wireless transmission link 322 is preferably an infrared link (IR) as shown. Upon establishing the second wireless transmission link 322 with one of the standard components 324, the remote control 316 series as a universal remote capable of operating the standard component 324. The standard component 324 may, for example, be an audio receiver (stereo amplifier), an audiovisual receiver, a video monitor (television), etc. The standard components 324 may be physically separate from, but linked to, the respective remote clients 314 or may be physically integrated into the respective remote clients 314 like integrated device 324c.

The digital content stored on the digital content server 310 may be formatted as a compact disc (CD), digital video disc (DVD), MP3, electronic book, software, etc. When the remote control 316 is linked to one of the remote clients 314, a user may scan and select digital content to be downloaded from the digital content server 310 to the remote client 314 and converted by the remote client 314 to a standard playable format (e.g., analog format) that can be played on the associated standard component 324. The selected digital content is downloaded from the digital content server 310 to the remote client 314 as raw digital data packets. The remote client 314, in turn, converts the downloaded digital content to a standard component output(s) compatible with a standard component 324 connected to the remote client 314, and the standard component 324 plays the digital content. Ports may, for example, include S-Video, RCA jacks, serial ports, Universal Serial Bus, Ethernet, Wi-Fi, Firewire™, Bluetooth, RF, or other similar outputs. The standard component 324 incorporates, or is linked to, audio speakers for broadcasting any audio signals received from the remote client 314 and a video monitor for displaying any video signals received from the remote client 314.

All content is stored on the digital content server 310 digitally, and is key-secured if obtained via the download or broadcast acquisition options of FIGS. 6 and 8. If the digital content is key-secured, the plurality of remote clients 314 include decryption circuitry (i.e., receiver/decoder circuit) for unlocking the digital content. The digital content selected for download from the digital content server 310 to a remote client 314 preferably remains encrypted until converted to a standard component output(s) in the remote client 314. The remote client 314 acts as a converter between key-secured digital content from the digital content server 310 and the standard component output(s). To decrypt the selected digital content, the remote control 316 contains a physical key initially acquired from a key provider in accordance with the present invention. The digital content is initially acquired from a content provider 326 that marks the digital content with an activation code associated with the physical key. The decryption circuitry in the

remote client 314 receives an activation code from the remote control 316 via the wireless transmission link 320 and is enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content. If the activation code in the remote control 316 is not associated with the activation code in the digital content, the remote client 314 will not unlock and convert the digital content.

In an alternative embodiment, the remote clients 314 are eliminated and the standard components 324 are linked directly to standard component outputs of the distribution hub 312 by the backbone transmission network 315. In this case, the distribution hub 312 serves as a switch, and the digital content server 310 contains the decryption circuitry for unlocking the digital content. As the digital content is decrypted, it is converted to a playable format and fed to the distribution switch 312 for delivery to the appropriate standard component 324. The decryption circuitry in the digital content server 310 receives the activation code from the remote control 316 and is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content.

Instead of decrypting the digital content so that it can be played, the digital content may be downloaded (or "passed through") in its encrypted format to a storage device such as a media burner 324a or computer hard disk 324b for storage thereon. When a user ultimately desires to play the stored digital content on a media player, the media player must contain the decryption circuitry for unlocking the digital content. After unlocking the digital content, the media player converts the unlocked digital content to a playable format and plays the digital content. The decryption circuitry in the media player receives the activation code from the remote control 316 or physical key with the same activation code. The media player is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 or physical key is associated with the activation code in the digital content.

In addition to downloading selected digital content from the digital content server 310 to the remote clients 314, data (e.g., MP3, CD, DVD, software, etc.) from the standard components 324 can be uploaded to the digital content server 310 and stored digitally thereon. This allows for storage of legacy content on the digital content server 310.

Referring to FIG. 11 generally, a digital content security system and method protects computers from unauthorized use and protects the digital content stored on computers from being wrongfully accessed, copying, and/or distributed. The basic components of the Personal Digital Key Digital Content Security System (PDK-DCSS) are (1) a standard hard drive device 330, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) 332 integrated into the controller 334, and (2) a PDK-Key 336 associated with the PDK-RDC as described above. The standard computer hard drive 330 incorporates the integrated PDK-RDC 332 for the purpose of enabling multiple methods of securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the PDK-RDC 332 as being integrated with the hard drive's controller 334, all OS-level protections described below can be implemented using externally-based PDK-RDCs.

A PDK hard drive 330 is similar to any standard, currently available hard drive with the exception of the PDK-RDC 332 (which is integrated into the drive's controller circuit 334). A PDK-RDC 332 is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content. Additionally, this circuit 332 is able to secure the hard drive 330 itself. This is implemented by the circuit 332 enabling or disabling the hard drive's controller 334 depending on whether an associated PDK-Key 336 (one which is uniquely and permanently associated with the PDK hard drive 330) is present. Each PDK hard drive 330 would typically be delivered with its own PDK-Key 336.

Secure RF communications between a PDK-Key 336 and its associated hard drive 330 occurs in the same manner as described above. It should be noted that

software drivers can optionally be designed to allow for dynamic key assignment (assigning of keys after purchase to enable key swapping, or assigning of individual keys to multiple devices).

The PDK-Key and RDC technology is utilized to provide two categories of protection:

1) Hard drive access control - where an entire drive 330 is either completely accessible (unlocked) or inaccessible (locked), and/or individual data sectors or clusters of data sectors are optionally encrypted/decrypted, depending on whether the specific PDK-Key 336 associated (and shipped) with the drive 330 is within range. This category of protection can be accomplished transparently to the operating system (OS) responsible for managing the drive.

2) OS-level independent file protection - where the drive's RDC 332 functions independently of the drive 330 to protect individual files (typically copyrighted material) from wrongful copying. In this role, the RDC 332 works with any PDK-Key 336 (not just the one delivered with the drive 330) and any PDK-compliant file (they do not have to be stored on or associated with the hard drive 330). This category of protection requires an OS-level software driver be run under the OS responsible for managing the drive.

By utilizing these two categories of protection in various ways, four unique levels of content protection are enabled. Two of the levels (Drive-Level and Sector-Level) do not require external software support, while the remaining two (File-Level and Network-Level) require software drivers, as well as a stand-alone application for Network-Level implementations. Each of the four levels is defined below.

Referring to FIGS. 12 and 13 for Drive-Level protection, when implemented, a PDK hard drive 330 will only function when the associated PDK-Key 336 is within range. The drive's controller 334 is disabled whenever the PDK-Key 336 is not present. The contents of files stored on the drive 330 are not encrypted. The Drive-Level protection feature is designed to protect the hard drive's owner by locking access to the PDK hard drive 330 whenever the associated PDK-

Key 336 is not present (i.e. when the owner momentarily steps away from the computer, if the computer is stolen, etc.).

Referring to FIGS. 12 and 13 for Sector-Level protection, when enabled, every sector (or cluster of sectors) read or written is encrypted/decrypted by the RDC 332 using the drive's associated PDK-Key 336. Because the encryption is performed at Sector-Level as opposed to File-Level, the encoding can be accomplished without requiring any changes, involvement, or acknowledgement of the OS responsible for managing the drive. The Sector-Level protection feature is designed to further protect the hard drive's owner (beyond Drive-Level protection) by encrypting the contents of the files stored on the drive, without requiring any software modifications (OS, application, etc.). The security advantage is that if the drive access is in some way defeated, the contents of files on the drive are still protected. It should be noted that if users retrieve files from drive and purposely transfer them anywhere else (via email, memory sticks, etc.), the data will no longer be protected. Drive-Level protection and Sector-Level protection may be used individually or in combination. Also, as noted above, it should be understood that Sector-Level protection may be applied to individual data sectors or clusters of data sectors.

FIG. 13 illustrates the logic executed by the RDC 332 for implementing Drive-Level protection and Sector-Level protection. The logic ensures OS-level commands (save entire file, read entire file, etc.) are given adequate time to complete. This enables implementation of logic without requiring OS changes, involvement, or acknowledgement.

Referring to FIG. 14 for File-Level protection, implemented as an OS-level software driver utilizing the PDK-RDC 332 integrated in the PDK hard drive 330, File-Level protection provides standard PDK digital rights management services and functionality as described above. As needed, the driver instructs the RDC 332 to acquire PDK-Key information, validate the key-to-file match, and use the key's information to perform actual encryption/decryption of the file (as a whole, not at

the sector level). In the illustrated example, the file ABC 338 (which can reside on any storage device, in memory, etc.) is compared to any PDK-Key 336 within range of the PDK-RDC 332. If a match is found, the PDK-RDC 332 will decrypt the file 338 for use with whatever playback mechanism placed the request. Any PDK-Key 336 can be utilized, not just the key 336 associated with the PDK hard drive 330. When employed for File-Level protection (and Network-Level protection as described below), the PDK-RDC 332 functions independently of the hard drive 330 in which it resides. While PDK-compliant files it encrypts or decrypts may reside on the resident hard drive 330 and may be associated with the drive's PDK-Key 336, they do not have to be. The PDK-RDC 332 can work with other PDK-Keys and files residing on other mediums. When used in this manner, the PDK-RDC 332 can be thought of as just coincidently residing within the hard drive 330. For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

The primary use of File-Level protection is to secure and protect private or copyrighted material from wrongful copying and distribution. Because copies of any PDK-compliant files can only be accessed when the associated PDK-Key is present, File-Level protection enables copies (intended for use by the holder of the associated key) to be produced effortlessly and securely. In addition to the distribution of copyrighted content such as music and movies as described above, software developers can distribute their software products via the Internet with the same ease and security. Software distributed in this manner would allow the legal recipient to make unlimited copies (for backup purposes, use on a home computer, etc.), yet the copies would only function when the associated key is present, preventing unauthorized copies from being wrongfully distributed and used.

The File-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key

holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and pasted into another application (e.g., an email program) thereby defeating the protection. Therefore the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations.

Referring to FIG. 15 for Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application / database called a PDK Document Controller (DC) 340 ruing on a server 342. A DC 340 enables the creation of Groups 342 that list which PDK-Keys 344 are allowed access to files in specific directories. All files stored in directories controlled by the DC 340 are automatically encrypted using the DC administrator's PDK-Key and thereby become PDK-compliant files. This process places all files stored in the DC 340 in a uniformly encrypted format.

Each user request for a file residing in a directory listed in a DC Group 342 results in the following steps. An RDC located in the requester's workstation 346 acquires information from the user's PDK-Key 344 and relays that information to the DC 340. The DC then enables appropriate access as defined by the DC's Group database information. Specifically, the DC 340 performing a lookup of the requester's PDK-Key 344 in the appropriate Group's tables. If the DC 340 determines that the PDK-Key 344 is listed in a Group 342 that also lists the directory containing the file the user wishes to access, the DC 340 knows that a valid PDK-Key 344 was used in the file request and grants access. The requested file is first decrypted with the administrator's PDK-Key, re-encrypted with the requester's PDK-Key 344, and then downloaded to the user's workstation 346. The foregoing process mirrors the process employed when using PDK to download digital media files from the Internet.

The Network-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and paste into another application (e.g., an email program) thereby defeating the protection. Therefore, the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations. The system is well suited for establishing centralized databases of secure documents intended for distribution to entrusted recipients such as personnel in a law firm or medical facility.

While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention. A number of enhancements and variations can be implemented/utilized that effectively broaden the PDK technology's scope and utility. These enhancements and alternative embodiments are summarized below.

Integration of RDCs into Alternative Storage Devices. This embodiment involves integrating RDCs into alternative storage mechanisms beyond those of basic hard drives. These storage mechanisms include pure RAM/ROM-based storage commonly included/used in devices such as PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, and DVR players, as well as portable storage devices such as Memory Sticks, Secure Digital memory cards, or any similar such product, in which case the RDC is either directly installed on the device, or integrated into the device in which the memory cards/sticks are inserted.

When an RDC is utilized in this manner, File-Level and Network-Level security function in the same manner as that described above for PDK hard drives. Drive-Level and Sector-Level security function in the same *logical* manner as that described for hard drives, but the *physical* implementation varies so as to control the bus structure that provides the communications path between the storage mechanisms and their hosting devices. As with PDK hard drives, access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either "ready" or "busy," effectively enabling/disabling the device itself. To save batteries, RDCs used in this manner may only check for the presence of the associated PDK-Key on some periodic basis (versus every read or write sequence). And similar to PDK hard drives, Sector-Level security can be optionally utilized to encrypt/decrypt data traveling over the bus prior to writes and after reads to provide PDK's standard Sector-Level data encoding functionality.

As when utilized in PDK hard drives, the PDK's security features provide the same convenient, non-intrusive, wireless security mechanism for the above-defined devices. This security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely "disabled" to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled.

Dynamic PDK-Key Management. Utilizing dynamic PDK-Key management, PDK-Keys can be assigned to an RDC (whether integrated into a PDK hard drive or some other hosting device, or implemented independently) by a user (versus requiring such assignment at time of production). This capability is accomplished by including the required logic within the RDC's internal firmware (versus using an externally-based software driver to supply such capability).

Using this capability, a user can optionally assign any PDK-Key to act as the RDC's *master* key (the first key assigned to the device). Then by involving this

master key (to prove the original "owner's" validation of the process), the user can assign (or remove) *additional* keys to the PDK-device. The general benefits of this feature include:

- The ability for the individual possessing the *master* key to create backup keys (to be stored and later retrieved in the event the *master* is ever lost), and to allow other users (those possessing *additional* keys) to also access their PDK device(s).
- The option to ship PDK-RDCs (in any configuration, host devices, etc.) without any PDK-Keys. And to allow such devices containing these RDCs (such as PDK hard drives) to optionally function with all or part of the PDK-technology never enabled or utilized. For instance, a user may elect to not enable Drive-Level and Sector-Level security features, but still utilize the functionalities of File-Level and Network-Level security.
- Giving users the option to purchase and associate a PDK-Key at a later time, or importantly, assign a PDK-Key they *already* utilize for another PDK-based device. This allows a user to utilize a single PDK-Key to provide access to all their PDK-based devices.

This built-in (firmware-based) PDK-Key configuration/management capability greatly enhances PDK's overall flexibility and ease of setup/use.

Independent RDC configuration. While integrating an RDC into a hard drive offers numerous benefits, RDCs may exist separately from hard drive mechanisms. In this configuration (as previously defined) an RDC's physical circuitry may exist in the form of a PC Card, a PC expansion board that plugs into a standard PC expansion slot, a USB-based plug-in board, or any other similar design able to interface with a hosting device. Used in this manner, RDCs provide all previously defined functionalities with the exception of basic hard drive access-control.

Buffer Flush & Notification Software Driver. This enhancement involves using a simple software device driver to recognize when a PDK-Key is out of range

(by "watching" for signals from the RDC), and when such a condition is detected to flush (empty) the host system's "read" buffer (effectively clearing any data the system may have been cached in internal memory in order to speed data access), and display a simple message indicating the PDK-Key is in/out of range. This optional mechanism can be utilized with any RDC configuration and on any PDK-protected device.

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

CLAIMS:

1. A method of securing a storage device having a hard drive, comprising:

detecting a portable, physical key with a receiver/decoder circuit associated with the hard drive;

validating the detected portable, physical key with the receiver/decoder circuit; and

permitting access to the storage device or a portion thereof with the receiver/decoder circuit if the detected key is validated.

2. The method of claim 1, wherein the receiver/decoder circuit resides in the storage device.

3. The method of claim 1, wherein the detecting step includes detecting the key over a secure wireless link.

4. The method of claim 1, wherein the validating step includes determining whether or not the detected key is associated with the storage device.

5. The method of claim 4, wherein the receiver/decoder circuit enables the storage device if the detected key is validated and disables the storage device if the detected key is not validated in order to provide device-level protection.

6. The method of claim 5, wherein the storage device stores digital content that is not encrypted with the key.

7. The method of claim 4, wherein digital content read from or written to the storage device is decrypted or encrypted by the receiver/decoder circuit using the key associated with the storage device in order to provide sector-level protection.

8. The method of claim 4, wherein the key associated with the storage device is initially delivered with the storage device.

9. The method of claim 1, wherein the storage device is selected from a group consisting of PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, DVR players, memory sticks, and memory cards.

10. The method of claim 4, wherein the key associated with the storage device is assigned thereto by a user.

11. A system for securing a storage device of a computer, comprising:
a portable, physical key; and
a receiver/decoder circuit for detecting and validating the key and for permitting access to the storage device or a portion thereof if the detected key is valid, the receiver/decoder circuit being associated with the storage device;

12. The system of claim 11, wherein the receiver/decoder circuit resides in the computer.

13. The system of claim 11, wherein the receiver/decoder circuit detects the key over a secure wireless line.

14. The system of claim 11, wherein the receiver/decoder circuit validates the key by determining whether or not the detected key is associated with the storage device.

15. The system of claim 14, wherein the receiver/decoder circuit enables the storage device if the detected key is validated and disables the storage device if the detected key is not validated in order to provide device level protection.

16. The system of claim 15, wherein digital content stored on the computer is not encrypted with the key.

17. The system of claim 14, wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the storage device using the key associated with the storage device in order to provide sector-level protection.

18. The system of claim 14, wherein the key associated with the storage device is initially delivered with the storage device.

19. The system of claim 11, wherein the storage device is selected from a group consisting of PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, DVR players, memory sticks, and memory cards.

20. The system of claim 14, wherein the key associated with the storage device is assigned thereto by a user.

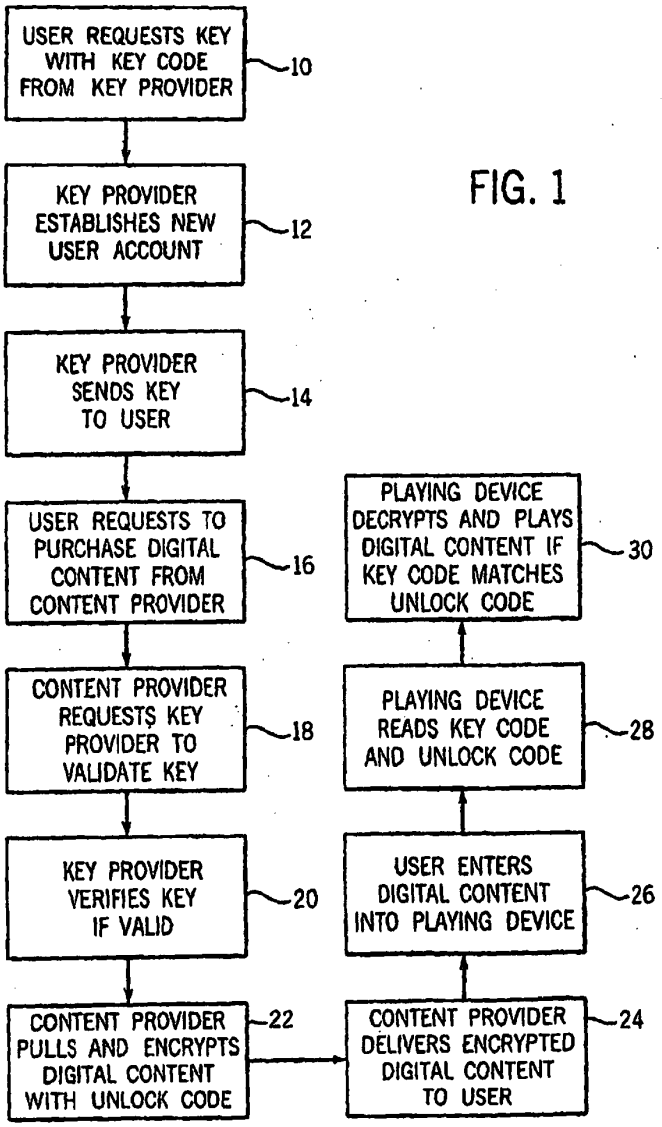

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT PROVIDER PULLS AND ENCRYPTS DIGITAL CONTENT WITH UNLOCK CODE
22
CONTENT PROVIDER DELIVERS ENCRYPTED DIGITAL CONTENT TO USER
24
USER ENTERS DIGITAL CONTENT INTO PLAYING DEVICE
26
PLAYING DEVICE READS KEY CODE AND UNLOCK CODE
28
PLAYING DEVICE DECRYPTS AND PLAYS DIGITAL CONTENT IF KEY CODE MATCHES UNLOCK CODE
30

FIG. 1

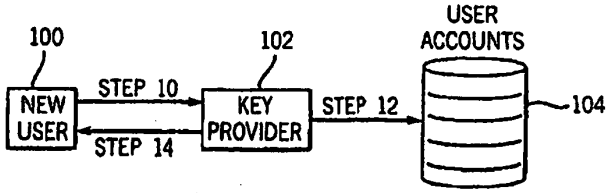


FIG. 2

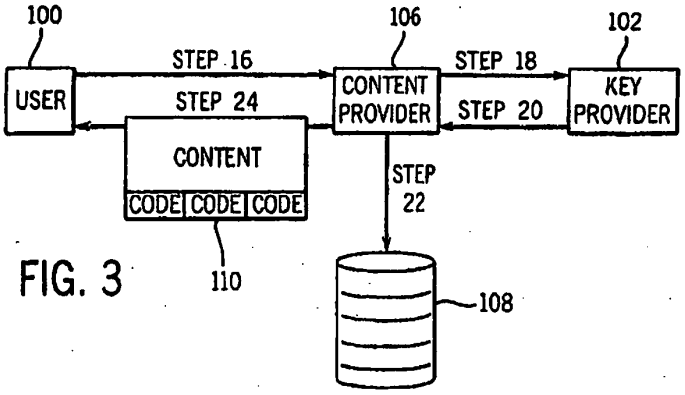


FIG. 3

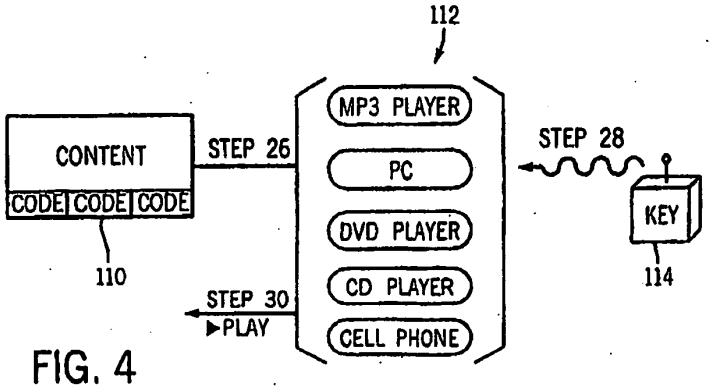


FIG. 4

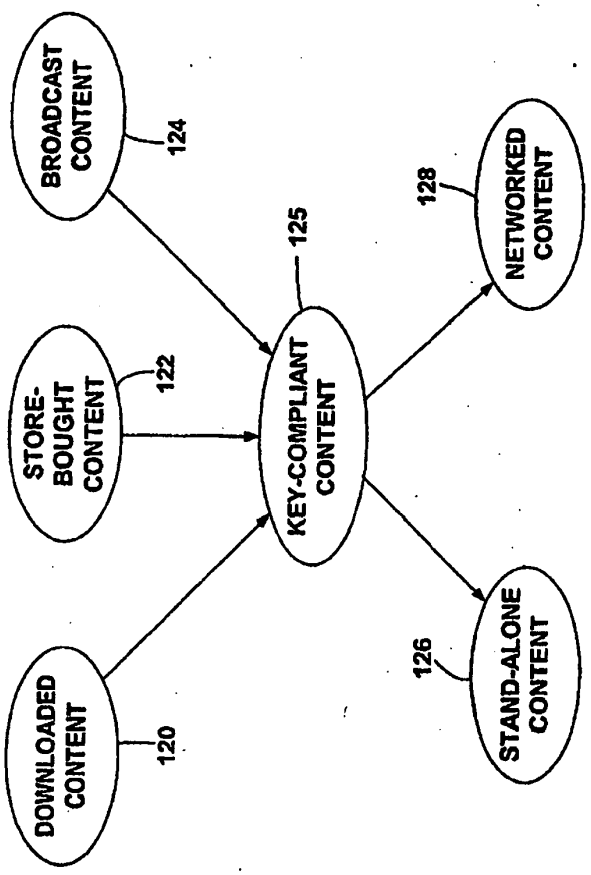

BROADCAST CONTENT
124
STORE-BOUGHT CONTENT
122
DOWNLOADED CONTENT
120
KEY-COMPLIANT CONTENT
125
NETWORKED CONTENT
128
STAND-ALONE CONTENT
126

FIG. 5

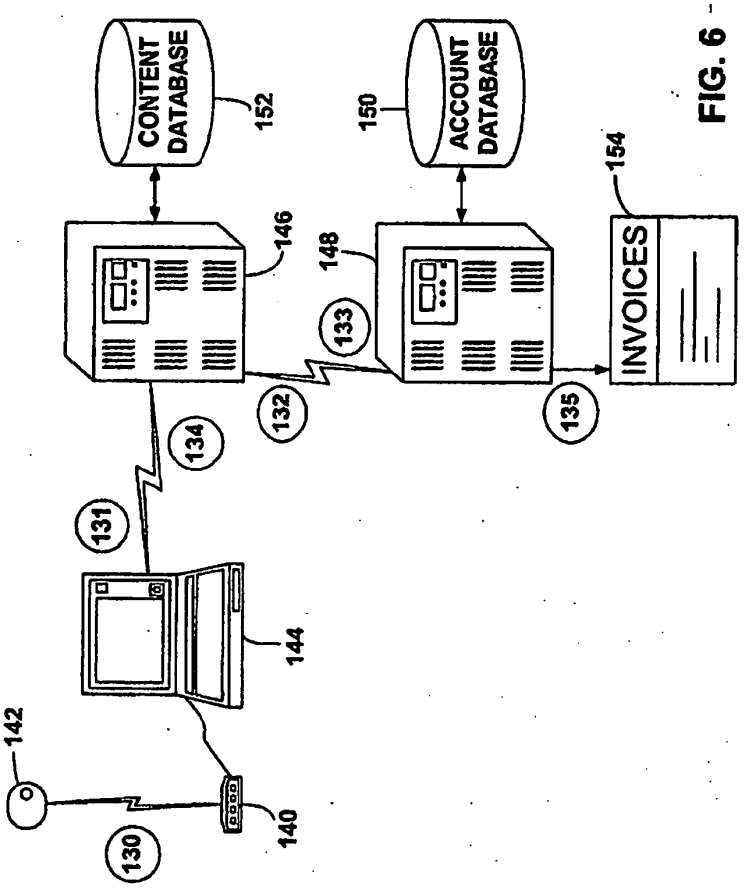

CONTENT DATABASE
152
ACCOUNT DATABASE
150
154
INVOICES
146
148
133
132
134
135
131
144
142
140
130

FIG. 6

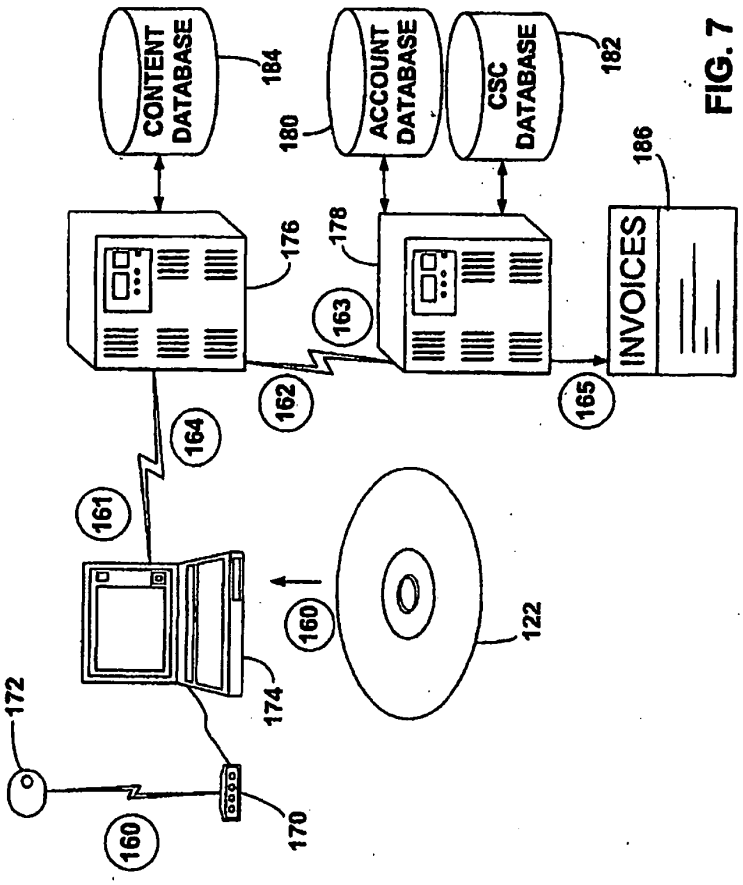

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
186
INVOICES
176
178
163
162
165
164
161
160
122
174
172
170
160

FIG. 7

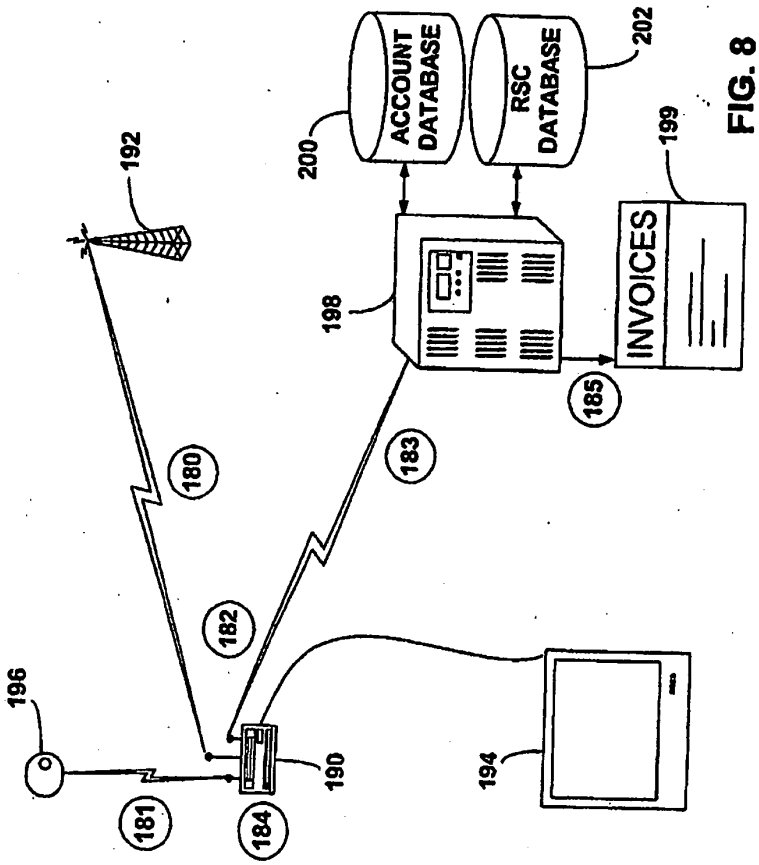

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
192
198
185
180
183
182
196
190
194
181
184

FIG. 8

FIG. 9a

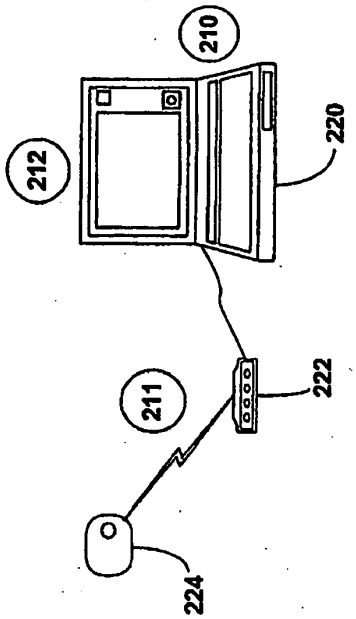
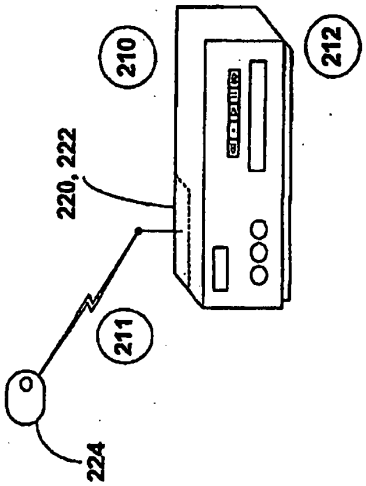


FIG. 9b



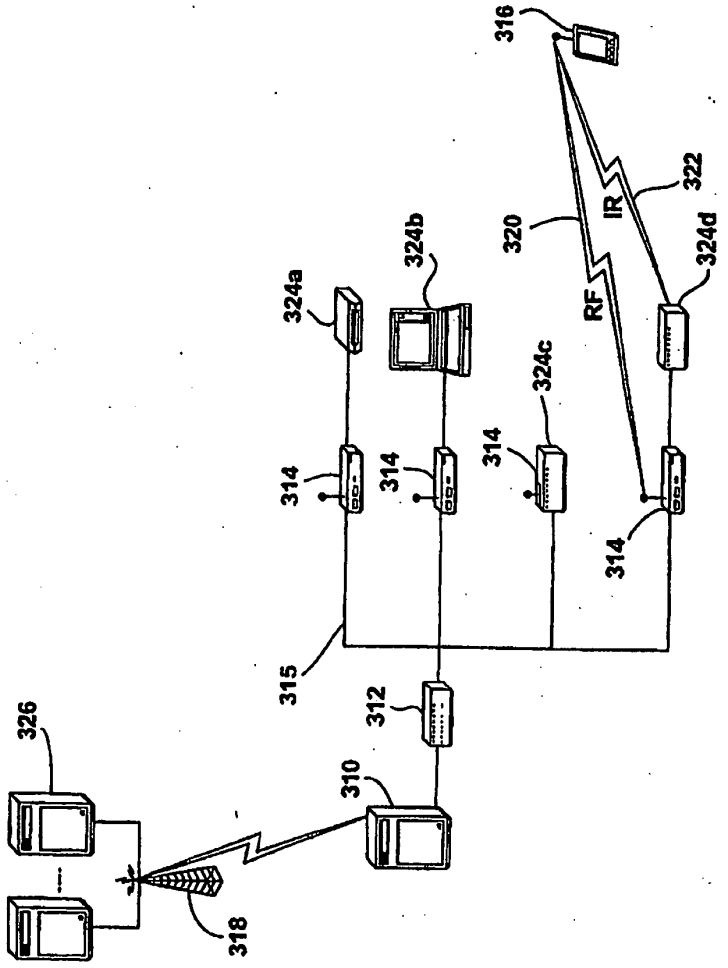

316
322
IR
320
RF
324d
324b
324a
324c
314
314
314
314
315
312
310
326
318

FIG. 10

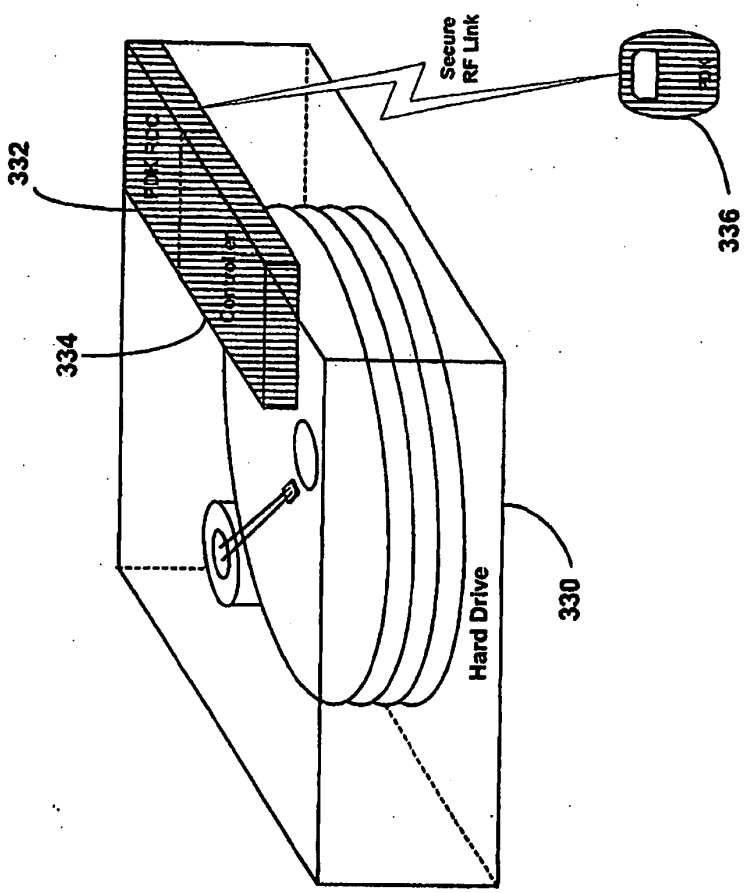

Secure
RF Link
FPK
336
332
Flash ROM
Controller
334
Hard Drive
330

FIG. 11

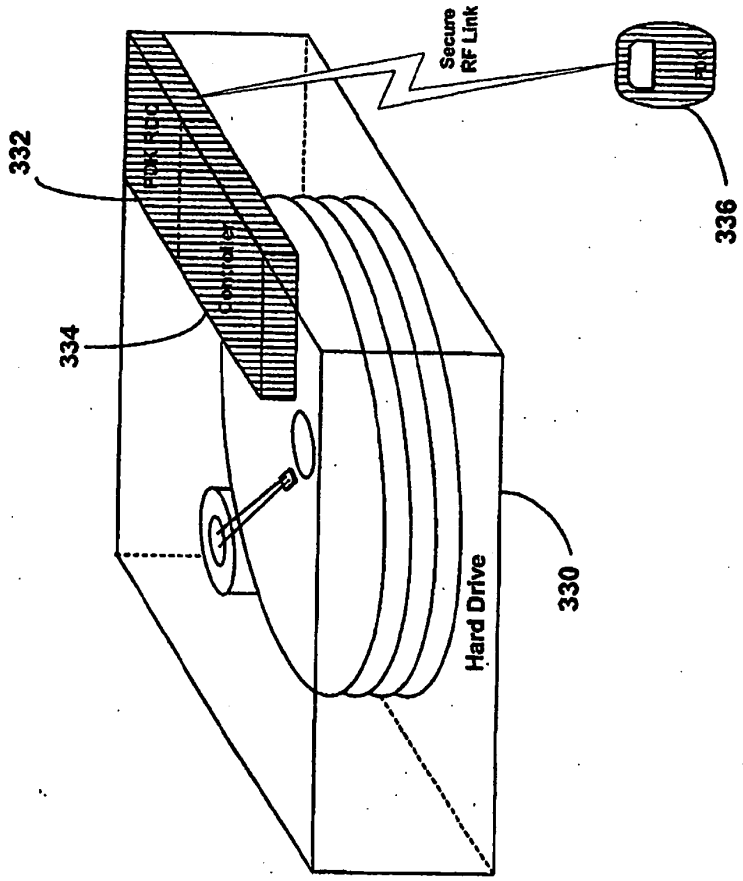


FIG. 12

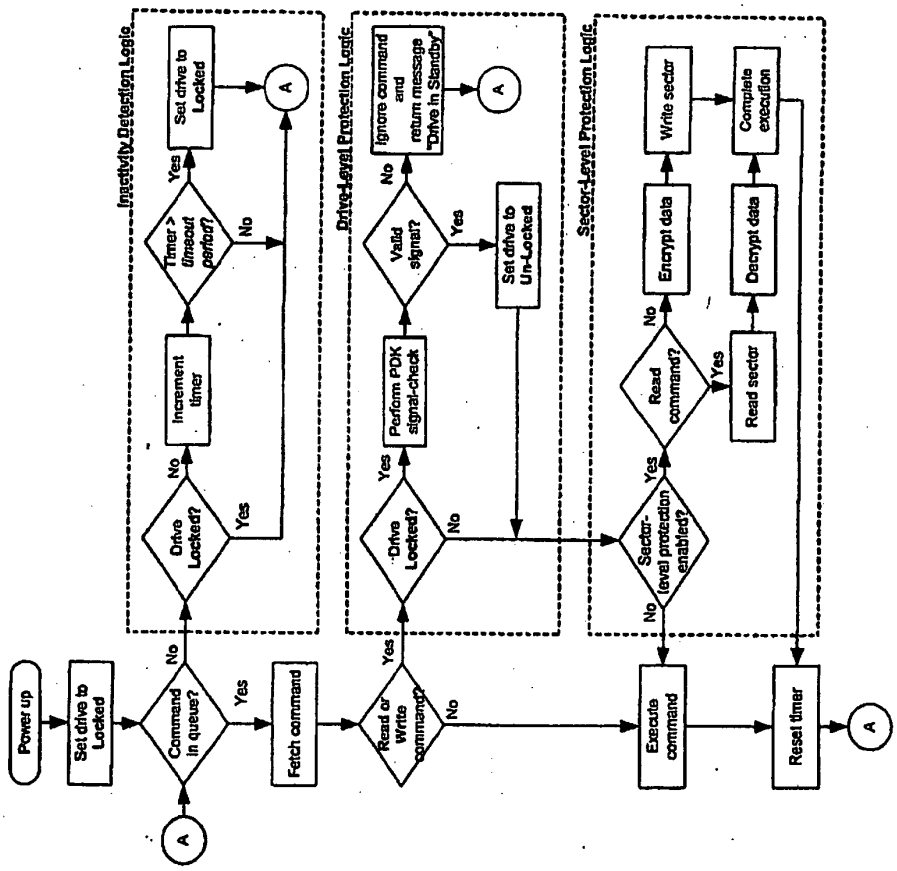

Power up
Set drive to Locked
Command in queue?
No
Yes
A
Fetch command
Read or Write command?
Yes
No
Inactivity Detection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
A
Drive-Level Protection Logic
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
A
Set drive to Un-Locked
Sector-Level Protection Logic
Sector-level protection enabled?
Yes
No
Read command?
No
Yes
Encrypt data
Write sector
Decrypt data
Read sector
Complete execution
Execute command
Reset timer
A

FIG. 13

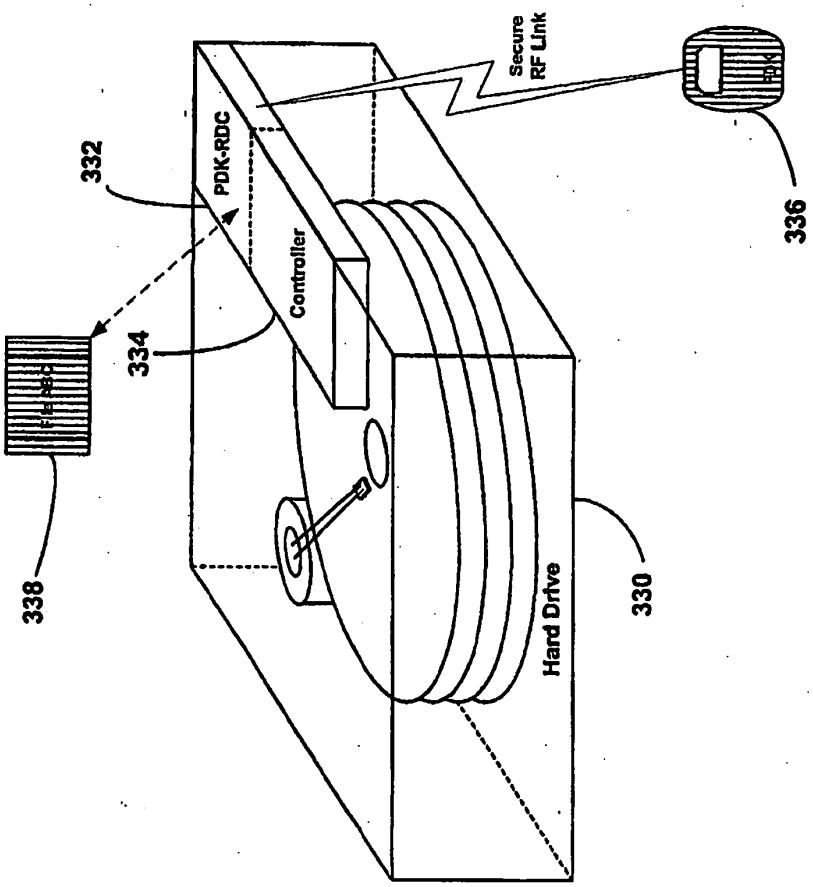

Secure
RF Link
PDK-RDC
Controller
Hard Drive
332
334
336
338
330

FIG. 14

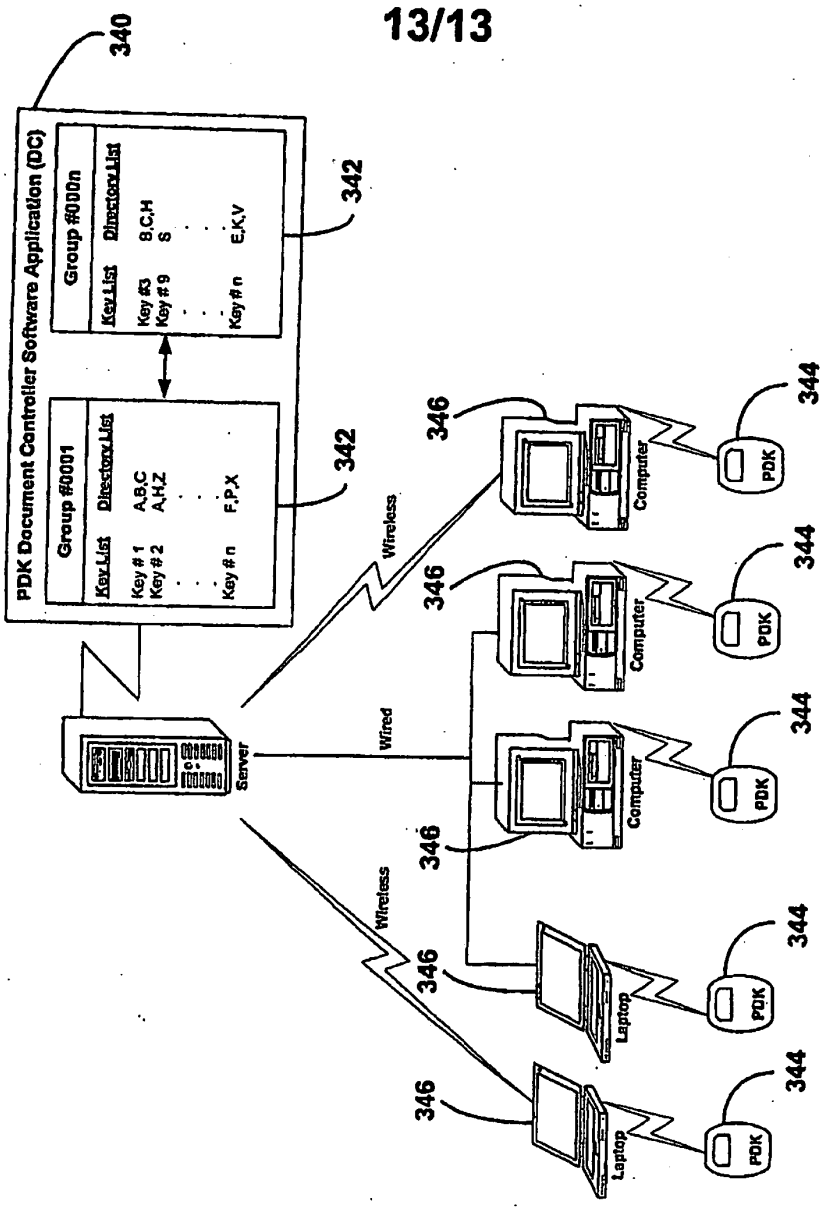

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key # 1
Key # 2
Key # n
A,B,C
A,H,Z
F,P,X
342
Group #000n
Key List
Directory List
Key #3
Key # 9
Key # n
B,C,H
S
E,K,V
342
Server
Wired
Wireless
Wireless
346
Computer
Computer
Computer
Laptop
Laptop
PDK
344

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
17 March 2005 (17.03.2005)

Date of mailing of the international search report
07 APR 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Gilberto Barron

Telephone No. 571-272-3799

Form PCT/ISA/210 (second sheet) (January 2004)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086802 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/007535

(22) International Filing Date: 8 March 2005 (08.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/551,320 8 March 2004 (08.03.2004) US

(71) Applicant *(for all designated States except US)*: **MARGENT DEVELOPMENT, LLC** [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GIOBBI, John, J.** [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: **STEFFEY, Charles, E.** et al.; P.O. Box 2938, Minneapolis, MN 55402 (US).

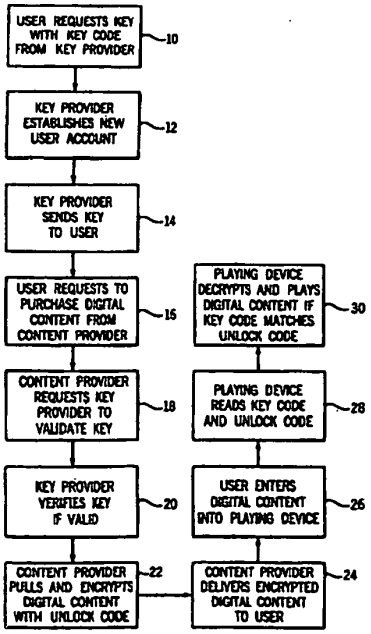
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)

(57) Abstract: One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.



WO 2005/086802 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)

FIELD OF THE INVENTION

The present invention relates generally to embodiments of a linked account system using personal digital key (PDK-LAS).

BACKGROUND OF THE INVENTION

The market for downloading digital content online is rapidly climbing because distribution of such content is inexpensive, fast, and easy and the quality of the content itself is acceptable. The market, however, remains disorganized due to competing standards, competing companies, discontented artists and producers, and outright theft of digital content.

Digital rights management (DRM) companies seek to solve the foregoing problems by delivering the digital content from the real producers to the right customers and ensuring that everyone who should be paid in fact is paid. DRM seeks to get everyone paid by managing the multiple steps for distributing digital content (music, video, software) online: watermarking, encryption, transaction management, and rights management. Some DRM companies perform all these steps, while other DRM companies specialize in one or two steps of the process.

First, watermarking stamps each piece of digital content with a digital mark so it can be tracked wherever it goes. Digital watermarks are just like paper watermarks, except they cannot be seen or heard. Special software is required to read a digital watermark.

Second, encryption scrambles watermarked digital content and stores it inside a digital safe for shipment around the Internet. The safe protects the content during shipping by allowing only those with the right software key to the safe to decrypt and use the content.

Third, transaction management handles actual payments for the digital content using credit card techniques found elsewhere in e-commerce. An order

is placed, a credit card number is taken, account status is checked, and the exchange is authorized.

Finally, rights management manages the information about the digital content itself: what it is, who gets it, how it is delivered, how many times it may be used, how long the rights last, who gets paid, how much they get paid, and how. This information travels with the digital content in something called a digital permit. The permits rests on top of the digital content as it travels the Internet and allows legal users to enjoy the digital content for as long as the rights last.

The primary objective of DRM companies is to deploy technologies that protect digital content as it is distributed online. Some of these proposed technologies and DRM in general are discussed in the article "Digital Rights Management May Solve the Napster 'Problem'," *Technology Investor*, October 2000, pp. 24-27. Although such technologies should reduce the amount of digital theft, they generally favor the content provider at the expense of the consumer or favor the consumer at the expense of the content provider. That is, the rights of either the content provider or the consumer are compromised. For example, some technologies severely limit the consumer's ability to make extra copies of digital content even when the digital content is solely for personal use. Other technologies facilitate the making of copies of digital content which can be used by different consumers without the content provider being compensated by each consumer. The present inventor has discovered an improved DRM system and method that effectively balances and protects the rights of both the consumer and the content provider. In addition, the present inventor has discovered an associated digital content security system for protecting computers and other storage devices from unauthorized use and protecting the digital content stored on computers and other storage devices from being wrongfully accessed, copied, and/or distributed.

With the advent of the Internet, and online shopping, banking and so forth, the Internet has enabled the incidence of credit card, bank account

information, and similar data being stolen has risen dramatically. The cost to providers of transactions performed with these stolen items is enormous and results in higher transaction fees and product pricing to consumers, as it is the providers who are typically responsible for charges applied to stolen account information.

Additionally, the inconvenience and tangential problems that victims, consumers, suffer as a result of such crimes are often traumatic, but are minimally troublemsome. The insufficient technologies and procedures currently utilized to secure account-based transaction processing do little to prevent these crimes. The problem is most notable in the case of the largest growing segment for such transactions, the on-line environment.

SUMMARY OF THE INVENTION

One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a flow chart of a method of managing digital rights in accordance with the present invention;

FIGS. 2, 3, and 4 are block diagrams of portions of a DRM system for implementing the method in FIG. 1;

FIG. 5 is a conceptual model of core options for acquiring digital content that can be encoded to produce key-secured content and core options for playing back the key-secured content;

FIG. 6 is a block diagram for implementing a core acquisition option of downloaded content;

FIG. 7 is a block diagram for implementing a core acquisition option of store-bought content;

FIG. 8 is a block diagram for implementing a core acquisition option of broadcast content;

FIGS. 9a and 9b are block diagrams for implementing a core playback option of stand-alone devices;

FIG. 10 is a block diagram for implementing a core playback option of networked devices;

FIG. 11 is a block diagram of a standard computer hard drive incorporating an integrated PDK-RDC (receiver/decoder circuit) for the purpose of enabling multiple methods of securing digital content;

FIG. 12 is a block diagram for implementing Drive-Level protection and Sector-Level protection in connection with the computer hard drive;

FIG. 13 is a flow chart of the logic executed by the PDK-RDC for implementing Drive-Level protection and Sector-Level protection;

FIG. 14 is a block diagram for implementing File-Level protection in connection with the computer hard drive; and

FIG. 15 is a block diagram for implementing Network-Level protection by expanding File-Level protection to a network environment.

FIG. 16 is a schematic view of a PDK key system embodiment of the invention.

FIG. 17 is a schematic view of a PDK key system embodiment of the invention.

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

DESCRIPTION OF SPECIFIC EMBODIMENTS

Definitions

As used herein, "PDK Key or Key" refers to a PDK-compliant wireless key providing access to PDK-protected objects. The acronym "PDK" refers to "personal digital key."

A "PDK-hard drive" refers to a physical or "electronic" hard drive containing an integrated RDC.

A "PDK-protected product/object" refers to a hard drive or accounts or content protected via PDK technology .

An "assigned key" is a PDK key assigned to one or more protected objects.

An "RDC" refers to a Reader/Decoder circuit installed in a user's computer, or built into computer hard drive, or point-of-sale (POS) credit card swipe unit which communicates with PDK keys and decodes PDK data.

A "POS RCD" refers to a reader/decoder circuit integrated in a standard point-of-sale (POS) credit-card swipe unit.

A "manufacturer" as used herein refers to a manufacturer of PDK-keys.

A "provider" as used herein refers to an entity issuing a PDK-linked account, PDK hard drives and so forth.

A "customer" or "user" refers to an individual possessing or utilizing a PDK key.

A "master" or "master key" refers to a PDK key initially assigned to a PDK protected object, and which is required to be present for configuration transactions.

Description

One system embodiment of the invention, illustrated at 1000 in FIG. 16 includes a personal digital key, PDK, 1010, a point-of-sale reader decoder circuit, POS RDC, 1012, a PDK reader decoder circuit, 1014 that is connected to a provider 1016 having a database 1018. For some

embodiments, the PDK reader decoder circuit and POS RDC 1014 are in a single unit 1020, which for some embodiments, is a standard credit card swipe unit integrated with RDC. For some embodiments, a standard credit card 1022 is readable in the reader 1020. The provider 1016 may be a credit card processor, bank or other similar entity. The account database 1018 maintains the account number, PDK key number and other identifiers of the user.

In another embodiment, illustrated at 2000 in FIG. 17, the PDK 1010 interfaces with a computer 2002 through a secure RF link 2004. The computer 2002 is a standard personal computer, with integrated RDC, PDK-hard drive or RDC adaptor card. The computer 2002 communicates with the provider 1016 through a standard Internet connection 2006. The provider 1016 communicates with the database 1018 in a manner as described in the embodiment described above.

Once in possession of a PDK key, a user optionally registers the key with the key manufacturer or a central key database. No usage data, credit or bank account numbers, hard drive IDs, etc. is maintained in the manufacturer's database, only user verification information. This information includes a customer account number, indicating for some embodiments, a customer's record within the manufacturer's database, customer name, address and phone, key number, and status of key, in-use, stolen, lost and so forth. This information is used primarily for verification purposes during lost key replacement procedures.

The data fields stored in PDK keys include a user label which includes user text label in an unprotected field. The data fields also include an account number, which is a user's manufacturer account number, which is in a protected field. The data fields also include a key number which is a unique key identification and is a protected field.

The PDK key communicates with one of three basic implementations of a PDK-RDC which include POS RDC, a standard credit card swipe type device with an integrated RDC. A second implementation is an RDC

adaptor, which is an add-on PC board RDC, interfacing via USB, firewall, PC card, expansion slot and so forth. A third implementation is a PDK hard drive which is a standard hard drive with an integrated RDC.

POS RDC devices are used in stores at checkout lanes, purchase counters, hand-held swipes, and so forth. RDC adaptors or PDK hard drives are intended for PC based use.

Physical cards such as credit/debit card accounts, bank accounts, membership accounts, or similar types of accounts, intended for use with the PDK LAS technology are conventional cards. No changes are required to such cards in order to ready them for use with the PDK LAS technology. From a consumer standpoint, this feature, along with an ability for a PDK-key to be purchased and assigned to an object at any point, enables easy acceptance of the technology.

Additionally, the PDK-LAS technology offers great flexibility in how PDK-keys are distributed, assigned, and used. For example, providers may optionally allow dynamic key assignment, assigning keys at a later date, assigning multiple keys to the same account and so forth, and users may elect to use one PDK key for all their PDK based security needs, i.e. one PDK key can be assigned to multiple accounts, PDK hard drives, and other PDK based products.

Specific examples illustrating uses of the PDK linked account embodiments are described as follows. These examples are presented to show particular applications of the PDK linked accounts and are not intended to limit embodiments of the invention.

In a first example, a user wishes to assign a key to a new PDK linked account. The user logs onto a provider's site over the Internet via the user's personal computer, in one embodiment. The user inputs whatever validation the provider typically requires. Sufficient data is requested by the provider during this transaction to authenticate the user. An RDC reads the user's PDK key data and transmits the data to the provider. The provider confirms the user's request to link the PDK key to the account. Once confirmed, the

PDK key data is permanently stored in the provider's database as a master PDK key and can only be changed by directly contacting the provider.

In one other embodiment, users phone providers directly and verbally relay all required information, including master PDK key data, printed on a card included with the PDK key at purchase. For users with Internet access but no RDC, this information is hand entered on the provider's website.

In a second example, a user wishes to assign additional keys to a PDK linked account. The user logs onto a provider site and inputs whatever validation the provider typically requires. The user ensures that the assigned master PDK key is within the vicinity of RDC. The RDC reads the master and additional PDK key data and transmits the data to the provider. The provider confirms a user's request to link additional PDK keys to the account number, or change PDK keys or remove PDK keys. Once confirmed, the updated PDK key data is stored in the provider's database along with master PDK key data.

In an alternate embodiment, to facilitate users without an RCD equipped personal computer and Internet access, users may phone providers directly and verbally relay all required information, including both master and additional PDK key data, printed on cards (or similar) included with PDK keys at purchase. For users with Internet access but no RDC, this information may be hand entered on the provider's website.

In a third example, the user wishes to utilize a PDK linked account to purchase a product at a store. The user ensures that an assigned PDK key is within the vicinity of POS RDC at a checkout counter. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using currently accepted procedures, to the provider for verification. If more than one PDK key is read at the counter, either data from all of the PDK keys may be transmitted to the provider or User Labels may be displayed on POS RDC to enable the user or clerk to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to

information stored in the record. If a match is confirmed, the sales transaction is completed normally. If not confirmed, the transaction cannot be completed.

A fourth example is one where a user desires to utilize a PDK linked account to purchase a product on –line or the user wishes to access account information on line. The user must ensure that an assigned PDK key is within the vicinity of RDC. The RDC reads the user's PDK key and transmits data, along with the user's account number, acquired using conventional techniques, to the provider for verification. If more than one PDK key is read at RDC, either data from all PDK keys is transmitted to the provider or User Labels are displayed on a computer screen to enable the user to select the appropriate PDK key. The provider looks up the account record in its database using the transmitted account number and compares the transmitted PDK key data to information stored in the record. If a match is confirmed, the transaction/session is completed normally. If not confirmed, the transaction/session cannot be completed.

A fifth example is one where the user loses a PDK key. After an initial master PDK key setup, users are encouraged to immediately assign an additional PDK key, which serves as a day-to-day key, and store the master PDK key in a safe location. If the day-to-day key is lost, the master is usable to assign the new day-to-day key. As a last resort, for users losing all PDK keys, the key manufacturer may be contacted and, after authentication is performed, instructed to ship a replacement PDK key.

Turning now to the drawings and referring initially to FIG. 1, there is depicted a method of managing digital rights in accordance with the present invention. First, a new user requests a physical electronic key or data unit from a key provider (step 10). The key provider may offer a web site on the Internet, a toll free telephone number, and/or retail outlet where the key may be acquired. In addition, the key provider may allow a key to be requested in writing, preferably using a form designed by the key provider. In one model the user may acquire

as many keys as desired, while in another model each user is only entitled to a single key.

Second, in response to the user's request for a physical key, the key provider establishes a new secure account for that new user in a secure user account database (step 12). The new account may include the following data fields: account number, password, software encryption key, user label, number of users (linked to account), address, telephone number, e-mail address, and custom fields. The custom fields may, for example, include demographic information such as the user's age, gender, marital status, income level, interests, hobbies, etc. The physical key may include the following data fields: user label, account number, software decryption key, and a custom storage area. The user label and the account number serve as a first activation code (or key code) for the acquired physical key. All data fields on the physical key, except for the user label, are preferably encrypted. To allow the user to view his or her account in the future, the user is preferably assigned a login name and the above-noted password.

Third, the key provider ships the physical electronic key to the new user via a package courier such as the U.S. Postal Service, United Parcel Service, or Federal Express (step 14). In one pricing model the physical key is sent to the user at no charge, while in another pricing model the physical key must be purchased by the
user. If the physical key must be purchased by the user, either the user must provide credit/debit card information to the key provider in step 10 to pay with a credit/debit card, or the key provider includes an invoice with the shipped key in step 14.

FIG. 2 is a block diagram of a system for implementing steps 10, 12, and 14 of the method of managing digital rights. The system includes the new user 100, the key provider's web site 102, and the user account database 104.

Referring back to FIG. 1, fourth, the user transmits his or her activation code in the physical key to a digital content provider, who may have a cooperative relationship with the key provider, and requests to purchase digital

content (music, video, or software) from that content provider (step 16). The content provider may offer a web site on the Internet containing a listing of digital content available for purchase. To transmit the activation code to the content provider via the web site, the user may manually enter the activation code onto a secure page of the web site. Alternatively, the transmission of the activation code may be automatically implemented with wireless technology. Specifically, the user's computer may be outfitted with a detector that detects the activation code in the user's physical key and then relays the activation code to the content provider via the web site. The content provider may be affiliated with the key provider or may be separate from the key provider but have an arrangement therewith.

Fifth, the content provider requests the key provider to verify the activation code transmitted by the user (step 18). The content provider may send this request to the key provider's web site. Sixth, the key provider in turn accesses the user's account in the user account database and determines whether the activation code is in fact valid (step 20). The key provider may also determine whether the activation code is associated with the user that transmitted the activation code to the content provider. If the activation code is rejected as being invalid, the content provider is so informed and the content provider in turn will not honor any request by the user to purchase digital content. If, however, the activation code is accepted as being valid, the content provider is so informed and the purchase transaction proceeds. As used herein, the term "key provider" generically refers to the entity or entities that manufacture, distribute, and validate the physical keys. These functions may actually be performed by multiple entities at different locations or by a single entity at a single location.

Seventh, after securing validation of the first activation code in the physical key, the content provider pulls the requested digital content from a digital content database/library, marks the digital content with a second activation code (or unlock code) associated with the first activation code in the physical key, and encrypts the marked digital content (step 22). The second

activation code in the digital content may simply be the same as the first activation code in the physical key, but at least partially encrypted for security. In one embodiment, the "key-secured" content file includes the following data fields: user label, account number, and digital content. The user label and the account number serve as the second activation code for the digital content. If the content is merely for sampling (described in connection with FIG. 6), the file may include such additional data fields as a receiver/decoder circuit identification number, hour stamp, and life hours. All data fields on the content file, except for the user label, are preferably encrypted.

Eighth, the content provider delivers the encrypted digital content to the user (step 24). The encrypted digital content may be delivered by downloading the encrypted digital content to the user's computer while the user is online at the content provider's web site, by attaching the digital content to an e-mail addressed to the user, or by shipping a disk containing the encrypted digital content to the user via a package courier. The user may pay for the digital content either by providing credit/debit card information to the content provider in step 16 or by paying off of an invoice included with delivered digital content. If the digital content is delivered online, the user is preferably required to provide the credit/debit card information and have such information approved as a prerequisite to delivery of the digital content. If the user possesses more than one physical electronic key and would like the acquired digital content to function with each of the user's keys, all of the activation codes are applied to the digital content. The content provider charges the user based on the number of keys with which the user would like the digital content to function. For example, the user may be charged the same amount for each activation code, or may be charged a larger amount for one activation code and lesser amounts (e.g., surcharges) for additional activation codes.

FIG. 3 is a block diagram of a system for implementing steps 16, 18, 20, 22, and 24 of the method of managing digital rights. The system includes the new user 100, the content provider 106, the key provider's web site 102, the digital content database 108, and the acquired digital content 110.

Returning to FIG. 1, ninth, the user enters the encrypted digital content into a playing device of a type suitable for playing the digital content (step 26). The device may, for example, be an MP3 player, a personal computer, a DVD player, a CD player, a cellular phone, or other portable device. In one embodiment, the device contains a wireless transceiver adapted to receive a radio frequency signal transmitted by a corresponding wireless transceiver in the user's physical electronic key. The wireless transceiver in the device is optionally tracked and "secured" for audit purposes by permanently including a unique identifier assigned by the device manufacturer in the transceiver.

Tenth, with the user's physical electronic key within a short range (e.g., few meters) of the playing device, the playing device reads (1) the first activation code carried in a secure radio frequency signal transmitted by the transceiver in the physical key to the transceiver in the device and (2) the second activation code marked on the encrypted digital content (step 28). The device contains decryption software or hardware for decrypting the encrypted digital content to the extent necessary to read any encrypted portion of the second activation code.

Eleventh, the playing device compares the first activation code and the second activation code and determines whether the first activation code is associated with the second activation code (step 30). Steps 29 and 30 may be performed, for example, when the user presses a "play" button on the playing device or when the user first enters the encrypted digital content into the playing device. If the first activation code is associated with the second activation code, the device decrypts and plays the digital content. If the first activation code is not associated with the second activation code, the device does not play the digital content. If the second activation code is simply the same as the first activation code, then the foregoing comparison determines whether there is a match between the first activation code and the second activation code. In a preferred embodiment, the device continues to play the digital content only while the physical key is sufficiently close to the device to communicate the first activation code to the device and allow the device to compare the first activation

code to the second activation code at least partially encrypted with the digital content even while the digital content is being played. If the physical key is moved out of range, the device is no longer enabled to decrypt and play the digital content. In an alternative embodiment, once the device is initially enabled to decrypt and play the digital content, the device remains enabled until either the "play" function is stopped, a play track/song ends, or the digital content is removed from the device, even if the physical key is moved out of range such that the key can no longer communicate the first activation code to the device.

FIG. 4 is a block diagram of a system for implementing steps 26, 28, and 30 of the method of managing digital rights. The system includes the encrypted digital content 110, the key-enabled playing devices 112, and the user's physical electronic key 114.

As stated above, the user's physical electronic key and the key-enabled playing device contain respective wireless transceivers to communicate the activation code in the key to the device. In a preferred embodiment, the transceivers are small, inexpensive *Bluetooth* radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are plugged into electronic devices, which can then communicate over short distances and through obstacles by means of radio waves. *Bluetooth* is a term used to describe the protocol of a short range (e.g., about 10 meters) frequency-hopping radio link between devices containing the radio chips. These devices are then termed "*Bluetooth*-enabled." The secure radio link replaces a cable that would otherwise be used to connect the devices. Further details concerning *Bluetooth* wireless technology may be obtained from www.bluetooth.com.

Wireless technologies other than *Bluetooth* may be used to communicate the activation code from the user's physical electronic key to the playing device. One example of an alternative wireless technology is known by a trade term "Wi-Fi," which is short for wireless fidelity and is another name for IEEE 802.11

b. Products certified as Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA) are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

In other alternative embodiments, the communication between the user's physical electronic key and the playing device is not wireless. Rather, in one alternative embodiment, the user's physical electronic key communicates the activation code to the playing device via a transmission line such as a serial cable that plugs into the key at one end and the playing device at the other end. In another alternative embodiment, the key is a smart card or magnetic card into which the activation code is encoded, and the key is configured to physically fit into a card reader slot on the playing device.

The above-described DRM method and system for implementing the method are advantageous in that they afford the key holder with tremendous versatility in copying and using encrypted digital content for personal use. At the same time, the rights of the content provider are protected because only the key holder with a key-enabled device can use the encrypted digital content. The key holder can copy the encrypted digital content as many times as desired, but can only play the encrypted digital content on a key-enabled device that is enabled with the physical electronic key coded to decrypt the encrypted digital content. Thus, the digital content, even when copied, remains personal to the key holder. Individuals other than the key holder cannot use the encrypted digital content, even if they copy it, because both the original and copies of the encrypted digital content are still encrypted and the individuals do not hold the physical electronic key coded to decrypt the digital content.

A core element of the present invention is the concept of a portable, physical electronic key that is personal to a particular user. The physical key represents a DRM solution that fully addresses the needs of both consumers and publishers of digital content. The physical key is permanently associated with a user's digital content library. At the time of content acquisition, the physical key becomes permanently associated with the newly acquired content. The user is

now "linked" to that acquired content. A user (e.g., individual or family) may own as many physical keys as desired, but every piece of encrypted digital content purchased is tied to one specific key. The user may duplicate or transfer the acquired content to any media or device for playback as many times as desired, as long as the associated physical key is present. Thus, the present invention guarantees that the acquired content is played only by the user who has legitimately paid for it. The present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to FIG. 5, the present invention fully supports the use of "key-secured" digital content 125 with all core content acquisition options and all core playback options. The key-secured digital content 125 is encoded with a second activation code associated with a first activation code stored on the user's physical electronic key. The core acquisition options include downloaded content 120, store-bought content 122, and broadcast content 124. The core playback options include stand-alone devices 126 and networked devices 128. Each of these options are described in further detail below.

Referring to FIG. 6 generally, as already noted in FIGS. 1 through 4, a primary application of the present invention is its use in the downloading of digital content from the Internet. A consumer shops a content distributor's website and selects a piece of content they wish to purchase (music, movies, software, E-books, etc.). The consumer then provides the web site with standard on-line purchase information including the selection's title and method of payment, as well as their physical electronic key information. Transparent to the consumer, the distributor's web site links to the key provider's web site and transmits the physical key information for validation. The key provider's web site then provides the distributor's web site with the information required to prepare the acquired content for secure shipment to the consumer (or notification that the physical key was invalid). The key provider's web site records the transaction for later billing. Finally, the distributor's web site retrieves a copy of the digital content from its library, permanently links it to the consumer's

physical key (by using the key's information to encrypt it), and transmits the secured content to the consumer. The consumer is now free to duplicate the content as often as desired, and to play the content on any key-enabled playback device.

Referring to the specifics of FIG. 6, the process of implementing the core acquisition option of downloaded digital content 120 (see FIG. 5) proceeds as follows. At step 130, a receiver/decoder circuit 140 retrieves an account number from a consumer's physical key (transponder) 142 over a secure RF link. At step 131, the consumer enters such data as a password, purchase selection, and method of payment via the consumer's personal computer 144. The data is transmitted to a content distributor's web site 146 from the consumer's personal computer 144. At step 132, the content distributor's web site 146 transmits the account number and password to a key provider's web site 148. At step 133, the key provider's web site 148 authenticates all data against its database 150 and, if authentic, returns such information as the account number, user label, number of users, and software encryption key to the distributor's web site 146. If the data is not valid, the key provider's web site 148 sends a message to the distributor's web site 146 indicating the same. A counter, used for the key provider's billing purposes, is incremented. At step 134, the distributor's web site 146 pulls the purchased content file from its database 152, encrypts it with the software encryption key it received in step 133, and builds a final key-secured content file that is then transmitted to the consumer's personal computer 144. Charges are assessed based on the number of users, etc. and billed to the consumer according to the method of payment. At step 135, invoices 154 are generated and sent to content distributors by the key provider's web site 148 on a regular cycle.

Optionally, to enable content providers to offer sample content (e.g., limiting playback to the device on which the content was originally downloaded, for a specified period of time) a special "enhanced" version of a receiver/decoder circuit 140 can be produced. These enhanced receiver/decoder circuits (primarily for PC's) would each include a unique identification number and additional functionality enabling them to "talk" to a key provider's web site 148

to acquire secured timing information. Sample content files may include the following information (in their encrypted header section):

- identification number of enhanced receiver/decoder circuit used for downloading and transmitted by the receiver/decoder circuit to the key provider's web site at the time of content purchase;
- hour stamp (i.e., the hour in which the content was downloaded; and
- life hours (i.e., number of hours content remains valid, such as perpetual, one hour, 24 hours, 48 hours, etc.).

The above information is used by an "enhanced" receiver/decoder circuit during playback to determine whether a content file has "expired" or is attempting to play on an unauthorized device (i.e., any device except the device on which the content
was originally downloaded). This capability allows content distributor web sites to distribute limited-use samples with associated tiered-pricing models.

Referring to FIG. 7 generally, the present invention can be extended to store-bought content. To fully integrate store-bought content into the present invention, traditional store-bought content is modified in two ways. First, the content is distributed in a copy protected format (e.g., using any valid copy protection technology). Second, the content contains a unique content serial code. The content serial code may be contained either directly in the digital content or as a physical label. Each content serial code is designated by a content distributor during manufacturing and stored in the key provider's database. This database is later used to validate that each content serial code is unique and used only a prescribed number of times. To a consumer, a content serial code on their newly purchased store-bought content represents a download of a key-secured version of that content for free or a prescribed price. This key-secured copy provides the consumer with exactly the same advantages and freedoms as any other key-secured content. From the consumer's standpoint, the download process occurs exactly as any other standard key-secured content download with the exception of how the payment is handled. The "payment" is the content serial code. By providing all of the advantages of the present

invention to consumers of legacy-capable store-bought content (by way of "content serial code downloads"), the scheme provides the industry with the first complete DRM solution.

Referring to the specifics of FIG. 7, the process of implementing the core acquisition option of store-bought digital content 122 (see FIG. 5) proceeds as follows. At step 160, a receiver/decoder circuit 170 retrieves an account number from a consumer's physical key (transponder) 172 over a secure RF link, and the consumer's personal computer 174 reads a content serial code from the store-bought content 122. The store-bought content 122 contains the content serial code that uniquely identifies the content. The format of the content serial code may, for example, be PPPP.FFF.0123456789 where PPPP is a provider identification, FFF is a facility identification, and the numbers represent a sequence number. The store-bought content 122 incorporates a copy protection scheme such as Macrovision™, key2audio™, or SafeAudio™. Disc "copy flags" (specified in SDMI standards) may also be set to further inhibit duplication efforts.

At step 161, the consumer enters such data as a password and purchase selection via the consumer's personal computer 174. The previously-read content serial code specifies that the method of payment is to a "content serial code-credit" (i.e., there is typically no charge for this download because the content serial code confirms that the download in process is of content that the consumer has already legitimately purchased). The data is transmitted to a content distributor's web site 176 from the consumer's personal computer 174. At step 162, the distributor's web site 176 transmits the content serial code, account number, and password to a key provider's web site 178. At step 163, the key provider's web site 178 authenticates all data against its databases 180 and 182 and, if authentic, returns such information as the account number, user label, number of users, software encryption key, and paid-flag (indicating the content serial code has been validated) to the distributor's web site 176. The key provider's web site 178 now sets the paid-flag to disable any further downloads and records the account number field in the content serial code database 182 for

auditing purposes. If the data is not valid, the key provider's web site 178 sends a message to the distributor's web site 176 indicating the same. A counter, used for the key provider's billing purposes, is incremented. Each entry in the content serial code database 182 may include the following data fields: CDC #, paid-flag, and account number. At step 164, the distributor's web site 176 pulls the content file from its database 184, encrypts it with the software encryption key it received in step 163, and builds a final key-secured file that is then transmitted to the consumer's personal computer 174. No charge is typically assessed because a valid content serial code serves as "payment" for the download. At step 165, invoices 186 are generated and sent to content distributors by the key provider's web site 178 on a regular cycle.

Referring to FIG. 8 generally, the present invention can be extended to broadcast content. To fully integrate broadcast content into the present invention, traditional broadcast content is only minimally modified. The modification is that the broadcast content is transmitted in a copy protected format (such as the DVD standard known as Content Scramble System (CSS)). The remainder of the process is described below. A key-enabled recording device, incorporating a unique identifier, receives copy-protected broadcast content. If only playback of the broadcast content is desired, basic decoding (e.g., CSS) is performed and the broadcast content is sent on for playback. If the consumer wishes to record the broadcast content, however, the recording device performs additional steps prior to sending the broadcast content on for playback. The recording device connects to the key provider's web site to validate the recording device's internal identifier and the consumer's physical key. If both are valid, the recording device translates the broadcast content into a key-secured format by encoding it with the consumer's activation code, and then stores the key-secured content file, with its identifier permanently embedded within, for later use. The end result is key-secured broadcast content that provides the owner of the associated physical key all the freedoms and advantages of the present invention. Although the content was originally broadcast, it cannot be

illegally copied or distributed. The present invention can be applied to pay per view offerings, as well as standard broadcast material.

Referring to the specifics of FIG. 8, the process of implementing the core acquisition option of broadcast digital content 124 (see FIG. 5) proceeds as follows. At step 180, a receiver/translator/recording device 190 receives digitally broadcast content in copy-protected format from a source 192 such as satellite, cable, Internet, or over-air. The broadcast content may be copy-protected using a copy-protection technology such as an enhanced CSS scheme. If a consumer wishes to only play (not record) the broadcast content, basic decoding (e.g., CSS decoding) is performed and the broadcast content is passed through to presentation device 194 for playback. The remaining steps below may be skipped.

If, however, the consumer wishes to record the broadcast content, the following additional steps are performed prior to sending the broadcast content on for playback. At step 181, the receiver/translator/recording device 190 retrieves an account number from the consumer's physical key (transponder) 196 over a secure RF link. At step 182, the receiver/translator/recording device 190 transmits the account number and its recorder serial code to a key provider's web site 198. Each device 190 contains a recorder serial code that uniquely identifies the device. The format of the recorder serial code may, for example, be MMMM.FFF.0123456789 where MMMM is a manufacturer identification, FFF is a facility identification, and the numbers represent a sequence number. At step 183, the key provider's web site 198 authenticates the data against its databases 200 and 202 and returns an "approved" or "rejected" response. A counter, used for the key provider's billing purposes, is incremented. At step 184, if a "rejected" response is received, the broadcast content cannot be recorded. If an "approved" response is received, the receiver/translator/recording device 190 translates the decoded content into a key-secured format by encoding it with the consumer's activation code, and records the key-secured content, with the recorder serial code permanently embedded within, to a storage device (that can optionally be an external device).

The broadcast content can now be copied to and played back on any key-enabled playback device. At step 185, invoices 199 are generated and sent to content distributors by the key provider's web site 198 on a regular cycle. While providing excellent additional security and protections, steps 182 and 183 are not mandatory for the present invention to function with broadcast content. It may be desirable, for cost purposes, to produce receiver/translator/recording devices 190 not capable of communicating with the key provider's web site 198.

Referring to FIGS. 9a and 9b generally, having acquired key-secured digital content and produced copies for playback on various devices such as a portable CD player, personal computer, home theater, etc., a consumer is now ready to use the digital content. Playback of key-secured content occurs as follows. A key-enabled playback device transparently reads information from a consumer's physical key and from the content file the consumer has requested to play. The pieces of information are then compared to validate that the physical key "matches" the content to be played. If the elements match, the device begins playback of the content. If the elements do not match, the device will not play the content and, depending upon the device's capabilities, may display an "invalid content" message. From a consumer's point of view, when used with legitimately-acquired content, the process is entirely transparent, effortless, and non-intrusive. The consumer is free to use their content on any key-enabled playback device, with the only restriction being that the content can be played only when the associated physical key is present. As noted above, the present invention gives consumers unprecedented freedoms and conveniences to use legitimately purchased content while still fully protecting content providers' rights.

Referring to the specifics of FIGS. 9a and 9b, the process of implementing the core playback option of stand-alone devices 126 (see FIG. 5) proceeds as follows. At step 210, a consumer requests playback of a key-secured content file via a playback device 220. The playback device 220 may, for example, be the consumer's personal computer (FIG. 9a) or a stereo amplifier (FIG. 9b) with integrated compact disc reader/player. At step 211, a

receiver/decoder circuit 222 searches for a physical key (transponder) 224. The circuit 222 may be a separate component from the playback device 220 as in FIG. 9a or integrated into the playback device 220 as in FIG. 9b. If the physical key is not found, the playback device 220 displays an "invalid content" message. If the physical key is found, the receiver/decoder circuit 222 retrieves all available information from the physical key 224 over a secure RF link. At step 212, the user labels in the physical key 224 and the key-secured content file are compared. If the user labels do not match, the playback device 220 displays an "invalid" message. If the user labels do match, the receiver/decoder circuit 222 retrieves the software decryption key from the physical key 224 over the secure RF link between the physical key 224 and the playback device 220 and begins decryption of the encrypted portion of key-secured file. When the account number is decrypted, it is matched against the account number retrieved from the physical key 224. If the account numbers do not match, the playback device 220 displays an "invalid content" message. If the account numbers do match, the software decryption key is used by the playback device 220 to decrypt remaining data in the key-secured file for playback. The user label and the account number in the physical key serve as a first activation code, and the user label and the account number in the content file serve as a second activation code. These activation codes must match (or have some other predetermined association) in order for playback to proceed.

Referring to FIG. 10 generally, while stand-alone playback devices (e.g., CD players, PCs, DVD players, etc.) are currently the norm, the convergence of these devices and the Internet will lead to an environment where centralized digital distribution systems proliferate. Security of content in these environments is critical yet challenging to accomplish without imposing great restrictions. The present invention can provide security to a centralized digital distribution system and, in addition, offers many important enhancements that greatly increase the convenience and usability of such a system. These enhancements include integration of the physical key into a portable handheld computer which then doubles as the system remote. In addition to controlling all

networked components, the remote is used for tasks such as purchasing content from the Internet, and tracking the movement of a user throughout a facility to provide automatic "content following" (i.e., where content playback follows the user from room to room). The centralized nature of the digital content distribution system means that only one storage device is required to maintain a consumer's entire digital content library (e.g., music, movies, software, E-books, etc.) and to feed that content to any networked playback device.

Referring to the specifics of FIG. 10, there is shown a centralized digital content distribution system for implementing the core playback option of networked devices 128 (see FIG. 5). The system is used in an establishment such as a residence or entertainment facility. The system includes a digital content server 310, a distribution hub 312, a plurality of remote clients 314, and a portable remote control 316. The digital content server 310 stores digital content acquired from a source 318 such as satellite, cable, Internet, or over-air. In addition, the digital content server 310 may store digital content uploaded from a standard component 324. The plurality of remote clients 314 are located in different rooms of the establishment and linked to the digital content server 310 via the distribution hub 312 or switch. The remote clients 314 are linked to the distribution hub 312 by a backbone transmission network 315. The backbone transmission network 315 may be wireless or wired with fiber optic cables, coaxial cables, or twisted pair cables, may employ a networking protocol such as Ethernet, Wi-Fi, Arcnet, or ATM (Asynchronous Transfer Mode), and may employ a communications protocol such as TCP/IP. Each remote client 314 includes a network interface card (NIC) for interfacing with the backbone transmission network 315.

The remote control 316 is adapted to communicate with each of the remote clients 314 and select the digital content stored in the digital content server 310. The remote control 316 is essentially a personal digital assistant (i.e., hand-held computer) including a display and added remote control circuitry. The display may, for example, be a liquid crystal display (LCD). The

added remote control circuitry includes "system remote" circuitry and "universal remote" circuitry.

The "system remote" circuitry in the remote control 316 is for establishing a first wireless transmission link 320 with each of the remote clients 314. The first wireless transmission link 320 may be a secure radio link (RF) as shown or an infrared link (IR). Upon establishing the first wireless transmission link 320 with one of the remote clients 314, the remote control 316 serves as a system remote capable of (1) displaying, scanning, and selecting the digital content available on the digital content server 310 and downloading the selected digital content from the digital content server 310 to the linked remote client 314 and (2) controlling the digital content server 310 to acquire or download digital content from a source 318 such as satellite, cable, Internet, or over-air. As used herein, the term "download" and similar variations thereof (e.g., downloaded, downloading, etc.) is intended to cover the transfer of content from one device to a receiving device whether the content is stored on the receiving device or merely "streamed" to the receiving device for immediate playback. The remote control 316 preferably includes a display for displaying the digital content. The display may, for example, be a liquid crystal display (LCD). As a user holding the remote control 316 moves from room to room of the establishment, the remote control 316 successively establishes wireless transmission links 320 with the remote clients 314 in the respective rooms. In this way, the digital content available on the digital content server 310 follows the user's movement from room to room.

In a preferred embodiment, the first wireless transmission link 320 is a secure radio link established by matching transceivers in the remote control 316 and each remote client 314. The matching transceivers are preferably small, inexpensive Bluetooth™ radio chips that operate in the unlicensed ISM band at 2.4 GHz and avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. The radio chips are integrated into the respective remote control 316 and each remote client 314, which can then communicate over short distances and through obstacles by means of radio

waves. Wireless technologies other than Bluetooth, such as Wi-Fi, may be used to communicate remote control signals between the remote control 316 and each remote client 314.

The "universal remote" circuitry in the remote control 316 is for establishing a second wireless transmission link 322 with standard components 324 connected to the remote clients 314. The second wireless transmission link 322 is preferably an infrared link (IR) as shown. Upon establishing the second wireless transmission link 322 with one of the standard components 324, the remote control 316 series as a universal remote capable of operating the standard component 324. The standard component 324 may, for example, be an audio receiver (stereo amplifier), an audiovisual receiver, a video monitor (television), etc. The standard components 324 may be physically separate from, but linked to, the respective remote clients 314 or may be physically integrated into the respective remote clients 314 like integrated device 324c.

The digital content stored on the digital content server 310 may be formatted as a compact disc (CD), digital video disc (DVD), MP3, electronic book, software, etc. When the remote control 316 is linked to one of the remote clients 314, a user may scan and select digital content to be downloaded from the digital content server 310 to the remote client 314 and converted by the remote client 314 to a standard playable format (e.g., analog format) that can be played on the associated standard component 324. The selected digital content is downloaded from the digital content server 310 to the remote client 314 as raw digital data packets. The remote client 314, in turn, converts the downloaded digital content to a standard component output(s) compatible with a standard component 324 connected to the remote client 314, and the standard component 324 plays the digital content. Ports may, for example, include S-Video, RCA jacks, serial ports, Universal Serial Bus, Ethernet, Wi-Fi, Firewire™, Bluetooth, RF, or other similar outputs. The standard component 324 incorporates, or is linked to, audio speakers for broadcasting any audio signals received from the remote client 314 and a video monitor for displaying any video signals received from the remote client 314.

All content is stored on the digital content server 310 digitally, and is key-secured if obtained via the download or broadcast acquisition options of FIGS. 6 and 8. If the digital content is key-secured, the plurality of remote clients 314 include decryption circuitry (i.e., receiver/decoder circuit) for unlocking the digital content. The digital content selected for download from the digital content server 310 to a remote client 314 preferably remains encrypted until converted to a standard component output(s) in the remote client 314. The remote client 314 acts as a converter between key-secured digital content from the digital content server 310 and the standard component output(s). To decrypt the selected digital content, the remote control 316 contains a physical key initially acquired from a key provider in accordance with the present invention. The digital content is initially acquired from a content provider 326 that marks the digital content with an activation code associated with the physical key. The decryption circuitry in the remote client 314 receives an activation code from the remote control 316 via the wireless transmission link 320 and is enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content. If the activation code in the remote control 316 is not associated with the activation code in the digital content, the remote client 314 will not unlock and convert the digital content.

In an alternative embodiment, the remote clients 314 are eliminated and the standard components 324 are linked directly to standard component outputs of the distribution hub 312 by the backbone transmission network 315. In this case, the distribution hub 312 serves as a switch, and the digital content server 310 contains the decryption circuitry for unlocking the digital content. As the digital content is decrypted, it is converted to a playable format and fed to the distribution switch 312 for delivery to the appropriate standard component 324. The decryption circuitry in the digital content server 310 receives the activation code from the remote control 316 and is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 is associated with the activation code in the digital content.

Instead of decrypting the digital content so that it can be played, the digital content may be downloaded (or "passed through") in its encrypted format to a storage device such as a media burner 324a or computer hard disk 324b for storage thereon. When a user ultimately desires to play the stored digital content on a media player, the media player must contain the decryption circuitry for unlocking the digital content. After unlocking the digital content, the media player converts the unlocked digital content to a playable format and plays the digital content. The decryption circuitry in the media player receives the activation code from the remote control 316 or physical key with the same activation code. The media player is only enabled to unlock and convert the digital content to a playable format if the activation code in the remote control 316 or physical key is associated with the activation code in the digital content.

In addition to downloading selected digital content from the digital content server 310 to the remote clients 314, data (e.g., MP3, CD, DVD, software, etc.) from the standard components 324 can be uploaded to the digital content server 310 and stored digitally thereon. This allows for storage of legacy content on the digital content server 310.

Referring to FIG. 11 generally, a digital content security system and method protects computers from unauthorized use and protects the digital content stored on computers from being wrongfully accessed, copying, and/or distributed. The basic components of the Personal Digital Key Digital Content Security System (PDK-DCSS) are (1) a standard hard drive device 330, with the addition of a PDK Receiver/Decoder Circuit (PDK-RDC) 332 integrated into the controller 334, and (2) a PDK-Key 336 associated with the PDK-RDC as described above. The standard computer hard drive 330 incorporates the integrated PDK-RDC 332 for the purpose of enabling multiple methods of securing digital content. Hard drives 330 incorporating a PDK-RDC 332 are referred to herein as PDK hard drives. While the PDK-DCSS diagrams show the PDK-RDC 332 as being integrated with the hard drive's controller 334, all OS-level protections described below can be implemented using externally-based PDK-RDCs.

A PDK hard drive 330 is similar to any standard, currently available hard drive with the exception of the PDK-RDC 332 (which is integrated into the drive's controller circuit 334). A PDK-RDC 332 is an integrated circuit able to process PDK-Key information, as well as encrypt/decrypt PDK-compliant digital content. Additionally, this circuit 332 is able to secure the hard drive 330 itself. This is implemented by the circuit 332 enabling or disabling the hard drive's controller 334 depending on whether an associated PDK-Key 336 (one which is uniquely and permanently associated with the PDK hard drive 330) is present. Each PDK hard drive 330 would typically be delivered with its own PDK-Key 336.

Secure RF communications between a PDK-Key 336 and its associated hard drive 330 occurs in the same manner as described above. It should be noted that software drivers can optionally be designed to allow for dynamic key assignment (assigning of keys after purchase to enable key swapping, or assigning of individual keys to multiple devices).

The PDK-Key and RDC technology is utilized to provide two categories of protection:

1) Hard drive access control - where an entire drive 330 is either completely accessible (unlocked) or inaccessible (locked), and/or individual data sectors or clusters of data sectors are optionally encrypted/decrypted, depending on whether the specific PDK-Key 336 associated (and shipped) with the drive 330 is within range. This category of protection can be accomplished transparently to the operating system (OS) responsible for managing the drive.

2) OS-level independent file protection - where the drive's RDC 332 functions independently of the drive 330 to protect individual files (typically copyrighted material) from wrongful copying. In this role, the RDC 332 works with any PDK-Key 336 (not just the one delivered with the drive 330) and any PDK-compliant file (they do not have to be stored on or associated with the hard drive 330). This category of protection requires an OS-level software driver be run under the OS responsible for managing the drive.

By utilizing these two categories of protection in various ways, four unique levels of content protection are enabled. Two of the levels (Drive-Level and Sector-Level) do not require external software support, while the remaining two (File-Level and Network-Level) require software drivers, as well as a stand-alone application for Network-Level implementations. Each of the four levels is defined below.

Referring to FIGS. 12 and 13 for Drive-Level protection, when implemented, a PDK hard drive 330 will only function when the associated PDK-Key 336 is within range. The drive's controller 334 is disabled whenever the PDK-Key 336 is not present. The contents of files stored on the drive 330 are not encrypted. The Drive-Level protection feature is designed to protect the hard drive's owner by locking access to the PDK hard drive 330 whenever the associated PDK-Key 336 is not present (i.e. when the owner momentarily steps away from the computer, if the computer is stolen, etc.).

Referring to FIGS. 12 and 13 for Sector-Level protection, when enabled, every sector (or cluster of sectors) read or written is encrypted/decrypted by the RDC 332 using the drive's associated PDK-Key 336. Because the encryption is performed at Sector-Level as opposed to File-Level, the encoding can be accomplished without requiring any changes, involvement, or acknowledgement of the OS responsible for managing the drive. The Sector-Level protection feature is designed to further protect the hard drive's owner (beyond Drive-Level protection) by encrypting the contents of the files stored on the drive, without requiring any software modifications (OS, application, etc.). The security advantage is that if the drive access is in some way defeated, the contents of files on the drive are still protected. It should be noted that if users retrieve files from drive and purposely transfer them anywhere else (via email, memory sticks, etc.), the data will no longer be protected. Drive-Level protection and Sector-Level protection may be used individually or in combination. Also, as noted above, it should be understood that Sector-Level protection may be applied to individual data sectors or clusters of data sectors.

FIG. 13 illustrates the logic executed by the RDC 332 for implementing Drive-Level protection and Sector-Level protection. The logic ensures OS-level commands (save entire file, read entire file, etc.) are given adequate time to complete. This enables implementation of logic without requiring OS changes, involvement, or acknowledgement.

Referring to FIG. 14 for File-Level protection, implemented as an OS-level software driver utilizing the PDK-RDC 332 integrated in the PDK hard drive 330, File-Level protection provides standard PDK digital rights management services and functionality as described above. As needed, the driver instructs the RDC 332 to acquire PDK-Key information, validate the key-to-file match, and use the key's information to perform actual encryption/decryption of the file (as a whole, not at the sector level). In the illustrated example, the file ABC 338 (which can reside on any storage device, in memory, etc.) is compared to any PDK-Key 336 within range of the PDK-RDC 332. If a match is found, the PDK-RDC 332 will decrypt the file 338 for use with whatever playback mechanism placed the request. Any PDK-Key 336 can be utilized, not just the key 336 associated with the PDK hard drive 330. When employed for File-Level protection (and Network-Level protection as described below), the PDK-RDC 332 functions independently of the hard drive 330 in which it resides. While PDK-compliant files it encrypts or decrypts may reside on the resident hard drive 330 and may be associated with the drive's PDK-Key 336, they do not have to be. The PDK-RDC 332 can work with other PDK-Keys and files residing on other mediums. When used in this manner, the PDK-RDC 332 can be thought of as just coincidently residing within the hard drive 330. For File-Level and Network-Level protection, the RDC 332 may be implemented as a separate circuit board (not integrated within the hard drive 330) and still provide identical functionality.

The primary use of File-Level protection is to secure and protect private or copyrighted material from wrongful copying and distribution. Because copies of any PDK-compliant files can only be accessed when the associated PDK-Key is present, File-Level protection enables copies (intended for use by the holder of

the associated key) to be produced effortlessly and securely. In addition to the distribution of copyrighted content such as music and movies as described above, software developers can distribute their software products via the Internet with the same ease and security. Software distributed in this manner would allow the legal recipient to make unlimited copies (for backup purposes, use on a home computer, etc.), yet the copies would only function when the associated key is present, preventing unauthorized copies from being wrongfully distributed and used.

The File-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and pasted into another application (e.g., an email program) thereby defeating the protection. Therefore the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations.

Referring to FIG. 15 for Network-Level protection, File-Level Protection can be expanded to a network environment by employing a centralized software application / database called a PDK Document Controller (DC) 340 ruing on a server 342. A DC 340 enables the creation of Groups 342 that list which PDK-Keys 344 are allowed access to files in specific directories. All files stored in directories controlled by the DC 340 are automatically encrypted using the DC administrator's PDK-Key and thereby become PDK-compliant files. This process places all files stored in the DC 340 in a uniformly encrypted format.

Each user request for a file residing in a directory listed in a DC Group 342 results in the following steps. An RDC located in the requester's workstation 346 acquires information from the user's PDK-Key 344 and relays that information to the DC 340. The DC then enables appropriate access as

defined by the DC's Group database information. Specifically, the DC 340 performing a lookup of the requester's PDK-Key 344 in the appropriate Group's tables. If the DC 340 determines that the PDK-Key 344 is listed in a Group 342 that also lists the directory containing the file the user wishes to access, the DC 340 knows that a valid PDK-Key 344 was used in the file request and grants access. The requested file is first decrypted with the administrator's PDK-Key, re-encrypted with the requester's PDK-Key 344, and then downloaded to the user's workstation 346. The foregoing process mirrors the process employed when using PDK to download digital media files from the Internet.

The Network-Level protection feature is designed to protect publishers of private or copyrighted material. Users can protect any file by converting it to PDK-compliant format; however, security of document files can be compromised by key holders not wishing to maintain the file's integrity. Because, while a Microsoft Word document (as an example) may be stored in the PDK-compliant protected format, once opened the contents could be cut and paste into another application (e.g., an email program) thereby defeating the protection. Therefore, the use of File-Level protection for use with documents is only applicable for entrusted recipients (individuals desiring to protect the content of which they are in possession). Non-document files, however, are not subject to these limitations. The system is well suited for establishing centralized databases of secure documents intended for distribution to entrusted recipients such as personnel in a law firm or medical facility.

While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention. A number of enhancements and variations can be implemented/utilized that effectively broaden the PDK technology's scope and utility. These enhancements and alternative embodiments are summarized below.

Integration of RDCs into Alternative Storage Devices. This embodiment involves integrating RDCs into alternative storage mechanisms

beyond those of basic hard drives. These storage mechanisms include pure RAM/ROM-based storage commonly included/used in devices such as PDAs, cell phones, printer, copiers, faxes, scanners, MP3 players, GPS systems, digital cameras, computer motherboards, and DVR players, as well as portable storage devices such as Memory Sticks, Secure Digital memory cards, or any similar such product, in which case the RDC is either directly installed on the device, or integrated into the device in which the memory cards/sticks are inserted.

When an RDC is utilized in this manner, File-Level and Network-Level security function in the same manner as that described above for PDK hard drives. Drive-Level and Sector-Level security function in the same *logical* manner as that described for hard drives, but the *physical* implementation varies so as to control the bus structure that provides the communications path between the storage mechanisms and their hosting devices. As with PDK hard drives, access to the storage is enabled/disabled by interrupting the communications path, signaling to the hosting device that the storage is either "ready" or "busy," effectively enabling/disabling the device itself. To save batteries, RDCs used in this manner may only check for the presence of the associated PDK-Key on some periodic basis (versus every read or write sequence). And similar to PDK hard drives, Sector-Level security can be optionally utilized to encrypt/decrypt data traveling over the bus prior to writes and after reads to provide PDK's standard Sector-
Level data encoding functionality.

As when utilized in PDK hard drives, the PDK's security features provide the same convenient, non-intrusive, wireless security mechanism for the above-defined devices. This security mechanism protects any data stored on such devices in the event they are ever stolen, left unattended, or even purposely "disabled" to prevent access to sensitive content (i.e. preventing minors from accessing adult files, websites, etc.). When the associated PDK-Key(s) is not present, these devices and their storage means are locked and disabled.

Dynamic PDK-Key Management. Utilizing dynamic PDK-Key management, PDK-Keys can be assigned to an RDC (whether integrated into a

PDK hard drive or some other hosting device, or implemented independently) by a user (versus requiring such assignment at time of production). This capability is accomplished by including the required logic within the RDC's internal firmware (versus using an externally-based software driver to supply such capability).

Using this capability, a user can optionally assign any PDK-Key to act as the RDC's *master* key (the first key assigned to the device). Then by involving this *master* key (to prove the original "owner's" validation of the process), the user can assign (or remove) *additional* keys to the PDK-device. The general benefits of this feature include:

- The ability for the individual possessing the *master* key to create backup keys (to be stored and later retrieved in the event the *master* is ever lost), and to allow other users (those possessing *additional* keys) to also access their PDK device(s).
- The option to ship PDK-RDCs (in any configuration, host devices, etc.) without any PDK-Keys. And to allow such devices containing these RDCs (such as PDK hard drives) to optionally function with all or part of the PDK-technology never enabled or utilized. For instance, a user may elect to not enable Drive-Level and Sector-Level security features, but still utilize the functionalities of File-Level and Network-Level security.
- Giving users the option to purchase and associate a PDK-Key at a later time, or importantly, assign a PDK-Key they *already* utilize for another PDK-based device. This allows a user to utilize a single PDK-Key to provide access to all their PDK-based devices.

This built-in (firmware-based) PDK-Key configuration/management capability greatly enhances PDK's overall flexibility and ease of setup/use.

Independent RDC configuration. While integrating an RDC into a hard drive offers numerous benefits, RDCs may exist separately from hard drive mechanisms. In this configuration (as previously defined) an RDC's physical circuitry may exist in the form of a PC Card, a PC expansion board that plugs into a standard PC expansion slot, a USB-based plug-in board, or any other

similar design able to interface with a hosting device. Used in this manner, RDCs provide all previously defined functionalities with the exception of basic hard drive access-control.

Buffer Flush & Notification Software Driver. This enhancement involves using a simple software device driver to recognize when a PDK-Key is out of range (by "watching" for signals from the RDC), and when such a condition is detected to flush (empty) the host system's "read" buffer (effectively clearing any data the system may have been cached in internal memory in order to speed data access), and display a simple message indicating the PDK-Key is in/out of range. This optional mechanism can be utilized with any RDC configuration and on any PDK-protected device.

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

CLAIMS:

1. A system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.
2. The system of claim 1, further comprising a reader/decoder circuit wherein the personal digital key is a tangible object, capable of wireless communication with the reader/decoder circuit.
3. The system of claim 2 further comprising a computer with a computer hard drive, wherein the reader/decoder circuit is located in the computer hard drive.
4. The system of claim 2 further comprising a swipe unit, wherein the reader/decoder circuit is located in the swipe unit.
5. The system of claim 1, further comprising a second personal digital key wherein the second digital key also authenticates a user attempting to access the computer readable medium.
6. The system of claim 1 wherein the personal digital key is a tangible article.
7. The system of claim 3, wherein the reader/decoder circuit is integrated with the computer.
8. The system of claim 3, wherein the computer comprises a personal digital key hard drive.
9. The system of claim 3, wherein the computer further comprises a reader/decoder circuit card.
10. The system of claim 3 wherein data from the personal digital key transfers and receives data through a secure RF port on the computer.
11. The system of claim 3 wherein the computer transmits and receives data from a provider through an Internet connection.
12. The system of claim 3, further comprising a database wherein the database includes an account identifier and a personal digital key identifier.

13. The system of claim 3 wherein data transmitted by the personal digital key to the computer is authenticated by personal digital key data stored in the database.

14. The system of claim 4 wherein the swipe unit transfers and receives data from a provider through an Internet connection.

15. The system of claim 4 wherein wherein data transmitted by the personal digital key to the reader is authenticated by personal digital key data stored in the database.

16. A method for securing computer readable media from unauthorized access, comprising:

Providing a tangible, personal digital key to a user, wherein the personal digital key is stores information unique to the user; and,

Authenticating the user if the information relayed from the personal digital key matches identification data separately provided.

17. The method of claim 16, wherein the identification data is data from a credit card.

18. The method of claim 16 wherein the personal digital key transmits the unique information through a wireless link.

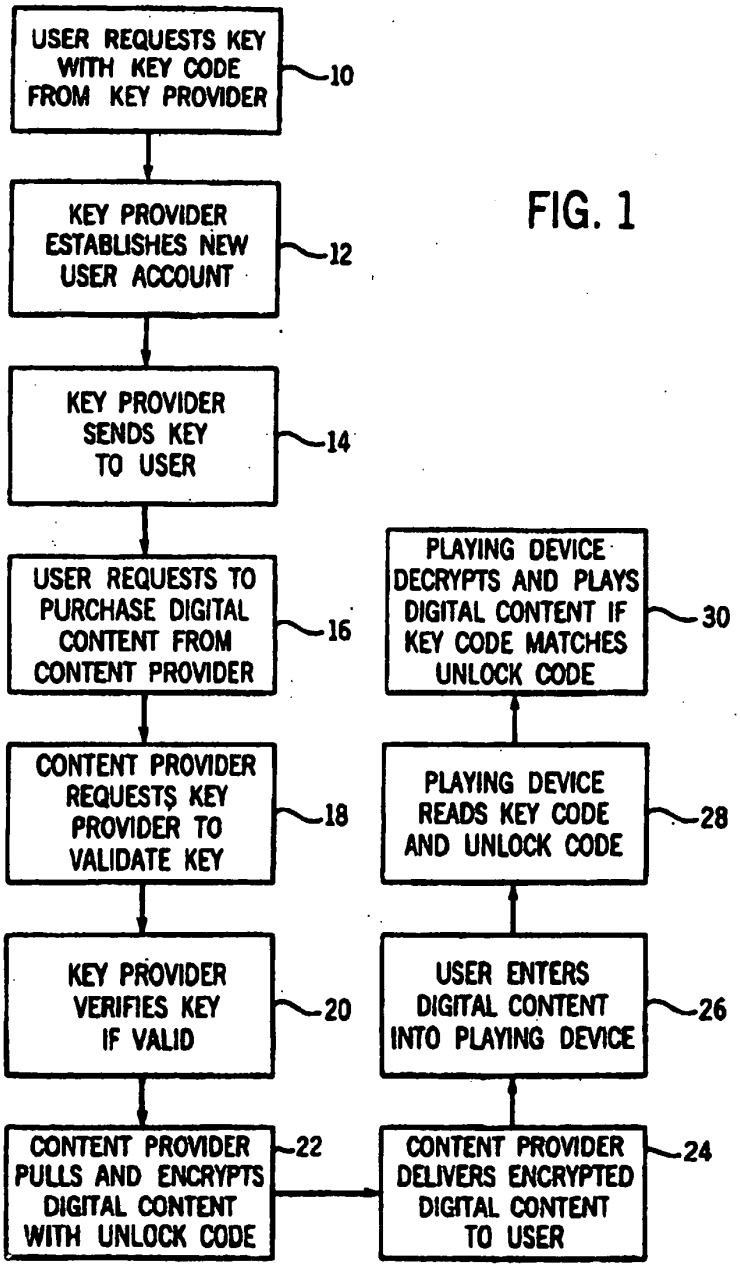

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT PROVIDER PULLS AND ENCRYPTS DIGITAL CONTENT WITH UNLOCK CODE
22
CONTENT PROVIDER DELIVERS ENCRYPTED DIGITAL CONTENT TO USER
24
USER ENTERS DIGITAL CONTENT INTO PLAYING DEVICE
26
PLAYING DEVICE READS KEY CODE AND UNLOCK CODE
28
PLAYING DEVICE DECRYPTS AND PLAYS DIGITAL CONTENT IF KEY CODE MATCHES UNLOCK CODE
30

FIG. 1

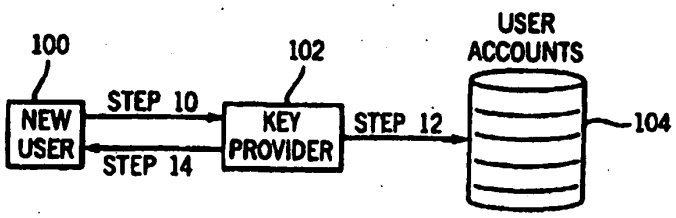


FIG. 2

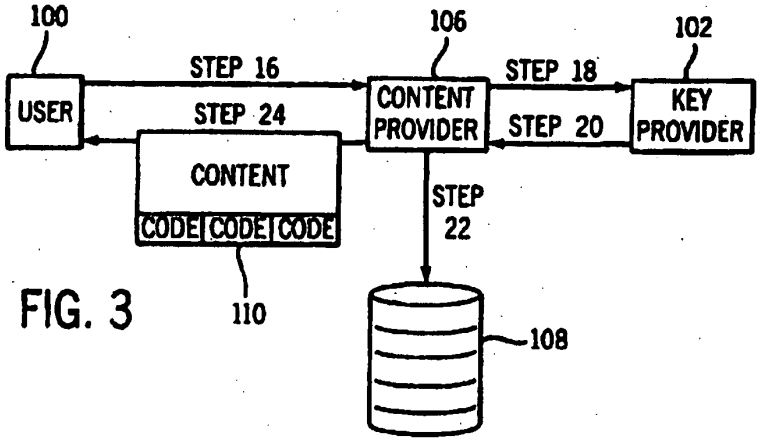


FIG. 3

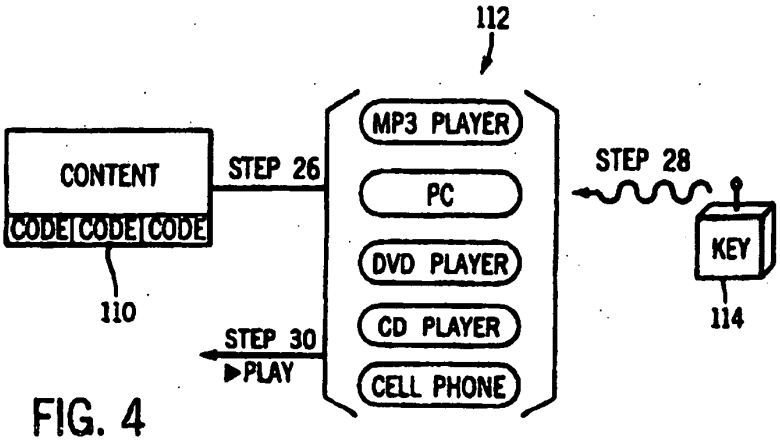


FIG. 4

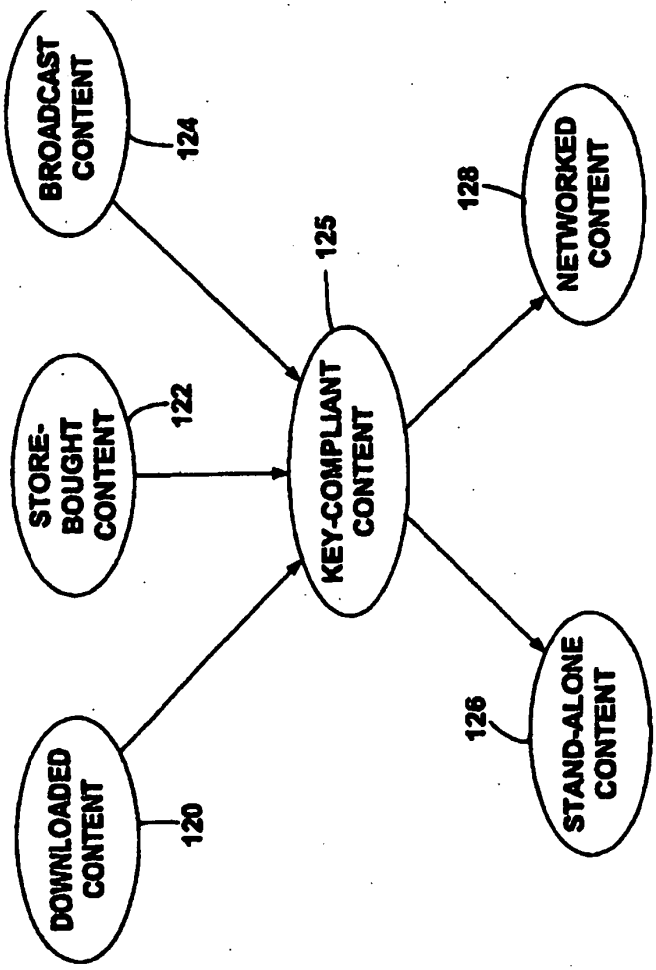

BROADCAST CONTENT
124
STORE-BOUGHT CONTENT
122
DOWNLOADED CONTENT
120
KEY-COMPLIANT CONTENT
125
NETWORKED CONTENT
128
STAND-ALONE CONTENT
126

FIG. 5

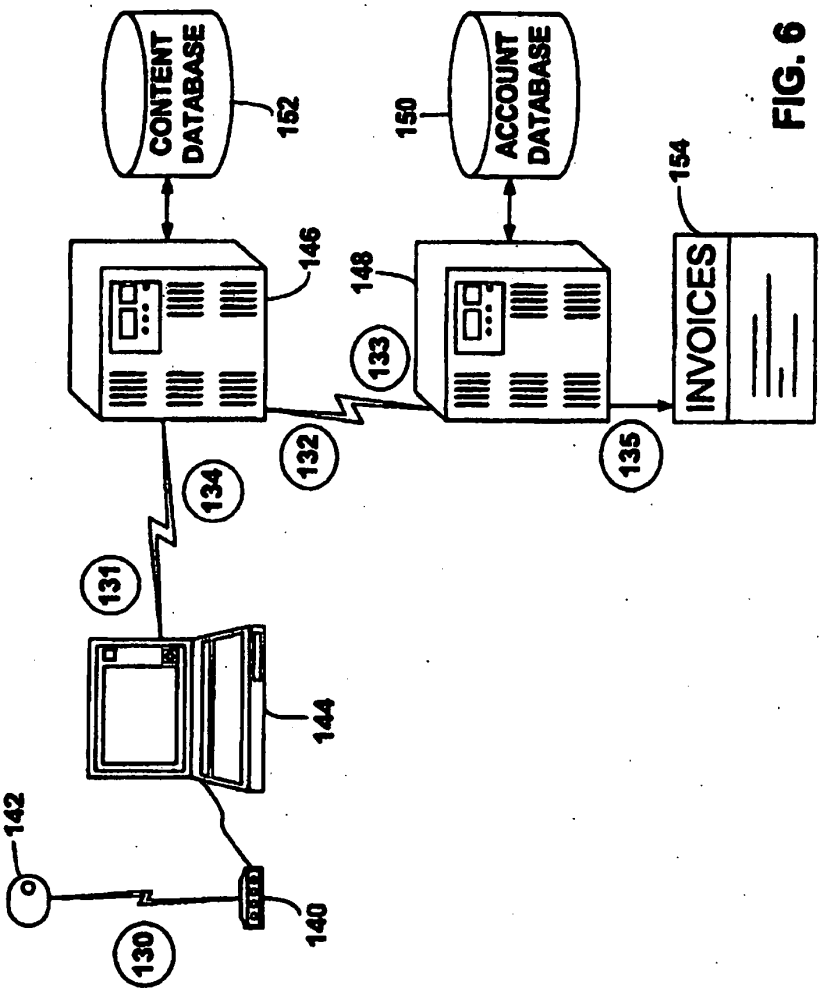

CONTENT DATABASE
152
ACCOUNT DATABASE
150
154
INVOICES
146
148
133
132
134
135
131
144
142
140
130

FIG. 6

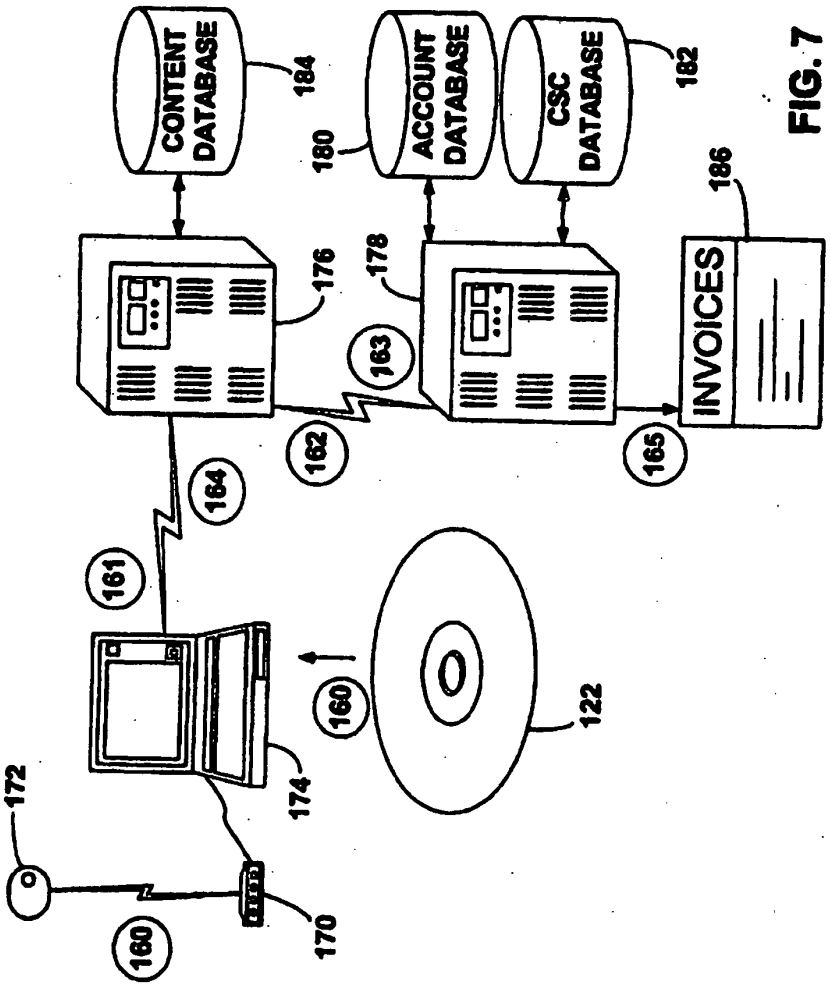

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
186
INVOICES
176
178
163
162
165
164
161
160
122
174
172
160
170

FIG. 7

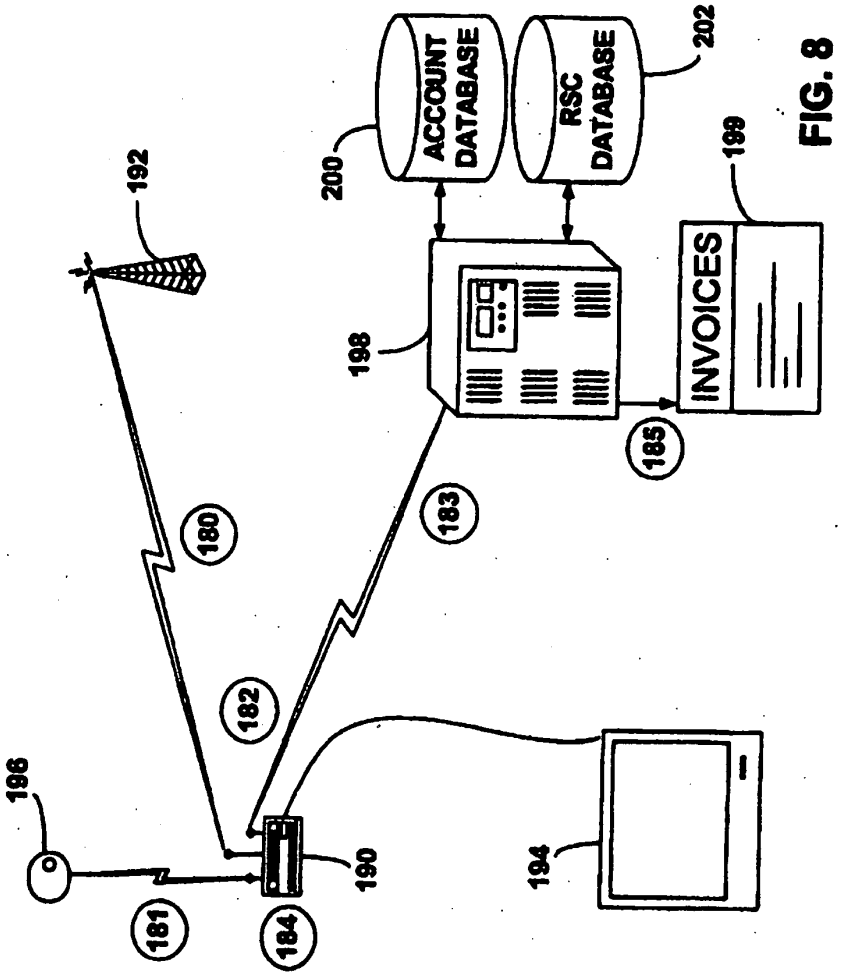

ACCOUNT DATABASE
RSC DATABASE
INVOICES
200
202
199
198
192
180
183
182
185
196
190
194
181
184

FIG. 8

FIG. 9a

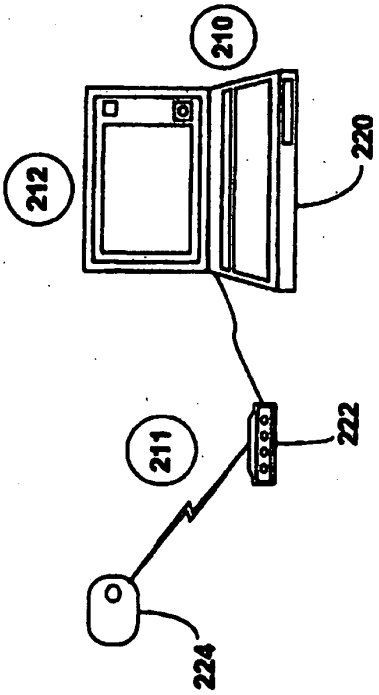
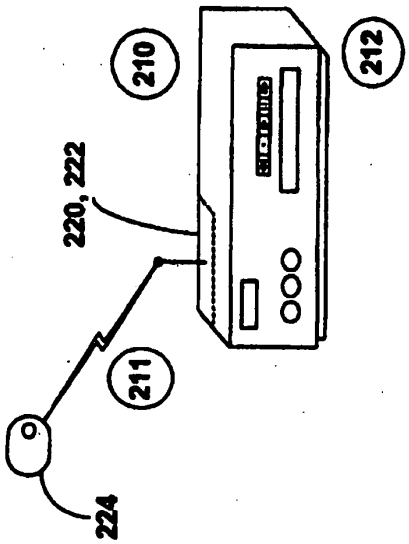


FIG. 9b



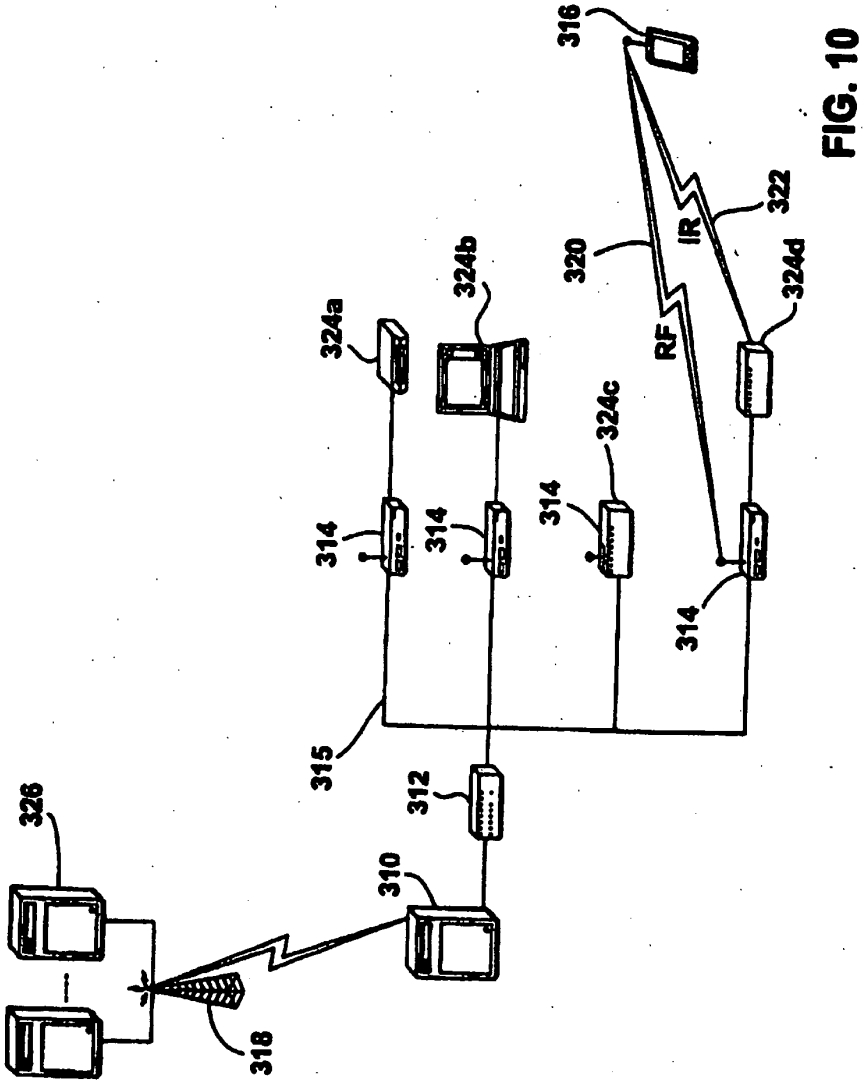

316
320
IR
322
RF
324d
324a
324b
324c
314
314
314
314
315
312
310
326
318

FIG. 10

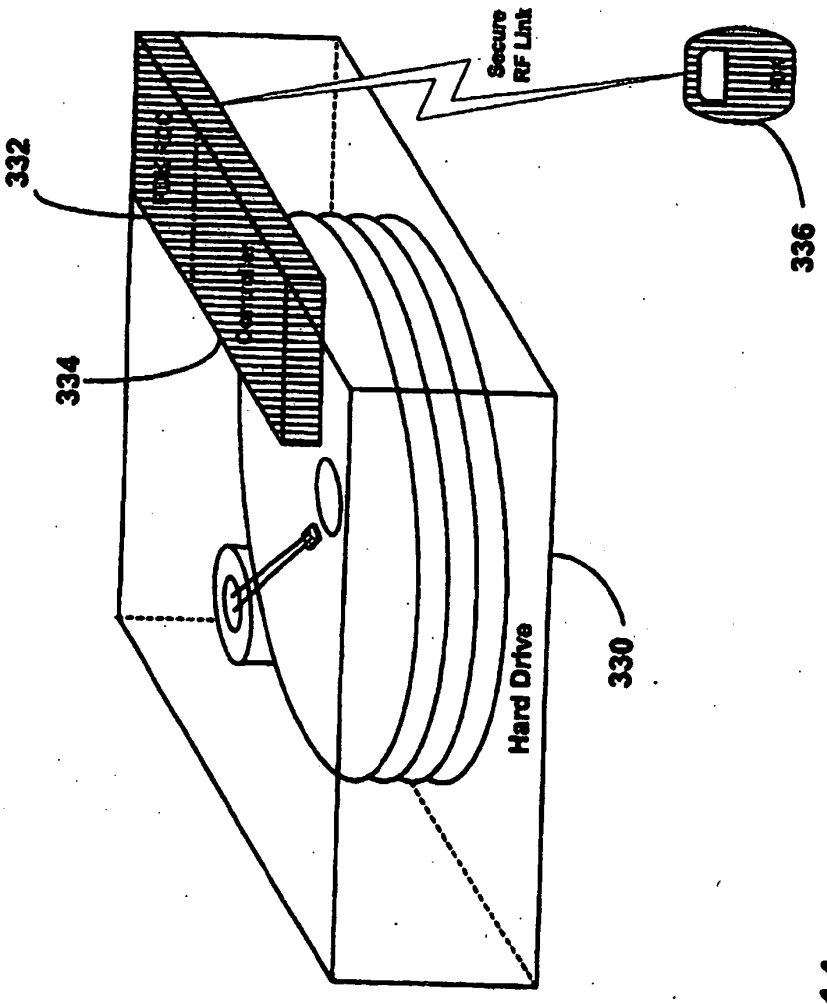


FIG. 11

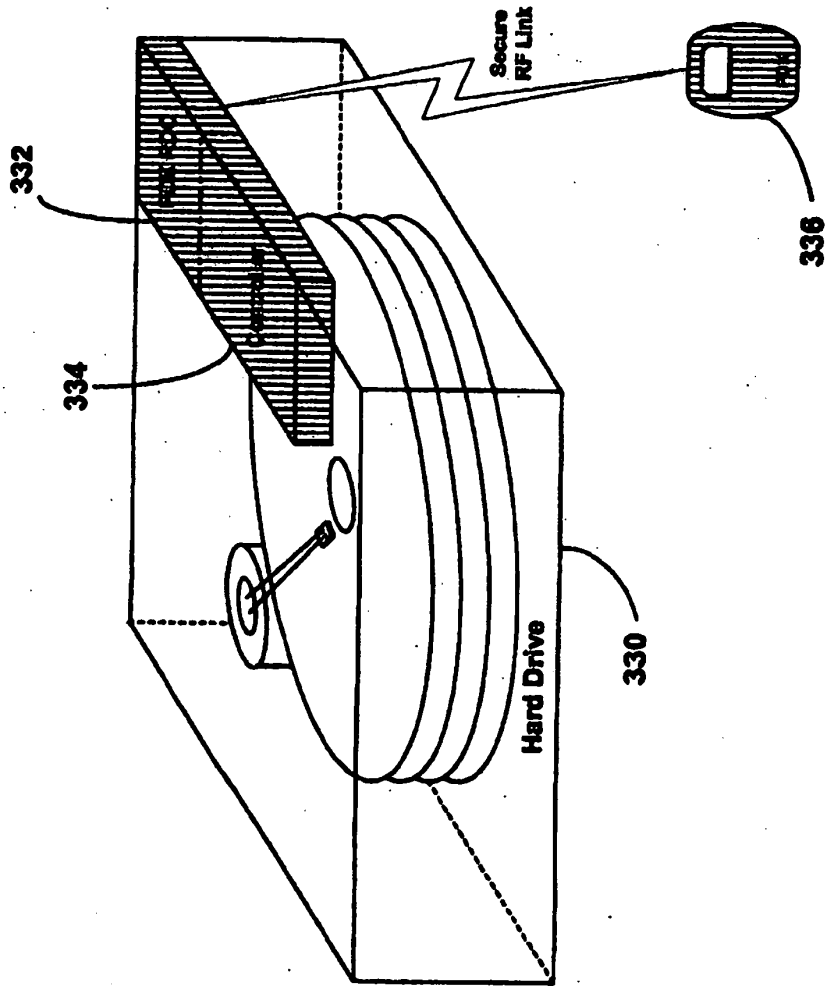


FIG. 12

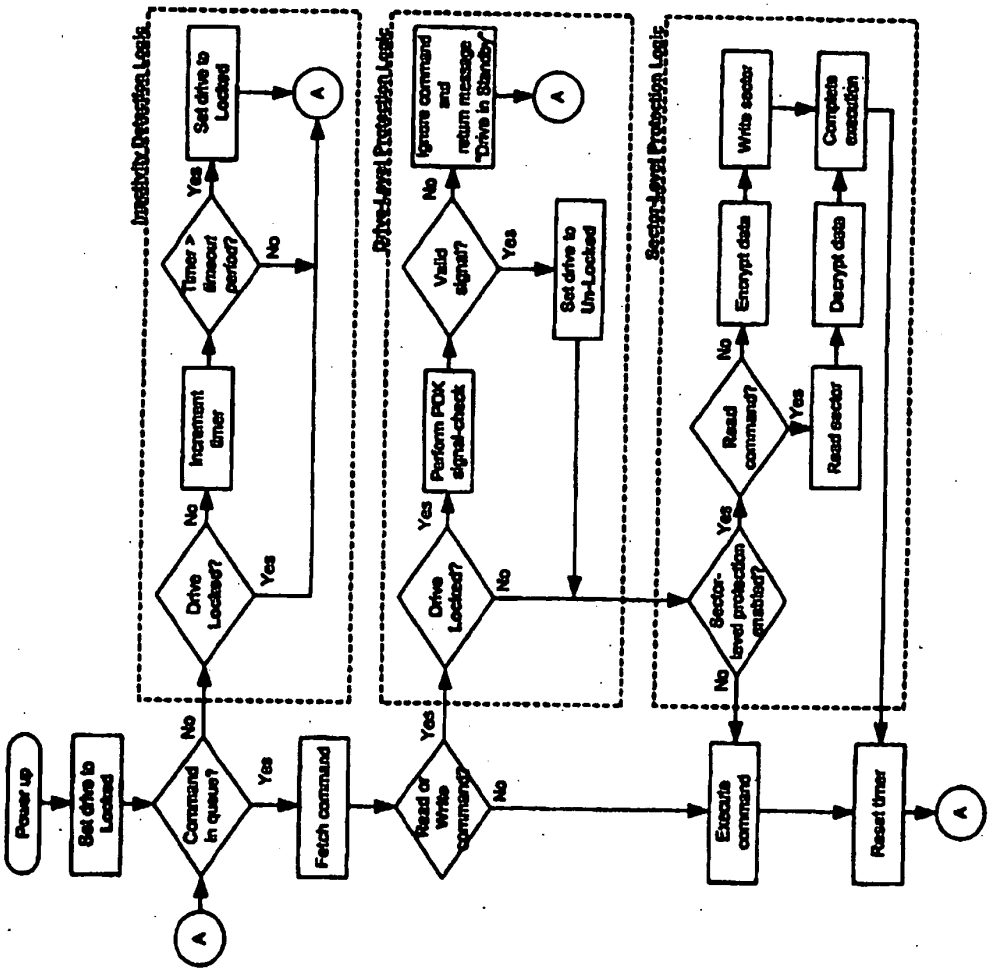

Power up
Set drive to Locked
Command in queue?
No
Yes
Fetch command
Read or Write command?
Yes
No
Inactivity Protection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
Drive-Level Protection Logic
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
Set drive to Un-Locked
Sector-Level Protection Logic
Sector-level protection enabled?
Yes
No
Read command?
No
Yes
Encrypt data
Read sector
Decrypt data
Write sector
Complete execution
Execute command
Reset timer
A

FIG. 13

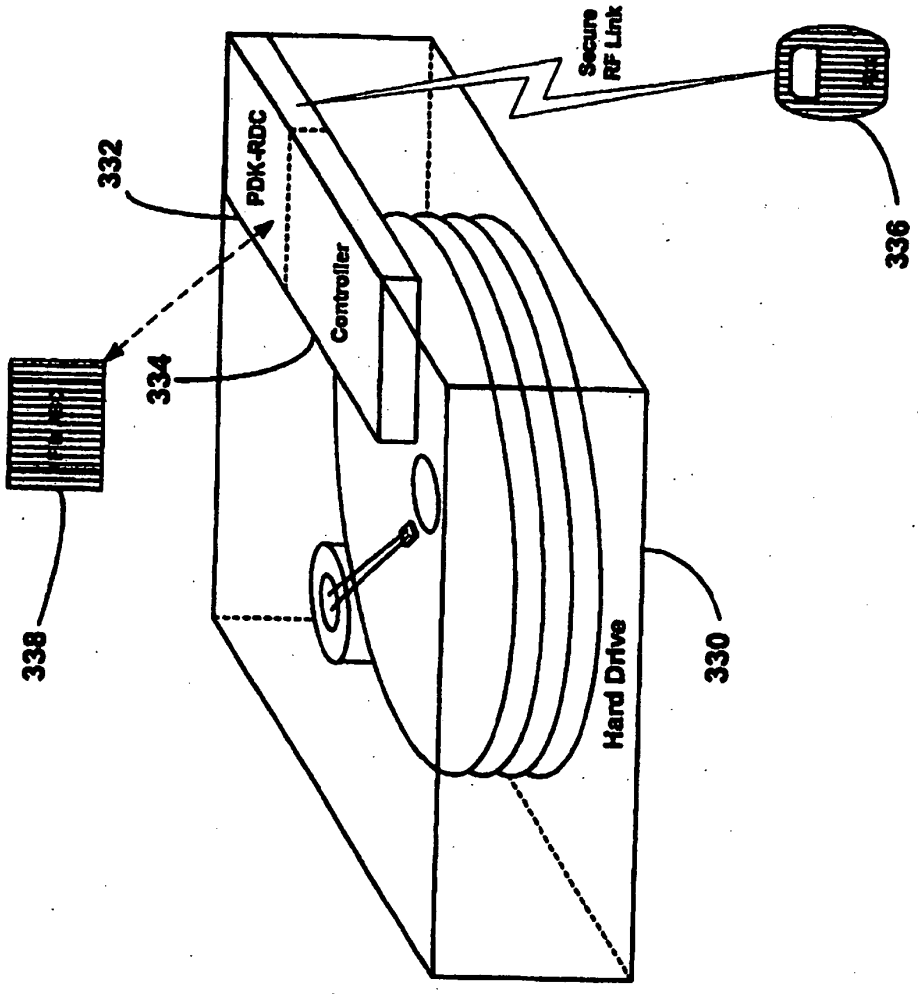

Secure RF Link
PDK-RDC
332
Controller
334
336
338
330
Hard Drive

FIG. 14

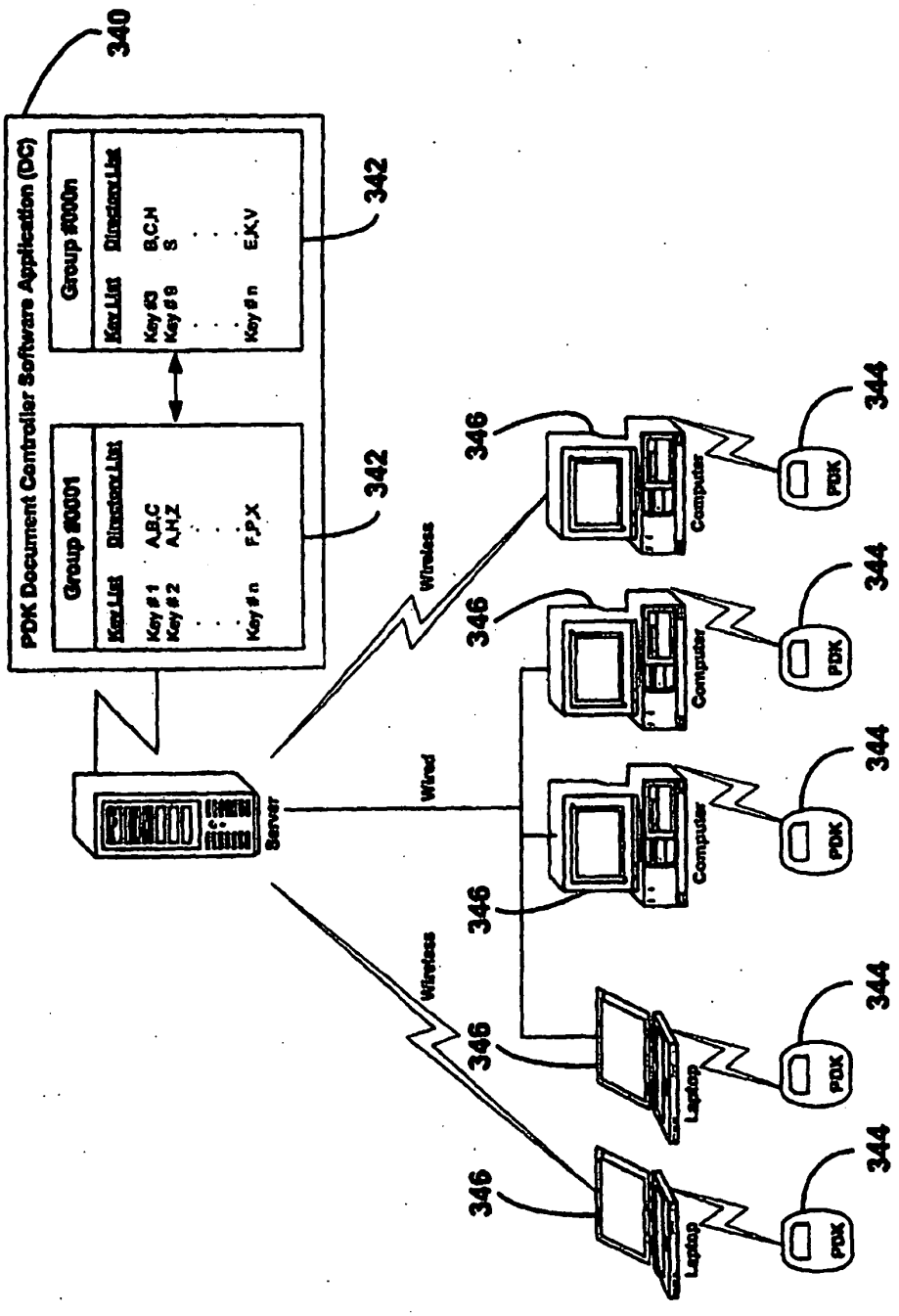

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key #1
Key #2
Key #n
A,B,C
A,H,Z
F,P,X
Group #000n
Key #3
Key #8
Key #n
B,C,H
S
E,K,V
342
342
Server
Wired
Wireless
Wireless
346
346
346
346
346
Computer
Computer
Computer
Laptop
Laptop
PDK
PDK
PDK
PDK
PDK
344
344
344
344
344

FIG. 15

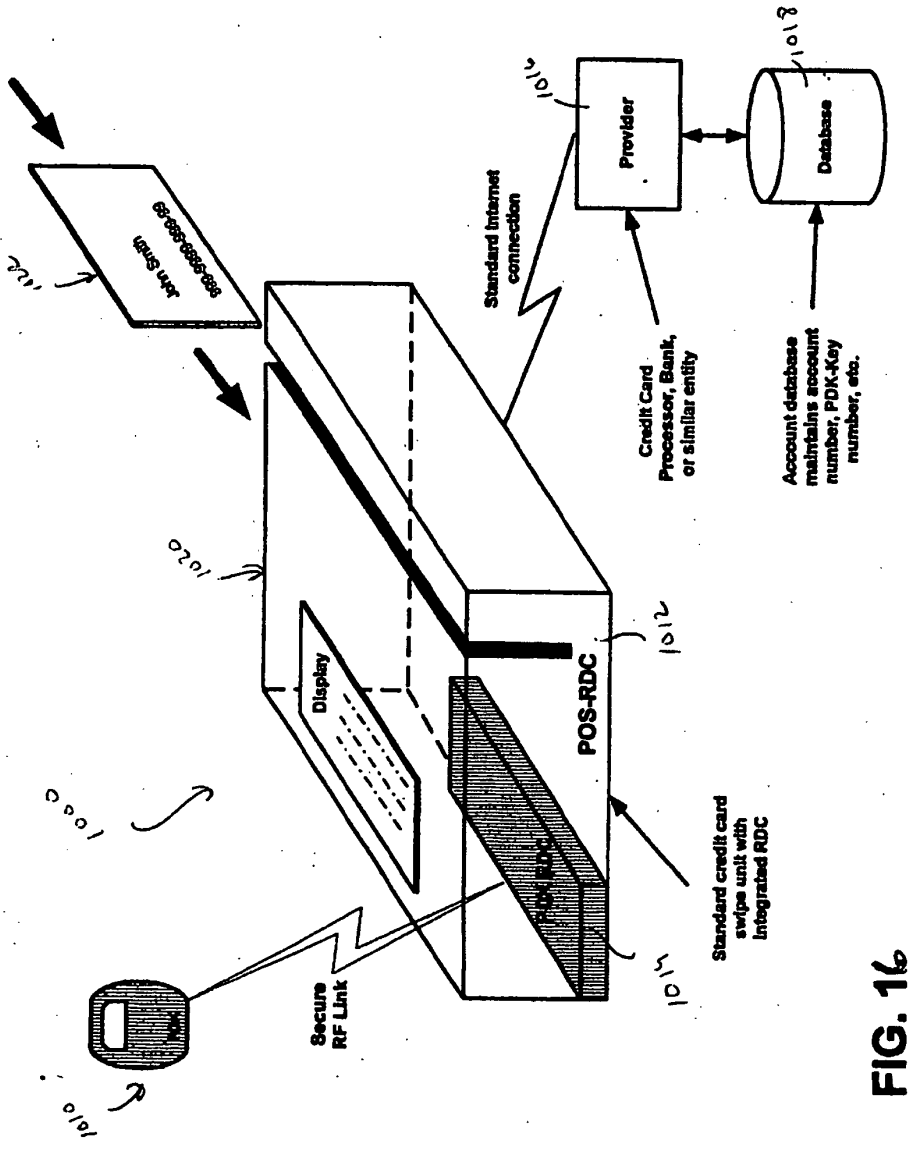

Provider
Database
Standard Internet connection
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
POS-RDC
Display
Standard credit card swipe unit with integrated RDC
Secure RF Link

FIG. 16

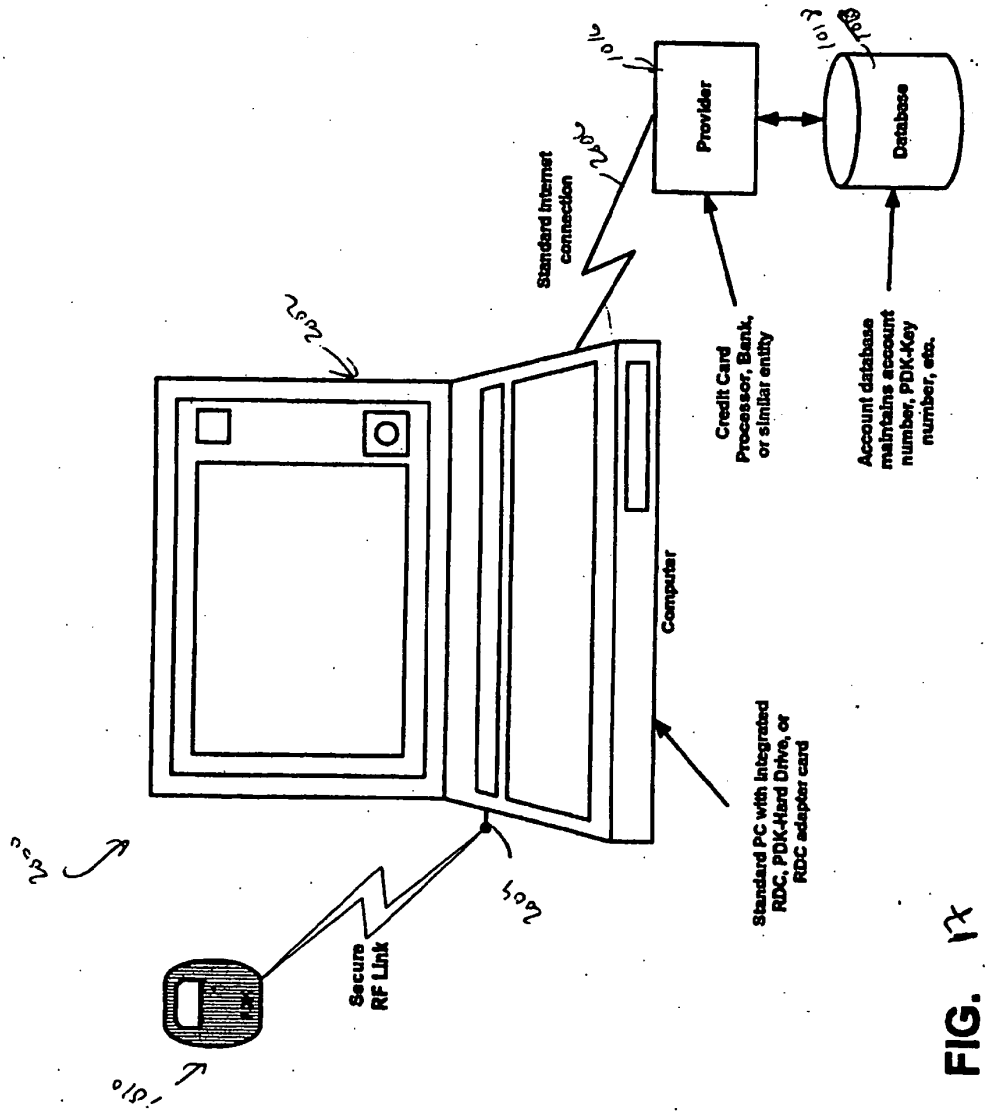

Provider
Database
Standard Internet connection
Credit Card Processor, Bank, or similar entity
Account database maintains account number, PDK-Key number, etc.
Computer
Standard PC with integrated RDC, PDK-Hard Drive, or RDC adapter card
Secure RF Link

FIG. 17

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086802 A3

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number:
PCT/US2005/007535

(22) International Filing Date: 8 March 2005 (08.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/551,320 8 March 2004 (08.03.2004) US

(71) Applicant *(for all designated States except US)*: MARGENT DEVELOPMENT, LLC [US/US]; 391 Taylor Boulevard, Suite 105, Pleasant Hill, California 94523 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: GIOBBI, John, J. [US/US]; 689 NW Stonepine Drive, Bend, Oregon 97701 (US).

(74) Agents: STEFFEY, Charles, E. et al.; P.O. Box 2938, Minneapolis, MN 55402 (US).

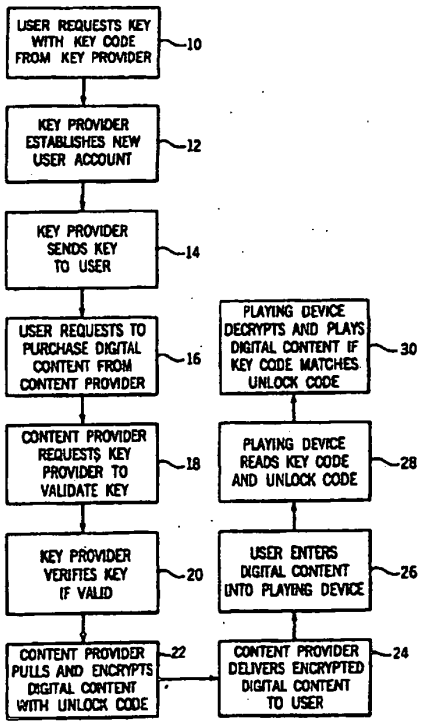
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: LINKED ACCOUNT SYSTEM USING PERSONAL DIGITAL KEY (PDK-LAS)



(57) Abstract: One embodiment of the invention includes a system comprising: a personal digital key and a computer readable medium that is accessible when authenticated by the personal digital key.

WO 2005/086802 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
26 January 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/07535

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 17/60
US CL : 705/51
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/51

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20020124251 A1 (Hunter ET AL.) 05 September 2002 (05.09.2002) PARAGRAPHS 0001-0017 AND 0014	1-18
X	US 20030079133 A1 (Breiter ET AL.) 24 April 2003 (24.04.2003) PARAGRAPHS 0018 AND 0025.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 October 2005 (07.10.2005)	06 DEC 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer James Trammel Telephone No. 571-272-3600

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

Electronic Acknowledgement Receipt

EFS ID:	20871295
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	04-DEC-2014
Filing Date:	03-FEB-2014
Time Stamp:	18:29:39
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	Information Disclosure Statement (IDS) Form (SB08)	04293US_IDS.pdf	618341 cc5f17c7d0d2bc1760d55b2a0e50d681b8b5e0a1	no	17

Warnings:	
Information:	

2	Non Patent Literature	01_AllianceActivities.pdf	304028 8177e408e7bc50cfd4f58a5e606985278542fe68	no	7
Warnings:					
Information:					
3	Non Patent Literature	02_AntonoffMichael_VisitingVideoValley.pdf	321867 d468437ccdca2ae67019190963a93705ed4745e9	no	3
Warnings:					
Information:					
4	Non Patent Literature	03_ApplyingBiometricstoDoorAccess.pdf	342271 86145913cdba4173881a012e24bc69fae6c17728	no	5
Warnings:					
Information:					
5	Non Patent Literature	04_IntheAgeofNapster.pdf	102749 e56cb481660b56064bc95a136366153ad503ec14	no	2
Warnings:					
Information:					
6	Non Patent Literature	05_SoundWavesCouldHelp.pdf	102181 a3edd87ac48cdba90d0cd332fed25dafcc4bc40c	no	2
Warnings:					
Information:					
7	Non Patent Literature	06_BlumJonathan_DigitalRightsManagementMaySolvetheNapsterProblem.pdf	422052 9a552ad310e7fe5bd0e031334cbb3612cbac092b	no	4
Warnings:					
Information:					
8	Non Patent Literature	07_BROWN_TechniquesForPrivacy.pdf	1466779 e9994101cf772158a26be562b13cdc9bc9278598	no	5
Warnings:					
Information:					
9	Non Patent Literature	08_TheSmart.pdf	930650 c392ba70c4c999149f893387a9721773f71bb2c9	no	28
Warnings:					
Information:					
10	Non Patent Literature	09_Debow_CreditDebitDebutsinMidwestSmart.pdf	325765 27547efd2278caf9a2bc4796ff59620fd4b081f9	no	4
Warnings:					
Information:					

11	Non Patent Literature	10_Dennis_DigitalPassportsNeedNotInfringe.pdf	76969 9072b2042616d55337f839b05dcfc5ef5f8a32fa	no	2
Warnings:					
Information:					
12	Non Patent Literature	11_FascaChad_TheCircuit.pdf	133830 252d5ba5ce53f3bd680e6e3659a9fd45f9f3fb2f	no	2
Warnings:					
Information:					
13	Non Patent Literature	12_FirecrestShowsHowTrulyCommerciallyMindedCompanies.pdf	168250 54dccaa012e9574d487be6b5233c23c8563b0e1e	no	2
Warnings:					
Information:					
14	Non Patent Literature	13_FrequentlyAskedQuestions.pdf	227406 df1a84bfda1659a5ea18e736ebfc0d4ede7d3c1f	no	5
Warnings:					
Information:					
15	Non Patent Literature	14_NEL_GenerationOfKeys.pdf	910233 fd11cdf8990a8f29081f2758c263fa7c7551e124	no	6
Warnings:					
Information:					
16	Non Patent Literature	15_IEEE.pdf	97287 0713cdbf1495c47af4001ee94d95f3cca29c4868	no	6
Warnings:					
Information:					
17	Non Patent Literature	16_LakeMatt_DowloadingforDollars.pdf	439792 41d6d0568f2756a249222fba44f3452021722e4f9	no	2
Warnings:					
Information:					
18	Non Patent Literature	17_LewisSonyandVisainOnlLineEntertainmentVenture.pdf	35032 467d10cb2972f6f5e19968b24dd2cefc7d36914b	no	1
Warnings:					
Information:					
19	Non Patent Literature	18_McIverR_IdentificationandVertificationWorkingTogether.pdf	342440 c9bbfbae7afcd1475d7b611464e3d9c5752481f5	no	5
Warnings:					
Information:					

20	Non Patent Literature	19_NilssonJ_MatchOnCardforJavaCards.pdf	1006923 d895840b045befbf77ecc561705acb7a215ce732	no	5
Warnings:					
Information:					
21	Non Patent Literature	20_NordinB_MatchOnCardTechnology.pdf	1526333 bad204fc95c13dbcb231c0a3af5eadfda0ba9e57	no	7
Warnings:					
Information:					
22	Non Patent Literature	21_PCTInternationalSearchReport20050407.pdf	966474 f564a7ef2a1c01722018277aa56303401e2f95c6	no	10
Warnings:					
Information:					
23	Non Patent Literature	22_PagetPaul_TheSecurityBehindSecureExtranets.pdf	320208 cf247e0a2a6b98c532eafdb0fa33f9de43f006ec	no	4
Warnings:					
Information:					
24	Non Patent Literature	23_PCTInternationalSearchReport20081020.pdf	345605 e083fca5e3d8644e13aee0d2d9ab6f31d1219e76	no	9
Warnings:					
Information:					
25	Non Patent Literature	24_PCTInternationalSearchReport20080423.pdf	364630 7c98850642ad25e496c1e829d0e144c51ee65551	no	8
Warnings:					
Information:					
26	Non Patent Literature	25_PCTInternationalSearchReport20070222.pdf	337655 52f09459ee4d5e714d550f17d7b16e000b214dec	no	7
Warnings:					
Information:					
27	Non Patent Literature	26_PCTInternationalSearchReport20080301.pdf	534409 12f3a065680566e7d293bc00e93e84ffab58104f	no	10
Warnings:					
Information:					
28	Non Patent Literature	27_PCTInternationalSearchReport20080319.pdf	604465 68279e306d4f4e5735bfda98faaa1b464a2665d0	no	10
Warnings:					
Information:					

29	Non Patent Literature	28_PersonalServersasDigitalKeys.pdf	809801 330ecb78f4dc8a3202248ce62b26b0fab262222b	no	10
Warnings:					
Information:					
30	Non Patent Literature	29_MicronasandThomsonMultimedia.pdf	172940 bf91a390b2cffedb3fed5d49a4dca0490814b1ad	no	3
Warnings:					
Information:					
31	Non Patent Literature	30_ContentProtectionPlanTargetsWireless.pdf	135274 506e32867b74e96919ef8d34ff7aea4d7c8f7d19	no	2
Warnings:					
Information:					
32	Non Patent Literature	31_ThompsonBetsonSmartCardsforVideoEncryption.pdf	57796 c6fec17f2b79f202b6633ad0d8afa1a1a779a244	no	1
Warnings:					
Information:					
33	Non Patent Literature	32_PressRelease_ThompsonMultimediaUnveilsCopyProtectionProposal.pdf	141389 c0742e55a04d2cd630fa5d68d912c8ce2c7ab037	no	2
Warnings:					
Information:					
34	Non Patent Literature	33_SAFModule_ALookIntoStrongAuthentication.pdf	400643 5083da5c1cfb896e161aaae5c49ca2f64e3a83e1	no	8
Warnings:					
Information:					
35	Non Patent Literature	34_SapsfordJathon_E-Business.pdf	102181 4e728a53b2af2adecf3269201b2385afbee52acb	no	2
Warnings:					
Information:					
36	Non Patent Literature	35_SayHellotoBluetooth.pdf	94764 84d35e9bc5058e64a43dfe1f2e2af254c73a1f93	no	5
Warnings:					
Information:					
37	Non Patent Literature	36_SmartCardsandBiometricsWhitePaper.pdf	304028 92aeec4629323d8e95ff38bd7e492665156e6192	no	7
Warnings:					
Information:					

38	Non Patent Literature	37_VanWindle_BluetooththeKingofConnectivity.pdf	803265 6bedb21f619f9cab859789e6fd9569f239a6c21a	no	6
Warnings:					
Information:					
39	Non Patent Literature	38_Wade_Using_FingerprintstoMakePaymentsatPOSSlowlyGainingPopularity.pdf	176486 699e1b3a1605244cdf0d883b722f1a30fe7efa59	no	3
Warnings:					
Information:					
40	Non Patent Literature	39_WallaceBob_TheInternetUnplugged.pdf	351892 aadb291b3759e069d3c28d9d9fee0bdea688c503	no	5
Warnings:					
Information:					
41	Non Patent Literature	40_WeberThomasE_IntheAgeofNapster.pdf	102749 2b71f65d6ed85b310476316e1b3ac9a6f8e90c01	no	2
Warnings:					
Information:					
42	Foreign Reference	01_WO2000062505ThomsonMultimedia.pdf	1054467 9d20f5f3614d730b7ab56aa82580764f3c76ebb7	no	27
Warnings:					
Information:					
43	Foreign Reference	02_WO2000122724ThomsonMultimedia.pdf	1255085 f7f6d54b7e19b8e3885a40b4331e93ec1561cb74	no	32
Warnings:					
Information:					
44	Foreign Reference	03_WO2000175876ThomsonMultimedia.pdf	1235470 261ed8a2cfd6fe0e1f68d4d74c58d5261a42eac2	no	28
Warnings:					
Information:					
45	Foreign Reference	04_WO2000177790ThomsonMultimedia.pdf	814723 0d53b58fca66b90d5e245936ff329e17a28437d3	no	20
Warnings:					
Information:					
46	Foreign Reference	05_WO2005050450MargentDevelopmentLLC.pdf	1792857 a898a088b199a0cec32f6ec9f97861571ed1d407	no	50
Warnings:					
Information:					

47	Foreign Reference	06_WO2005086802MargentDevelopmentLLC.pdf	2017612 c6624e237726d915a1d0fab3b4845c02b6a47d1d	no	58
Warnings:					
Information:					
48	Non Patent Literature	41_Non-FinalOfficeAction.pdf	975297 968838fe581284a95cc2ebe821d49797af9f70d8	no	12
Warnings:					
Information:					
		Total Files Size (in bytes):	26173343		

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

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

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

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

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	David L. Brown
APPLICATION NO:	14/171,705
FILING DATE:	February 3, 2014
TITLE:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
EXAMINER:	Jason T. Lee
GROUP ART UNIT:	2438
ATTY. DKT. NO:	10001-04293 US
CONFIRMATION NO:	7167

CERTIFICATE OF EFS-WEB TRANSMISSION

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

Dated: December 22, 2014 By: /Matthew Holmes/

Matthew Holmes, Reg. No. 65,160

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

AMENDMENT A

Responsive to the Non-Final Office Action mailed on September 22, 2014, which sets a shortened statutory period for response that expires on December 22, 2014, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Canceled)

2. (New) A hybrid device comprising:

an integrated personal digital key (PDK) for storing local, secured information and capable of communicating wirelessly with an external receiver-decoder circuit (RDC); and

an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.

3. (New) The hybrid device of claim 2, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.

4. (New) The hybrid device of claim 2, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.

5. (New) The hybrid device of claim 2, wherein the local, secured information includes biometric information for authenticating a user.

6. (New) The hybrid device of claim 2, wherein the local, secured information includes financial information.

7. (New) The hybrid device of claim 2, wherein the local, secured information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.

8. (New) The hybrid device of claim 2, wherein the hybrid device is a cell phone.

9. (New) The hybrid device of claim 2, wherein the external PDK is included in jewelry.

10. (New) The hybrid device of claim 2, comprising storage for inheritance information.

11. (New) A method comprising:

creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC, wherein the integrated PDK stores local, secured information;

receiving a first signal at the integrated RDC via the first wireless link from the external PDK;

generating an enablement signal enabling one or more of an application, a function and a service.

12. (New) The method of claim 11 comprising:

sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.

13. (New) The method of claim 11 comprising:

sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.

14. (New) The method of claim 11, wherein the local, secured information includes biometric information for authenticating a user.

15. (New) The method of claim 11, wherein the local, secured information includes financial information.

16. (New) The method of claim 11, wherein the hybrid device is a cell phone.

17. (New) The method of claim 11, wherein the external PDK is included in jewelry.

18. (New) The method of claim 11, wherein the local secured information includes biometric information for authenticating a user.

19. (New) The method of claim 11, wherein the local secured information includes financial information.

20. (New) The method of claim 11, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method comprises:

creating a second wireless link between the integrated PDK and an external RDC; and

sending the enablement signal from the integrated PDK to the external RDC using the second wireless link, the enablement signal based on financial information included in the local, secured information stored on the integrated PDK and used to complete a financial transaction.

21. (New) The method of claim 11, wherein the first signal includes inheritance information.

APPLE Ex. 1002, Page 421

REMARKS

Claims 1 was presented for examination. Claims 1 stands rejected in the Office Action dated September 22, 2014 (herein, "OA"). Claim 1 is canceled. Claims 2-21 are new. Support for the new claims is found throughout the Applicant's specification. Claims 2-21 are pending upon entry of this amendment.

Summary of Office Action

1. Claim 1 is rejected on the ground of non-statutory double patenting as being allegedly unpatentable over Claim 1 of U.S. Patent No. 8,171,528.

2. Claim 1 is rejected under 35 U.S.C. § 103 as being allegedly unpatentable over Finn et al. (U.S. Publication No. 2006/0208066, hereinafter "Finn") in view of Hochstein et al. (U.S. Publication No. 2006/0113381, hereinafter "Hochstein").

These rejections are traversed herein.

Response to Double Patenting Rejection

Claim 1 is rejected on the ground of non-statutory double patenting as being allegedly unpatentable over Claim 1 of U.S. Patent No. 8,171,528. Claim 1 is canceled. Accordingly, the Examiner's non-statutory double patenting rejection is moot, no terminal disclaimer is submitted herewith and withdrawal of the rejection is respectfully requested.

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

Claim 1 is rejected under 35 U.S.C. § 103 as being unpatentable over Finn in view of Hochstein. Claim 1 is canceled. Accordingly, the Examiner's non-statutory double patenting rejection is moot and withdrawal of the rejection is respectfully requested. Additionally, the references cited by the Examiner fail to disclose or suggest each and every element of new claims 2-21 nor does the Examiner argue such.

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,
DAVID L. BROWN

Dated: December 22, 2014 By: /Matthew Holmes/

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

MMH:cji

Electronic Acknowledgement Receipt

EFS ID:	21034219
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	22-DEC-2014
Filing Date:	03-FEB-2014
Time Stamp:	19:15:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		04293US_AmendmentA.pdf	86254 57f0f49befd1989a4213291f983128d1193ef243	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	7
Warnings:			
Information:			
	Total Files Size (in bytes):	86254	

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

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

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

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/171,705	Filing Date 02/03/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT	12/22/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

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

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

LIE
/MONICA FRANCIS/

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/171,705	Filing Date 02/03/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT 12/22/2014

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

AMENDMENT

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

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

LIE
/MONICA FRANCIS/

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.

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

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14171705
Filing Date	03-Feb-2014
First Named Inventor	David Brown
Attorney Docket Number	10001-04293 US
Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

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

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

Owner	Percent Interest
Proxense, LLC	100%

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

8171528

8646042

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

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14171705
Filing Date:	03-Feb-2014
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Filer:	Matthew M. Holmes
Attorney Docket Number:	10001-04293 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

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

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

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

Application No.: 14171705

Filing Date: 03-Feb-2014

Applicant/Patent under Reexamination: Brown et al.

Electronic Terminal Disclaimer filed on January 8, 2015

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

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

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	21162675
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Matthew M. Holmes
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	08-JAN-2015
Filing Date:	03-FEB-2014
Time Stamp:	20:31:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$160
RAM confirmation Number	8576
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33483 17c831f06ee23233626ac21fc640ab98f2651cec	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30484 fcbd21f9eef61a0700b0b0bda1b591cfa652f993	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	63967		

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

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

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

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

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/171,705	Filing Date 02/03/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

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

APPLICATION AS AMENDED – PART II

AMENDMENT	12/22/2014	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT	01/24/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

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

LIE
/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.

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 01/28/2015

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

EXAMINER
LEE, JASON T

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/28/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	02/03/2014	David L. Brown	10001-04293 US	7167

TITLE OF INVENTION: HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/28/2015

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

89194 7590 01/28/2015
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

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

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	02/03/2014	David L. Brown	10001-04293 US	7167

TITLE OF INVENTION: HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/28/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, JASON T	2438	726-003000

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

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

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

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

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

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

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

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

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	02/03/2014	David L. Brown	10001-04293 US	7167

89194 7590 01/28/2015

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

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 01/28/2015

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

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

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

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

PTOL-85 (Rev. 02/11)

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 14/171,705	Applicant(s) BROWN, DAVID L.	
	Examiner JASON LEE	Art Unit 2438	AIA (First Inventor to File) Status No

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

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

1. ☒ This communication is responsive to *12/22/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *2-17 and 20-23* . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

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

   * Certified copies not received: _____.

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

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

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

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 12/4/2014
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *1/9/2015* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON LEE/
Primary Examiner, Art Unit 2438

DETAILED ACTION

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Applicant filed the response on December 22, 2014 for the office action dated September 22, 2014. Claim 1 is cancelled. Claims 2-21 are added. As the result of Examiner's amendment in the instant office action, Claims 2, 5-7, 10-15 and 20 are amended. Claims 22 and 23 are added. Claims 18 and 19 are cancelled. Claims 2-17 and 20-23 are re-numbered as 1-20 are pending.

Terminal Disclaimer

4. The terminal disclaimer filed on 1/8/2015 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S patent 8,171,528 B1 and US patent No. 8, 646,042 B1 has been reviewed and is approved on 1/8/2015. The terminal disclaimer has been recorded.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/04/2014 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Response to Arguments

6. Applicant's filed Terminal disclaimer on 1/8/2015 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S patent 8,171,528 B1 and US patent No. 8, 646,042 B1 and is approved on 1/8/2015. Therefore, double patenting rejections for the previous office action have been withdrawn.

EXAMINER'S AMENDMENT

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

Authorization for this examiner's amendment was given in a telephone interview with Mr. Matthew Holmes (Registration No. 65,160) on 01/09/2015.

The application has been amended as follows:

1. (Canceled)

2. (Currently Amended) A hybrid device comprising:

an integrated personal digital key (PDK) for storing local, secured <u>biometric</u> information <u>for authenticating a user</u> and capable of communicating wirelessly with an external receiver-decoder circuit (RDC); and

an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service.

5. Currently Amended) The hybrid device of claim 2, wherein the local, secured ~~information includes~~ biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.

6. (Currently Amended) The hybrid device of claim 2, wherein the integrated PDK stores local, secured ~~information includes~~ financial information.

7. (Currently Amended) The hybrid device of claim 2, wherein the integrated PDK stores local, secured ~~information includes~~ financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.

10. (Currently Amended) The hybrid device of claim 2, comprising a storage for inheritance information.

11. (Currently Amended) A method comprising:

creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external personal digital key (PDK), the hybrid device including an integrated PDK and the integrated RDC, wherein the integrated PDK stores local, secured biometric information for authenticating a user;

receiving a first signal at the integrated RDC via the first wireless link from the external PDK;

generating an enablement signal enabling one or more of an application, a function and a service.

12. (Currently Amended) The method of claim 11 further comprising:

sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on the hybrid device.

13. (Currently Amended) The method of claim 11 further comprising:

sending the enablement signal to the hybrid device, wherein at least one of the one or more of the application, the function, and the service are enabled at least in part on a device external to the hybrid device and communicatively coupled to the external RDC.

14. (Currently Amended) The method of claim 11, wherein the local, secured ~~information includes~~ biometric information for authenticating a user is based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a photograph, a signature, a voice sample, DNA and RNA.

15. (Currently Amended) The method of claim 11, wherein the integrated PDK stores local, secured ~~information includes~~ financial information.

18. (Canceled)

19. (Canceled)

20. (Currently Amended) The method of claim 11, wherein the integrated PDK is electrically coupled to the integrated RDC, and the method further comprises:

creating a second wireless link between the integrated PDK and an external RDC; and

sending the enablement signal from the integrated PDK to the external RDC using the second wireless link, the enablement signal based on financial information ~~included in the local, secured information~~ stored locally and securely on the integrated PDK and used to complete a financial transaction.

22. (New) The method of claim 11, wherein the external PDK is included in a watch.

23. (New) The hybrid device of claim 2, wherein the external PDK is included in a watch.

Allowable Subject Matter

8. Newly amended independent claims 2 and 11 are allowed over prior art of record. Dependent claims 3-10, 23 and 12-17, 20-22 depend on the above-mentioned independent claims 2 and 11 are allowed by virtue of its dependency.

Examiner's statement of reasons for allowance

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

Newly amended independent claim 2 is allowed in view of the (examiner's) amendment and terminal disclaimer filed 1/8/2015 and telephone interview on 01/09/2015.

Prior art of record, Finn et al (US 2006/0208066 A1), in view of Hochstein et al (US 2006/0113381 A1) fails to teach alone, or in combination, at the time of the invention, the claimed features and limitations. None of the prior art of record teaches or made obvious the feature: "an integrated personal digital key (PDK) for storing local, secured biometric information for authenticating a user and capable of communicating wirelessly with an external receiver-decoder circuit (RDC)"; and "an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service" as recited in claim 2.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed. Therefore, claim 2 is considered to be allowable.

Independent claim 11 recites similar limitations to those found in claim 2. Therefore, claim 11 is considered to be allowable for the same reasons as discussed with claim 2 above.

Examiner performed updated search and additional search does not yield other specific references that reasonably, either singularly or in combination with cited references, would result a proper rejection that would have anticipated or made obvious all the steps disclosed in the independent claims 2 and 11 with proper motivation at or before the time it was effectively filed.

Dependent claims 3-10, 23 and 12-17, 20-22 depend upon the above-mentioned allowed claims 2 and 11 are therefore allowed by virtue of its dependency.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

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

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US20070271194; Walker et al; "Products and Processes for Providing Offers for Products Dispensed from a Dispensing Device" discloses "hard-wired circuitry or

custom hardware may be used with wireless personal digital assistants (PDAs), for authentication user."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/JASON LEE/

Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	14/171,705	BROWN, DAVID L.	
	Examiner	Art Unit	
	JASON LEE	2438	

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

(1) *JASON LEE*. (3)_____.

(2) *Mr. Matthew Holmes (Registration No. 65,160)* . (4)_____.

Date of Interview: *09 January 2015*.

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

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

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

Claim(s) discussed: *n/a*.

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

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

The examiner confirmed authorization from Attorney of record Mr. Matthew Holmes (Registration No. 65,160) to implement Examiner's Amendment based on Applicant's proposed examiner's amendment submitted by email on 01/09/2015..

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

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

☐ Attachment

/JASON LEE/ Primary Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 14/171,705	Applicant(s)/Patent Under Reexamination BROWN, DAVID L.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0271194	11-2007	Walker et al.	705/080
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	"20070271194".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:00
L6	0	(integrated personal digital key) with (biometric information) with (receiver-decoder circuit)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:15
L7	0	(integrated personal digital key) with (biometric information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:15
L8	0	(integrated key) with (biometric information)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:15
L9	5	(integrated key) with (biometric)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:16
L10	0	((integrated key) with (biometric)) same (decoder circuit)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2015/01/09 13:17
S1	2	"8171528".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:18
S2	2	"8646942".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:19
S3	2	"8646042".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 18:19
S4	2	"20060208066".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/16 19:50
S5	3	"20060113381".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/17 11:43
S6	2	"20060208066".pn. and signal	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2014/09/17 12:37

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	0	(integrated personal digital key) with (biometric information) with (receiver-decoder circuit).clm.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/01/09 13:13
L4	0	(integrated personal digital key) with (biometric information) same (receiver-decoder circuit) and (application or function or service).clm.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/01/09 13:14
L5	0	(integrated personal digital key) with (biometric information) with (receiver-decoder circuit)	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/01/09 13:15
L11	0	(integrated personal digital key) with (biometric information) with (receiver-decoder circuit).clm.	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/01/09 13:18

1/9/2015 1:19:08 PM
C:\Users\jlee16\Documents\EAST\Workspaces\14171705-091614.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	14171705
	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 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
/J.L./	1	4759060	A	1988-07-19	Hayashi et al.	
/J.L./	2	5187352	A	1993-02-16	Blair et al.	
/J.L./	3	5296641	A	1994-03-22	Stelzel	
/J.L./	4	5392433	A	1995-02-21	Hammersley et al.	
/J.L./	5	5422632	A	1995-06-06	Bucholtz et al.	
/J.L./	6	5450489	A	1995-09-12	Ostrover et al.	
/J.L./	7	5619251	A	1997-04-08	Kuroiwa et al.	
/J.L./	8	5629980	A	1997-05-13	Stefik et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	9	5644354	A	1997-07-01	Thompson et al.	
/J.L./	10	5666412	A	1997-09-09	Handelman et al.	
/J.L./	11	5773954	A	1998-06-30	VanHorn, David B.	
/J.L./	12	5784464	A	1998-07-21	Akiyama et al.	
/J.L./	13	5825876	A	1998-10-20	Peterson, Jr.	
/J.L./	14	5857020	A	1999-01-05	Peterson, Jr.	
/J.L./	15	5892825	A	1999-04-06	Mages et al.	
/J.L./	16	5894551	A	1999-04-13	Huggins et al.	
/J.L./	17	5898880	A	1999-04-27	Ryu	
/J.L./	18	5928327	A	1999-07-27	Wang et al.	
/J.L./	19	5991399	A	1999-11-23	Graunke et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	20	5991749	A	1999-11-23	Morrill, Jr.	
/J.L./	21	6035038	A	2000-03-07	Campinos et al.	
/J.L./	22	6035329	A	2000-03-07	Mages et al.	
/J.L./	23	6041410	A	2000-03-21	Hsu et al.	
/J.L./	24	6055314	A	2000-04-25	Spies et al.	
/J.L./	25	6070796	A	2000-06-06	Sirbu	
/J.L./	26	6088730	A	2000-07-11	Kato et al.	
/J.L./	27	6104334	A	2000-08-15	Allport	
/J.L./	28	6110041	A	2000-08-29	Walker et al.	
/J.L./	29	6148142	A	2000-11-14	Anderson	
/J.L./	30	6161179	A	2000-12-12	Seidel	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	31	6209089	B1	2001-03-27	Selitrennikoff et al.	
/J.L./	32	6219109	B1	2001-04-17	Raynesford et al.	
/J.L./	33	6247130	B1	2001-06-12	Fritsch	
/J.L./	34	6266415	B1	2001-07-24	Campinos et al.	
/J.L./	35	6295057	B1	2001-09-25	Rosin et al.	
/J.L./	36	6336121	B1	2002-01-01	Lyson et al.	
/J.L./	37	6336142	B1	2002-01-01	Kato et al.	
/J.L./	38	6367019	B1	2002-04-02	Ansell et al.	
/J.L./	39	6381747	B1	2002-04-30	Wonfor et al.	
/J.L./	40	6385596	B1	2002-05-07	Wiser et al.	
/J.L./	41	6392664	B1	2002-05-21	White et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	42	6397387	B1	2002-05-28	Rosin et al.	
/J.L./	43	6401059	B1	2002-06-04	Shen et al.	
/J.L./	44	6411307	B1	2002-06-25	Rosin et al.	
/J.L./	45	6424715	B1	2002-07-23	Saito	
/J.L./	46	6425084	B1	2002-07-23	Rallis et al.	
/J.L./	47	6434535	B1	2002-08-13	Kupka et al.	
/J.L./	48	6446130	B1	2002-09-03	Grapes	
/J.L./	49	6463534	B1	2002-10-08	Geiger et al.	
/J.L./	50	6480188	B1	2002-11-12	Horsley	
/J.L./	51	6490443	B1	2002-12-03	Freeny, Jr.	
/J.L./	52	6510350	B1	2003-01-21	Steen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	53	6523113	B1	2003-02-18	Wehrenberg	
/J.L./	54	6529949	B1	2003-03-04	Getsin et al.	
/J.L./	55	6546418	B1	2003-04-08	Schena et al.	
/J.L./	56	6550011	B1	2003-04-15	Sims, III	
/J.L./	57	6563805	B1	2003-05-13	Ma et al.	
/J.L./	58	6564380	B1	2003-05-13	Murphy	
/J.L./	59	6628302	B1	2003-09-30	White et al.	
/J.L./	60	6632992	B2	2003-10-14	Hasegawa	
/J.L./	61	6647417	B1	2003-11-11	Hunter et al.	
/J.L./	62	6667684	B1	2003-12-23	Waggamon et al.	
/J.L./	63	6683954	B1	2004-01-27	Searle	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03	
	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	64	6697944	B1	2004-02-24	Jones et al.	
/J.L./	65	6711464	B1	2004-03-23	Yap et al.	
/J.L./	66	6775655	B1	2004-08-10	Peinado et al.	
/J.L./	67	6804825	B1	2004-10-12	White et al.	
/J.L./	68	6806887	B2	2004-10-19	Chernock et al.	
/J.L./	69	6850147	B2	2005-02-01	Prokoski et al.	
/J.L./	70	6873975	B1	2005-03-29	Hatakeyama et al.	
/J.L./	71	6879567	B2	2005-04-12	Callaway et al.	
/J.L./	72	6950941	B1	2005-09-27	Lee et al.	
/J.L./	73	6957086	B2	2005-10-18	Bahl et al.	
/J.L./	74	6973576	B2	2005-12-06	Giobbi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03
(Not for submission under 37 CFR 1.99)	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

/J.L./	75	6975202	B1	2005-12-13	Rodriguez et al.	
/J.L./	76	7012503	B2	2006-03-14	Nielsen	
/J.L./	77	7159765	B2	2007-01-09	Frerking, Gary	
/J.L./	78	7249177	B1	2007-07-24	Miller	
/J.L./	79	7305560	B2	2007-12-04	Giobbi	

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
/J.L./	1	20020007456	A1	2002-01-17	Peinado et al.	
/J.L./	2	20020013772	A1	2002-01-31	Peinado	
/J.L./	3	20020015494	A1	2002-02-07	Nagai et al.	
/J.L./	4	20020026424	A1	2002-02-28	Akashi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705	14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03	
(Not for submission under 37 CFR 1.99)	First Named Inventor	David L. Brown	
	Art Unit	2438	
	Examiner Name	Jason T. Lee	
	Attorney Docket Number	10001-04293 US	

/J.L./	5	20020073042	A1	2002-06-13	Maritzen et al.	
/J.L./	6	20020104006	A1	2002-08-01	Boate et al.	
/J.L./	7	20020108049	A1	2002-08-08	Xu et al.	
/J.L./	8	20020109580	A1	2002-08-15	Shreve et al.	
/J.L./	9	20030055689	A1	2003-03-20	Block et al.	
/J.L./	10	20030213840	A1	2003-11-20	Livingston et al.	
/J.L./	11	20040129787	A1	2004-07-08	Saito et al.	
/J.L./	12	20050090200	A1	2005-04-28	Karaoguz et al.	
/J.L./	13	20050116020	A1	2005-06-02	Smolucha et al.	
/J.L./	14	20060111955	A1	2006-05-25	Winter et al.	
/J.L./	15	20060136742	A1	2006-06-22	Giobbi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03
(Not for submission under 37 CFR 1.99)	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

/J.L./	16	20060208066	A1	2006-09-21	Finn et al.		
/J.L./	17	20070159994	A1	2007-07-12	Brown et al.		
/J.L./	18	20070174809	A1	2007-07-26	Brown et al.		

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/J.L./	1	WO 2000/062505	WO	A1	2000-10-19	Thomson Multimedia		☐
/J.L./	2	WO 2001/022724	WO	A1	2001-03-29	Thomson Multimedia		☐
/J.L./	3	WO 2001/075876	WO	A1	2001-10-11	Thomson Multimedia		☐
/J.L./	4	WO 2001/077790	WO	A1	2001-10-18	Thomson Multimedia		☐
/J.L./	5	WO 2005/050450	WO	A1	2005-06-02	Margent Development, LLC		☐
/J.L./	6	WO 2005/086802	WO	A2	2005-09-22	Margent Development, LLC		☐

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
(Not for submission under 37 CFR 1.99)	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

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.	T5
/J.L./	1	"Alliance Activities: Publications: Identity- Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pages.	☐
/J.L./	2	Antonoff, Michael, "Visiting Video Valley," Sound & Vision, pp. 116 and 118-119, Nov. 2001.	☐
/J.L./	3	"Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002 [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.securitymagazine.comlCDA/Articles/ Technologies/3ae61Oeaa34d801OVgnVCM100000f932a8cO-> 5 pages.	☐
/J.L./	4	Article, "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, Jul. 24, 2000, 2 pages.	☐
/J.L./	5	Article, "Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, Aug. 14, 2000, 2 pages.	☐
/J.L./	6	Blum, Jonathan, "Digital Rights Management May Solve the Napster "Problem"," Technology Investor Industry Sector, (Oct. 2000), 24-27.	☐
/J.L./	7	Brown, D, Techniques for Privacy and Authentication in Personal Communication Systems; Personal Communications, IEEE; Vol. 2, Issue: 4 Publication Year: 1995, pp. 6-10.	☐
/J.L./	8	Dagan (Power over Ethernet (PoE) Midspan-The Smart Path to Providing Power for IP Telephony Author: Sharon Dagan, Product Manager, Systems Aug. 2005, PowerDsine Inc.), 28 pages.	☐
/J.L./	9	Debow, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p10, Nov. 1989, 4 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
(Not for submission under 37 CFR 1.99)	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

/J.L./	10	Dennis, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, Dec. 2, 1999, 2 pages.	☐
/J.L./	11	Fasca, Chad, "The Circuit," Electronic News, 45(45) (Nov. 8, 1999), 20 pages.	☐
/J.L./	12	Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, Jan. 18, 1996, 2 pages.	☐
/J.L./	13	"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.biopay.comlfaqs-lowes.asp>, 5 pages.	☐
/J.L./	14	Generation of keys for use with the digital signature standard (DSS) ; Nel, J.J.; Kuhn, G.J.; Communications and Signal Processing, 1993., Proceedings of the 1993 IEEE South African Symposium on Publication Year: 1993, pp. 6-11.	☐
/J.L./	15	"IEEE 802.15.4-2006-Wikipedia, the free encyclopedia," Wikipedia®, Last Modified Mar. 21, 2009 [Online] [Retrieved on Apr. 30, 2009] Retrieved from the Internet <URL:http://en.wikipedia.org/wiki/IEEE_802.15.4-2006>, 4 pages.	☐
/J.L./	16	Lake, Matt, "Downloading for Dollars," Sound & Vision, (Nov. 2000), pages 137-138.	☐
/J.L./	17	Lewis, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, Nov. 16, 1995, 1 page.	☐
/J.L./	18	McIver, R. et al., "Identification and Verification Working Together," Bioscrypt™, Aug. 27, 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.ibia.org/ membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf>, 5 pages.	☐
/J.L./	19	Nilsson, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise% 20Match-onCard%20for%20Java%20Cards.pdf>, 5 pages.	☐
/J.L./	20	Nordin, B., "Match-On-Card Technology," Precise™ Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.ibia.org/ Membersadmin/whitepapers/pdf/17 IPrecise%20Match-onCard%20technology.pdf>, 7 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

/J.L./	21	Notification of the International Search Report and Written Opinion, PCT/US04/38124, Apr. 7, 2005, 10 pages.	☐
/J.L./	22	Paget, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, (Dec. 1999), 4 pgs.	☐
/J.L./	23	PCT International Search Report and Written Opinion, PCT/US07/11105, Oct. 20, 2008, 10 pages.	☐
/J.L./	24	PCT International Search Report and Written Opinion, PCT/US07/11103, Apr. 23, 2008, 9 pages.	☐
/J.L./	25	PCT International Search Report and Written Opinion, PCT/US05/43447, Feb. 22, 2007, 7 pages.	☐
/J.L./	26	PCT International Search Report and Written Opinion, PCT/US05/46843, Mar. 1, 2007, 10 pages.	☐
/J.L./	27	PCT International Search Report and Written Opinion, PCT/US07/00349, Mar. 19, 2008, 10 pages.	☐
/J.L./	28	Personal Servers as Digital Keys; Beaufour, A.; Bonnet, P.; Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on Publication Year: 2004, pages 319-328.	☐
/J.L./	29	Press Release, "Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, Jan. 8, 2002, 3 pages.	☐
/J.L./	30	Press Release, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, January 11, 2002, 2 pages.	☐
/J.L./	31	Press Release, "Thompson Bets on Smart Cards for Video Encryption," www.informationweek.com. Jun. 7, 2001, 1 page.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
(Not for submission under 37 CFR 1.99)	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

/J.L./	32	Press Release, "Thompson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com May 30, 2001, 2 pages.	☐
/J.L./	33	"SAFModule™: A Look Into Strong Authentication," saflink Corporation, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pages.	☐
/J.L./	34	Sapsford, Jathon, "E-Business: Sound Waves Could Help Ease WebFraud Woes," Wall Street Journal, (Aug. 14, 2000), B1, 2 pages.	☐
/J.L./	35	"Say Hello to Bluetooth," Bluetooth Web site, 5 pages [Last retrieved on March 25, 2008].	☐
/J.L./	36	"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>, 7 pages.	☐
/J.L./	37	Van Winkle, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, (Jan. 2000), pp. 148-153.	☐
/J.L./	38	Wade, W., "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, Apr. 21, 2003, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL: http://www.biometricgroup.comlin_the_news/04.21.03.html>, 3 pages.	☐
/J.L./	39	Wallace, Bob, "The Internet Unplugged," InformationWeek, 765(22), (Dec. 13, 1999), pp. 22-24.	☐
/J.L./	40	Weber, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, (Jul. 24, 2000), B1, 2 pages.	☐
/J.L./	41	Non-Final Office Action, U.S. Appl. No. 11/939,451, Dated: May 12, 2010, 12 pages.	☐
If you wish to add additional non-patent literature document citation information please click the Add button			Add

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Receipt date: 12/04/2014	Application Number	14171705 14171705 - GAU: 2438
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2014-02-03
	First Named Inventor	David L. Brown
	Art Unit	2438
	Examiner Name	Jason T. Lee
	Attorney Docket Number	10001-04293 US

EXAMINER SIGNATURE			
Examiner Signature	/Jason Lee/	Date Considered	01/09/2015

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.L./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	**Art Unit**
	JASON LEE	2438

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

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

CLAIM		DATE								
Final	Original	09/17/2014	01/09/2015							
	1	✓	-							
1	2		=							
2	3		=							
3	4		=							
4	5		=							
5	6		=							
6	7		=							
7	8		=							
8	9		=							
9	10		=							
10	11		=							
11	12		=							
12	13		=							
13	14		=							
14	15		=							
15	16		=							
16	17		=							
	18		-							
	19		-							
17	20		=							
18	21		=							
19	22		=							
20	23		=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	3,4	9/16/14	JL

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched	9/16/14	JL
google patent searched with RFID smartcard with signal receiver	9/16/14	JL
google searched	1/9/15	JL
(integrated key) with (biometric) (integrated key) with (biometric); ((integrated key) with (biometric)) same (decoder circuit);	1/9/15	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
726	3	1/9/15	JL
	(integrated personal digital key) with (biometric information) same (receiver-decoder circuit) and (application or function or service).clm.; (integrated personal digital key) with (biometric information) with (receiver-decoder circuit).clm.	1/9/15	JL

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	**Art Unit**
	JASON LEE	2438

CPC						
Symbol					**Type**	**Version**
H04L		63	/	08	F	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

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

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/JASON LEE/ Primary Examiner.Art Unit 2438	01/09/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	2	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	**Art Unit**
	JASON LEE	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
726	3	G 0 6 F 21 / 00 (2013.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	1	2	4		
705	80				

NONE		Total Claims Allowed: 20	
(Assistant Examiner)	(Date)		
/JASON LEE/ Primary Examiner.Art Unit 2438	01/09/2015	O.G. Print Claim(s) 2	O.G. Print Figure 1
(Primary Examiner)	(Date)		

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14171705	BROWN, DAVID L.
	Examiner	**Art Unit**
	JASON LEE	2438

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

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

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/JASON LEE/ Primary Examiner.Art Unit 2438 (Primary Examiner)	01/09/2015 (Date)	O.G. Print Claim(s) 2	O.G. Print Figure 1

Doc code: Oath
Document Description: Oath or declaration filed

PTO/AIA/02 (07-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

SUBSTITUTE STATEMENT IN LIEU OF AN OATH OR DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (35 U.S.C. 115(d) AND 37 CFR 1.64)

Title of Invention	Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use

This statement is directed to:

☐ The attached application,

OR

☒ United States application or PCT international application number 14/171,705 filed on February 3, 2014.

LEGAL NAME of inventor to whom this substitute statement applies:

(*E.g.*, Given Name (first and middle (if any)) and Family Name or Surname)

David L. Brown

Residence (except for a deceased or legally incapacitated inventor):

City	State	Country
Jupiter	FL	US

Mailing Address (except for a deceased or legally incapacitated inventor):

17708 127th Dr. North

City	State	Zip	Country
Jupiter	FL	33478	US

I believe the above-named inventor or joint inventor to be the original inventor or an original joint inventor of a claimed invention in the application.

The above-identified application was made or authorized to be made by me.

I hereby acknowledge that any willful false statement made in this statement is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Relationship to the inventor to whom this substitute statement applies:

- ☐ Legal Representative (for deceased or legally incapacitated inventor only),
- ☒ Assignee,
- ☐ Person to whom the inventor is under an obligation to assign,
- ☐ Person who otherwise shows a sufficient proprietary interest in the matter (petition under 37 CFR 1.46 is required), or
- ☐ Joint Inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/AIA02 (07-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

SUBSTITUTE STATEMENT

Circumstances permitting execution of this substitute statement:

- ☐ Inventor is deceased,
- ☐ Inventor is under legal incapacity,
- ■ Inventor cannot be found or reached after diligent effort, or
- ☐ Inventor has refused to execute the oath or declaration under 37 CFR 1.63.

If there are joint inventors, please check the appropriate box below:

- ■ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) naming the entire inventive entity has been or is currently submitted.

OR

- ☐ An application data sheet under 37 CFR 1.76 (PTO/AIA/14 or equivalent) has not been submitted. Thus, a Substitute Statement Supplemental Sheet (PTO/AIA/11 or equivalent) naming the entire inventive entity and providing inventor information is attached. See 37 CFR 1.64(b).

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

Name: John J. Giobbi | Date (Optional):

Signature: John J. Giobbi

APPLICANT NAME AND TITLE OF PERSON EXECUTING THIS SUBSTITUTE STATEMENT:

If the applicant is a juristic entity, list the applicant name and the title of the signer:

Applicant Name: Proxense, LLC

Title of Person Executing This Substitute Statement: Chief Executive Officer

The signer, whose title is supplied above, is authorized to act on behalf of the applicant.

Residence of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent):

City Bend | State OR | Country US

Mailing Address of the signer (unless provided in an application data sheet, PTO/AIA/14 or equivalent)

689 NW Stonepine Drive

City Bend | State OR | Zip 97701 | Country US

Note: Use an additional PTO/AIA/02 form for each inventor who is deceased, legally incapacitated, cannot be found or reached after diligent effort, or has refused to execute the oath or declaration under 37 CFR 1.63.

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:	21347916
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	29-JAN-2015
Filing Date:	03-FEB-2014
Time Stamp:	16:44:30
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	Oath or Declaration filed	04293US_20150129_Substitute Statement.pdf	2381269 512c1ef5db8edd960bd9109413c4cd9295ee4fa8	no	3
Warnings:					
Information:					

Total Files Size (in bytes):	2381269

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.

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 01/28/2015
Patent Law Works/Proxense
Greg Sueoka
201 South Main Street, Suite 250
Salt Lake City, UT 84111

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

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	02/03/2014	David L. Brown	10001-04293 US	7167

TITLE OF INVENTION: HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	04/28/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, JASON T	2438	726-003000

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

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

1 Patent Law Works LLP
2
3

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

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

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

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

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

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

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

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

Authorized Signature /Paige Alsbury/ Date April 27, 2015
Typed or printed name Paige M. Alsbury Registration No. 72965

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

Electronic Patent Application Fee Transmittal

Application Number:	14171705
Filing Date:	03-Feb-2014
Title of Invention:	HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE
First Named Inventor/Applicant Name:	David L. Brown
Filer:	Paige McDede Alsbury/Esther Kim
Attorney Docket Number:	10001-04293 US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

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

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

Electronic Acknowledgement Receipt	
EFS ID:	22174099
Application Number:	14171705
International Application Number:	
Confirmation Number:	7167
Title of Invention:	HYBRID DEVICE HAVING A PERSONAL DIGITAL KEY AND RECEIVER-DECODER CIRCUIT AND METHODS OF USE
First Named Inventor/Applicant Name:	David L. Brown
Customer Number:	89194
Filer:	Paige McDede Alsbury
Filer Authorized By:	
Attorney Docket Number:	10001-04293 US
Receipt Date:	27-APR-2015
Filing Date:	03-FEB-2014
Time Stamp:	13:55:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$480
RAM confirmation Number	149
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	04293US_IssueFeeTransmittal.pdf	176221 da85457b3378640da81d7b10e26d971ad33bc498	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30981 2969ec8b382c56e37682e65586791c6e85820f9b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	207202		

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/171,705	06/02/2015	9049188	10001-04293 US	7167

89194 7590 05/13/2015

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

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

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

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

Proxense, LLC, Residence Not Provided;
David L. Brown, Jupiter, FL;

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.

AO 120 (Rev. 08/10)

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

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

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

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

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

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

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

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

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

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

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