US 20040255139A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0255139 A1

Giobbi (43) Pub. Date: Dec. 16, 2004

(54) DIGITAL CONTENT SECURITY SYSTEM

(76) Inventor: John J. Giobbi, Bend, OR (US)

Correspondence Address:
Michael J. Blankstein
2014 Harrison Street
Evanston, IL 60201 (US)

(21) Appl. No.: 10/847,135

(22) Filed: May 17, 2004

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/715,035, filed on Nov. 17, 2003, which is a continuation-in-part of application No. 10/153,979, filed on May 23, 2002, which is a continuation-in-part of application No. 09/750,487, filed on Dec. 27, 2000, and which is a continuation-in-part of application No. 10/016,857, filed on Dec. 14, 2001.

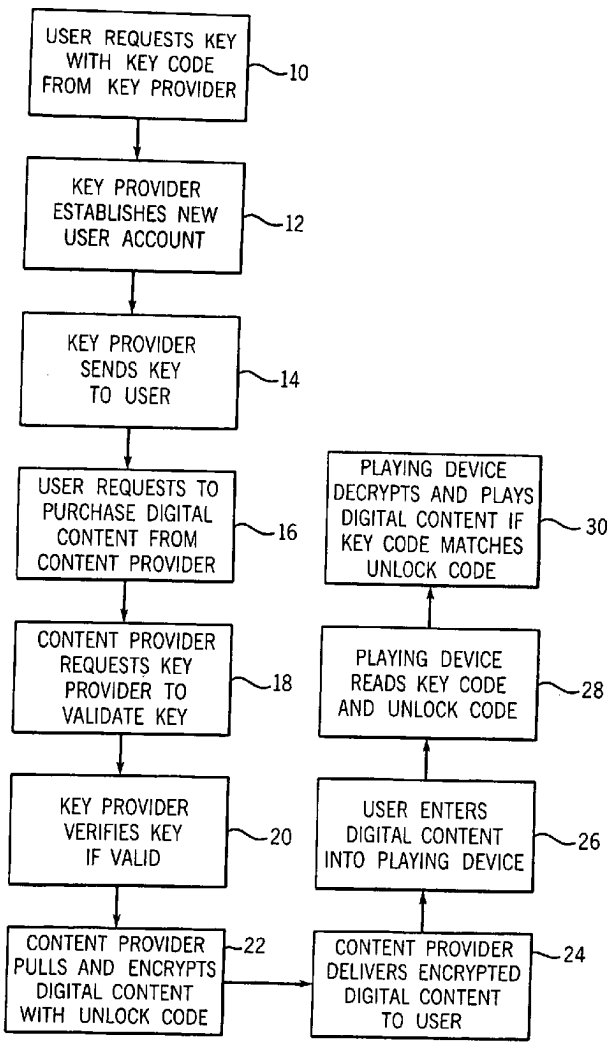
Publication Classification

(51) Int. Cl.[7] G06F 12/14; H04L 9/00

(52) U.S. Cl. 713/193; 380/231; 705/51

(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 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.



GOOGLE EXHIBIT 1007

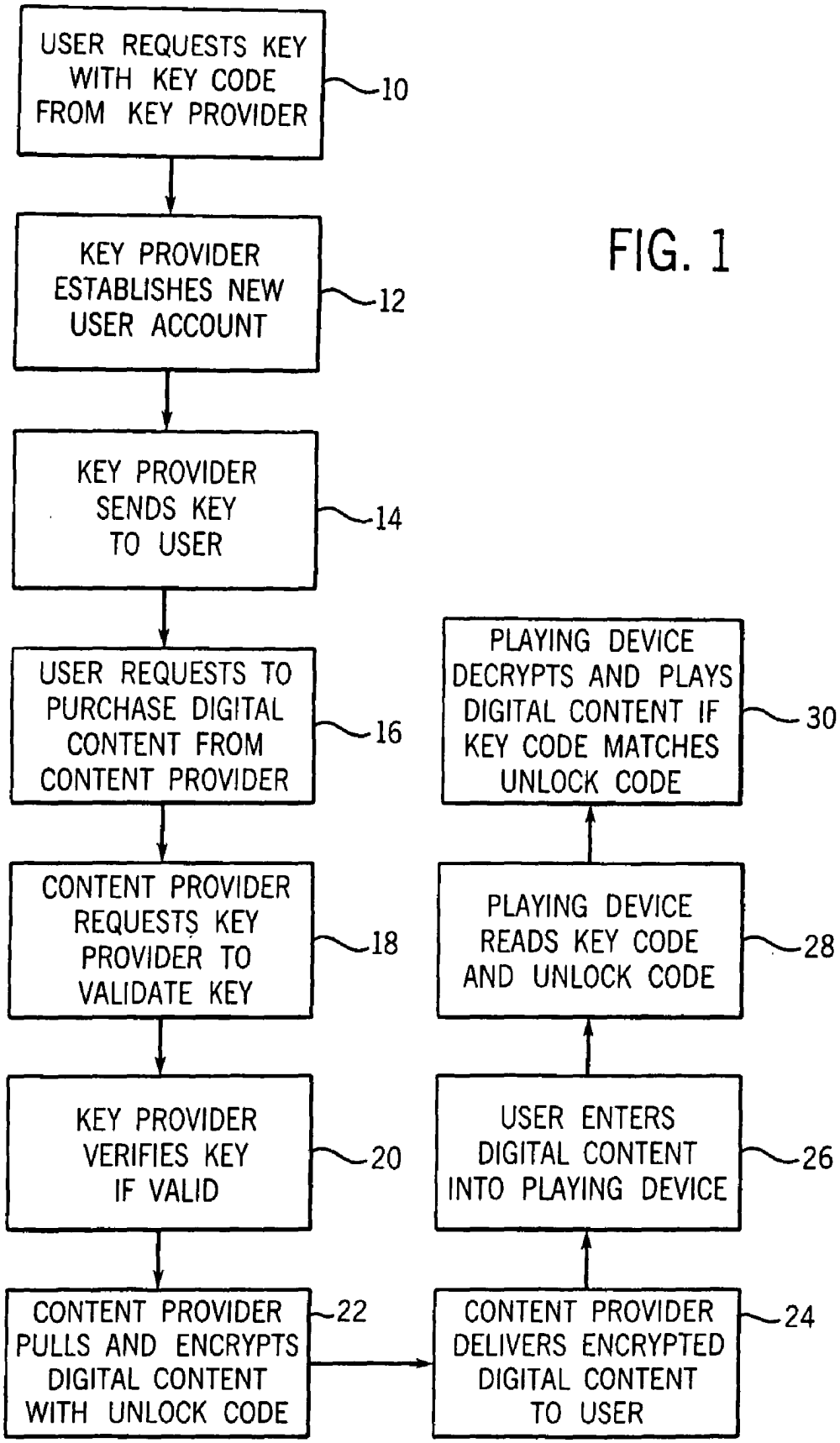

USER REQUESTS KEY WITH KEY CODE FROM KEY PROVIDER
10
KEY PROVIDER ESTABLISHES NEW USER ACCOUNT
12
KEY PROVIDER SENDS KEY TO USER
14
USER REQUESTS TO PURCHASE DIGITAL CONTENT FROM CONTENT PROVIDER
16
CONTENT PROVIDER REQUESTS KEY PROVIDER TO VALIDATE KEY
18
KEY PROVIDER VERIFIES KEY IF VALID
20
CONTENT 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

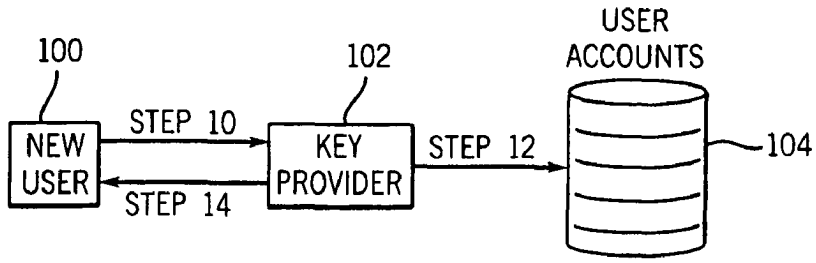


FIG. 2

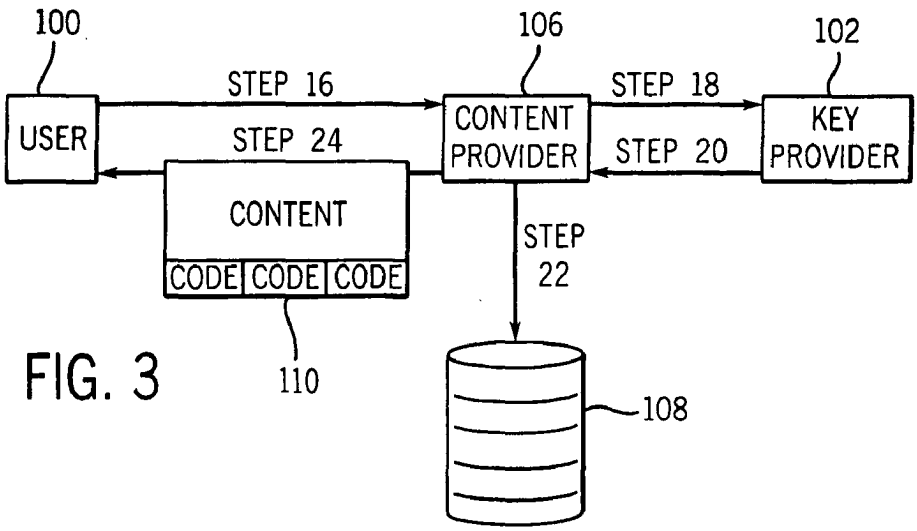


FIG. 3

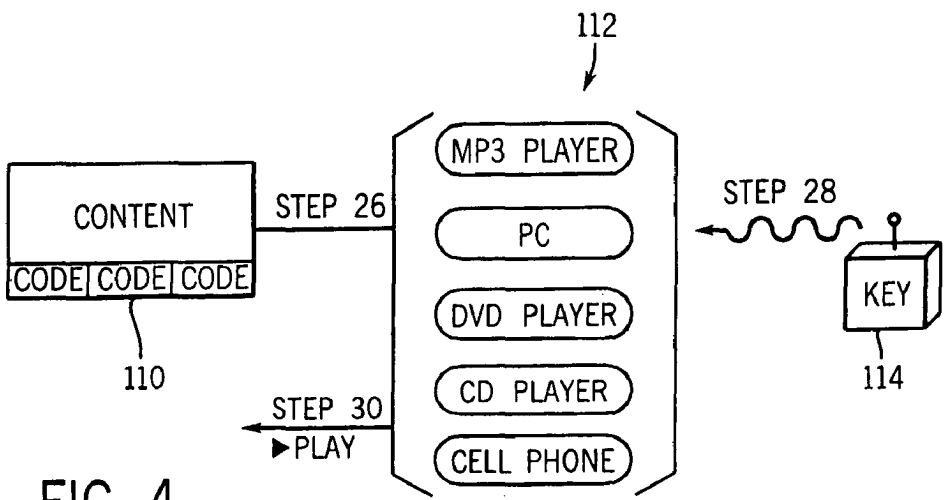


FIG. 4

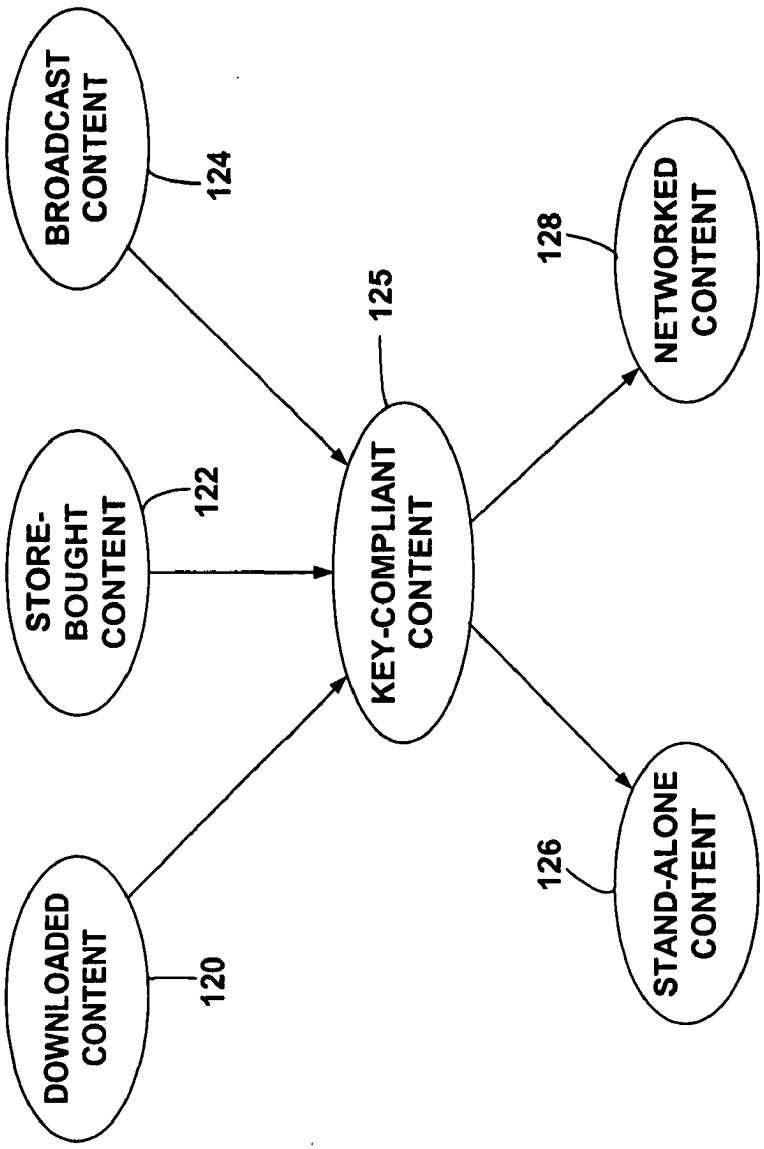

BROADCAST CONTENT
124
STORE-BOUGHT CONTENT
122
DOWNLOADED CONTENT
120
KEY-COMPLIANT CONTENT
125
NETWORKED CONTENT
128
STAND-ALONE CONTENT
126

FIG. 5

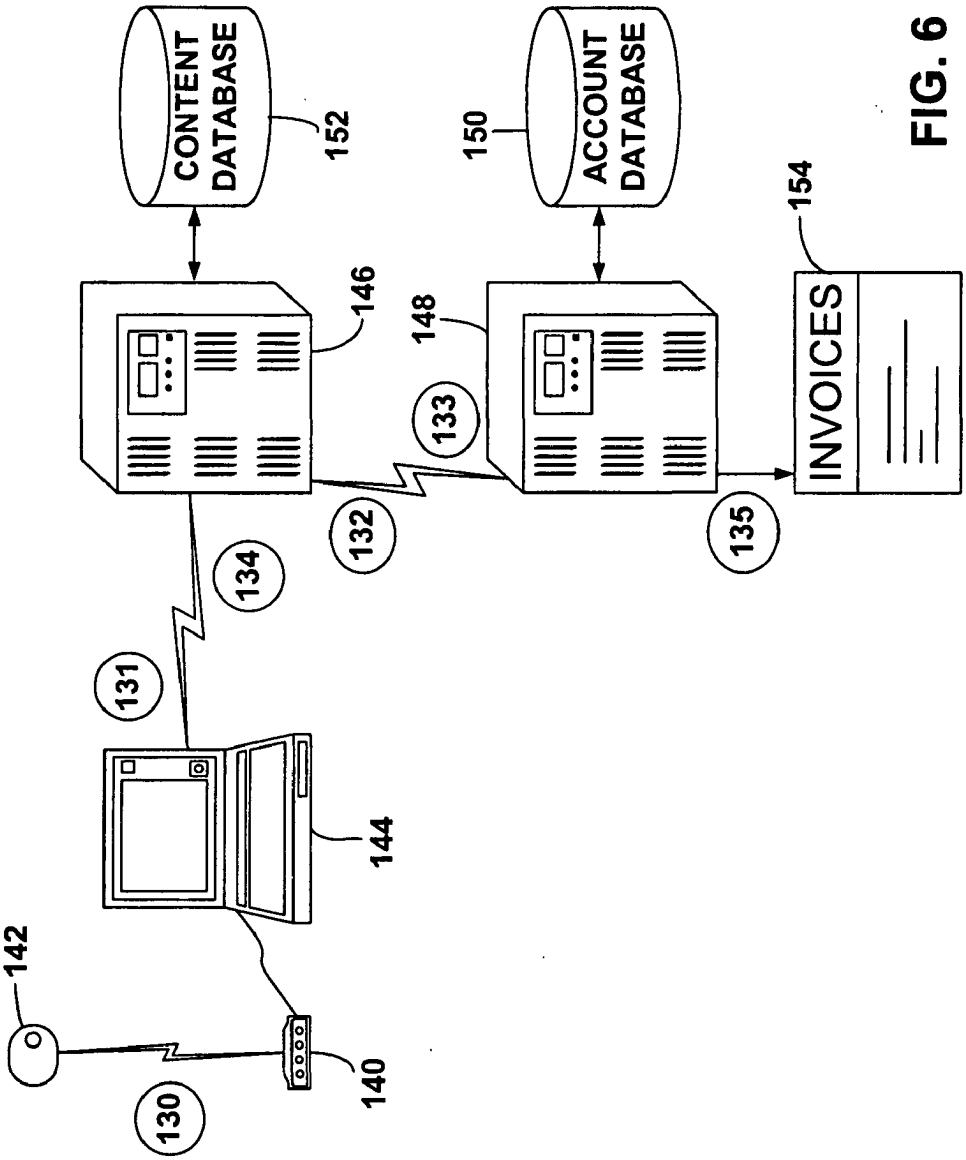

CONTENT DATABASE
152
ACCOUNT DATABASE
150
154
INVOICES
146
148
133
132
134
131
135
144
142
140
130

FIG. 6

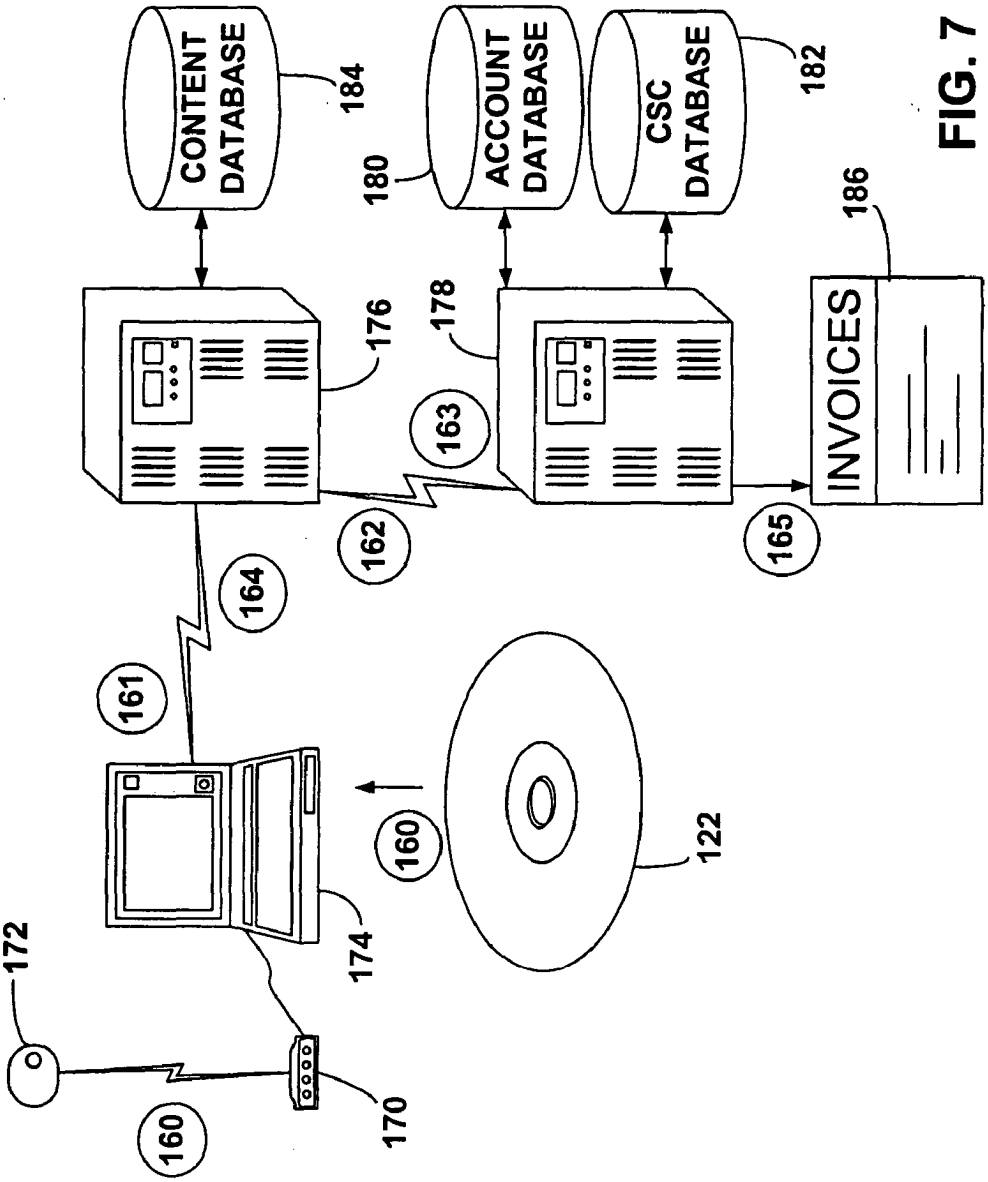

CONTENT DATABASE
184
ACCOUNT DATABASE
180
CSC DATABASE
182
186
INVOICES
176
178
163
162
165
164
161
160
122
174
172
170
160

FIG. 7

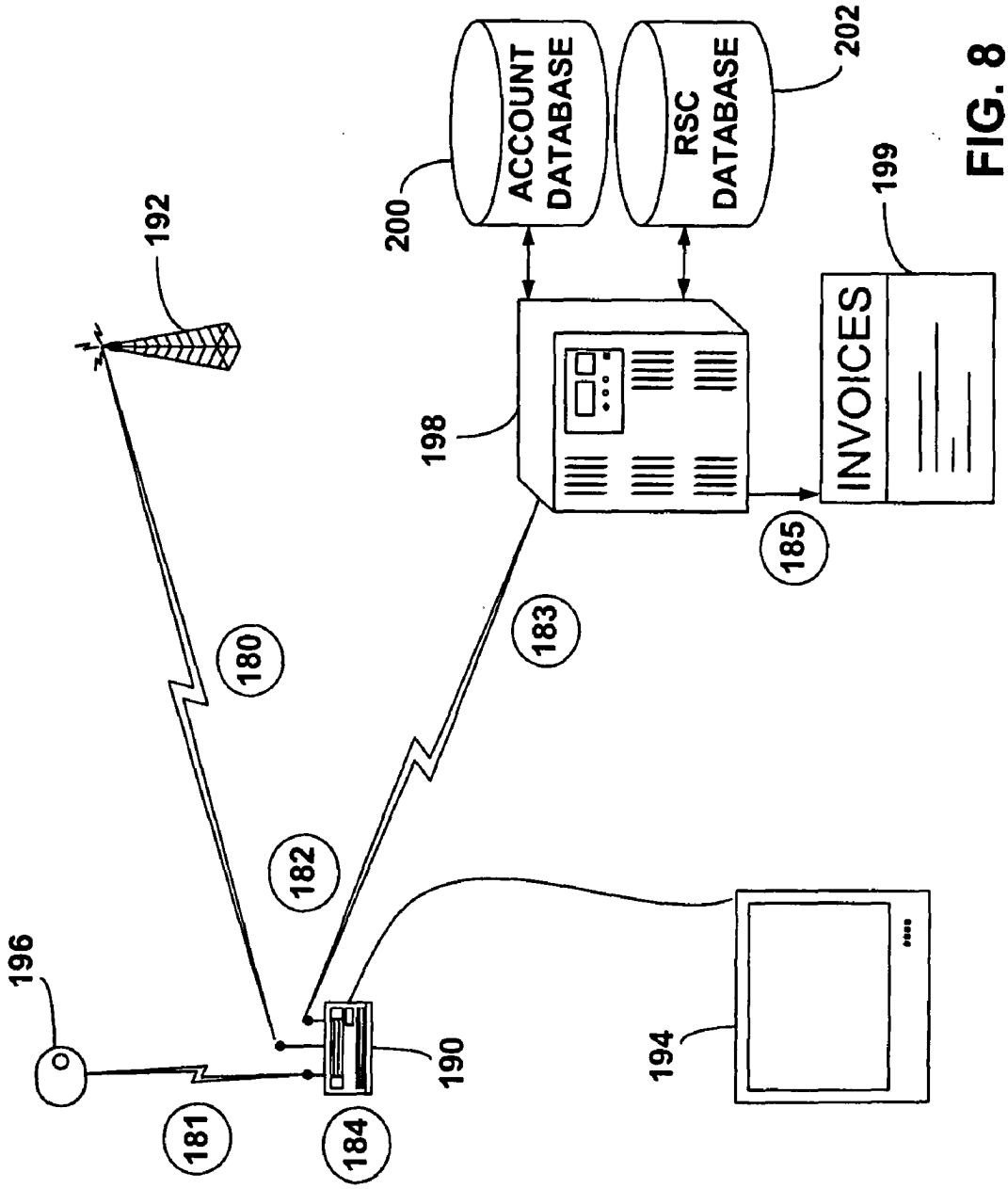

ACCOUNT DATABASE
RSC DATABASE
INVOICES
192
200
202
199
198
185
183
180
182
196
181
184
190
194

FIG. 8

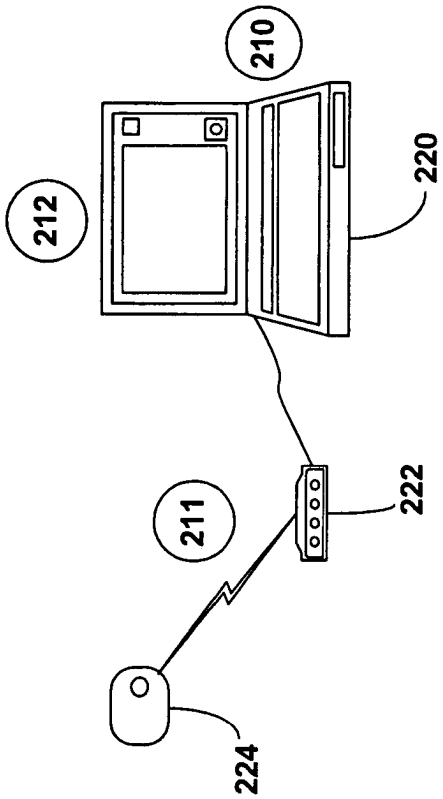


FIG. 9a

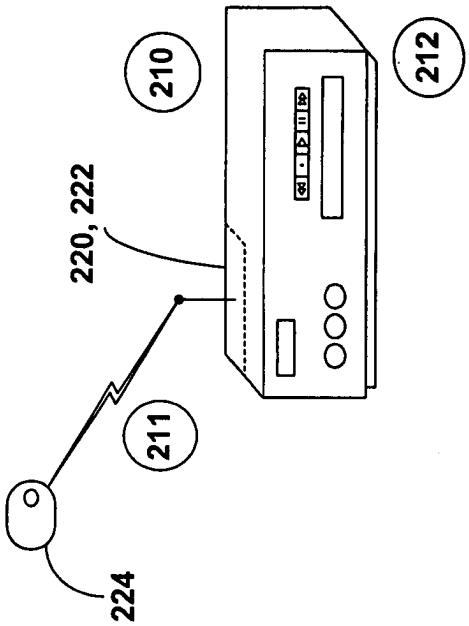


FIG. 9b

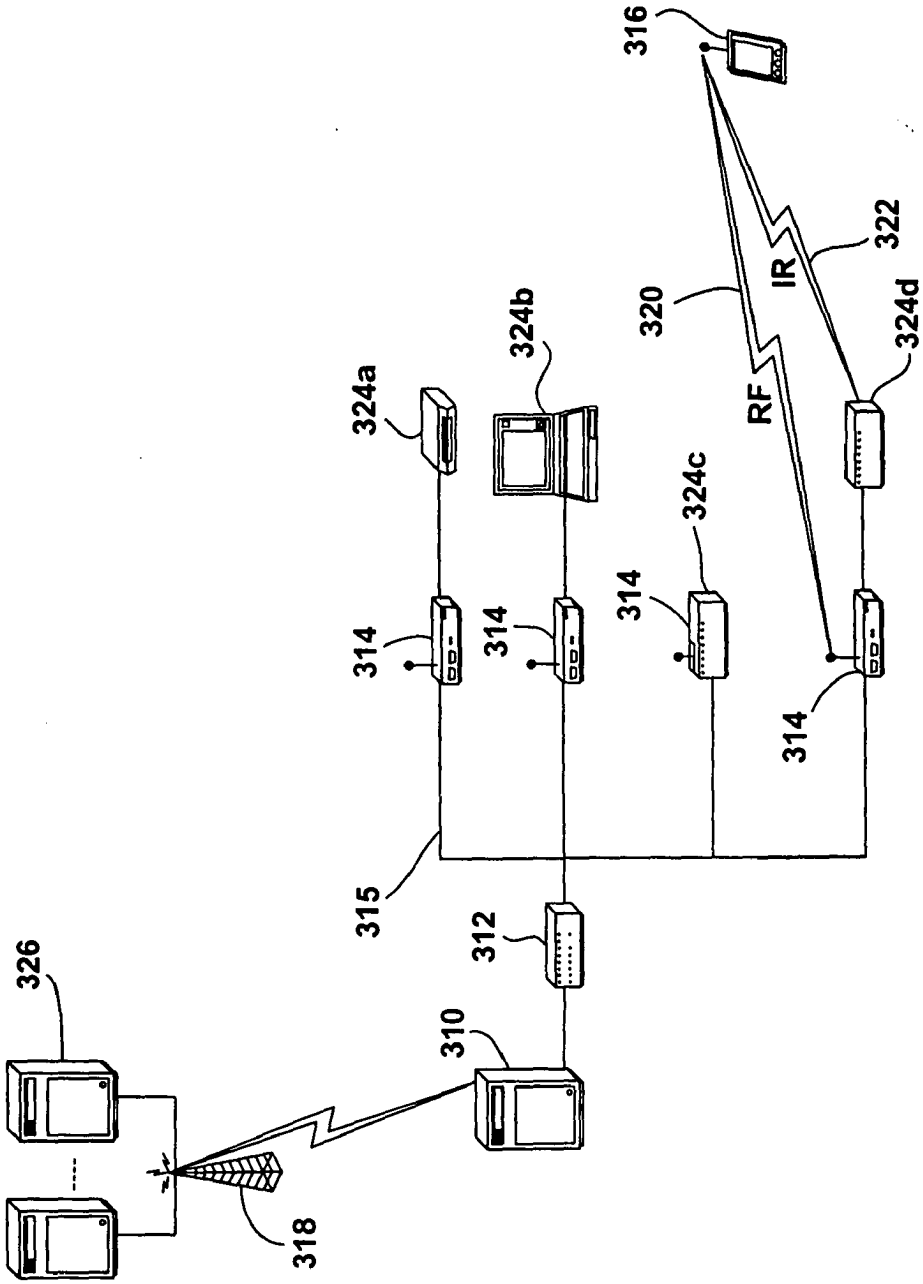

326
318
310
312
315
314
324a
314
324b
314
324c
320
RF
IR
322
316
324d
314

FIG. 10

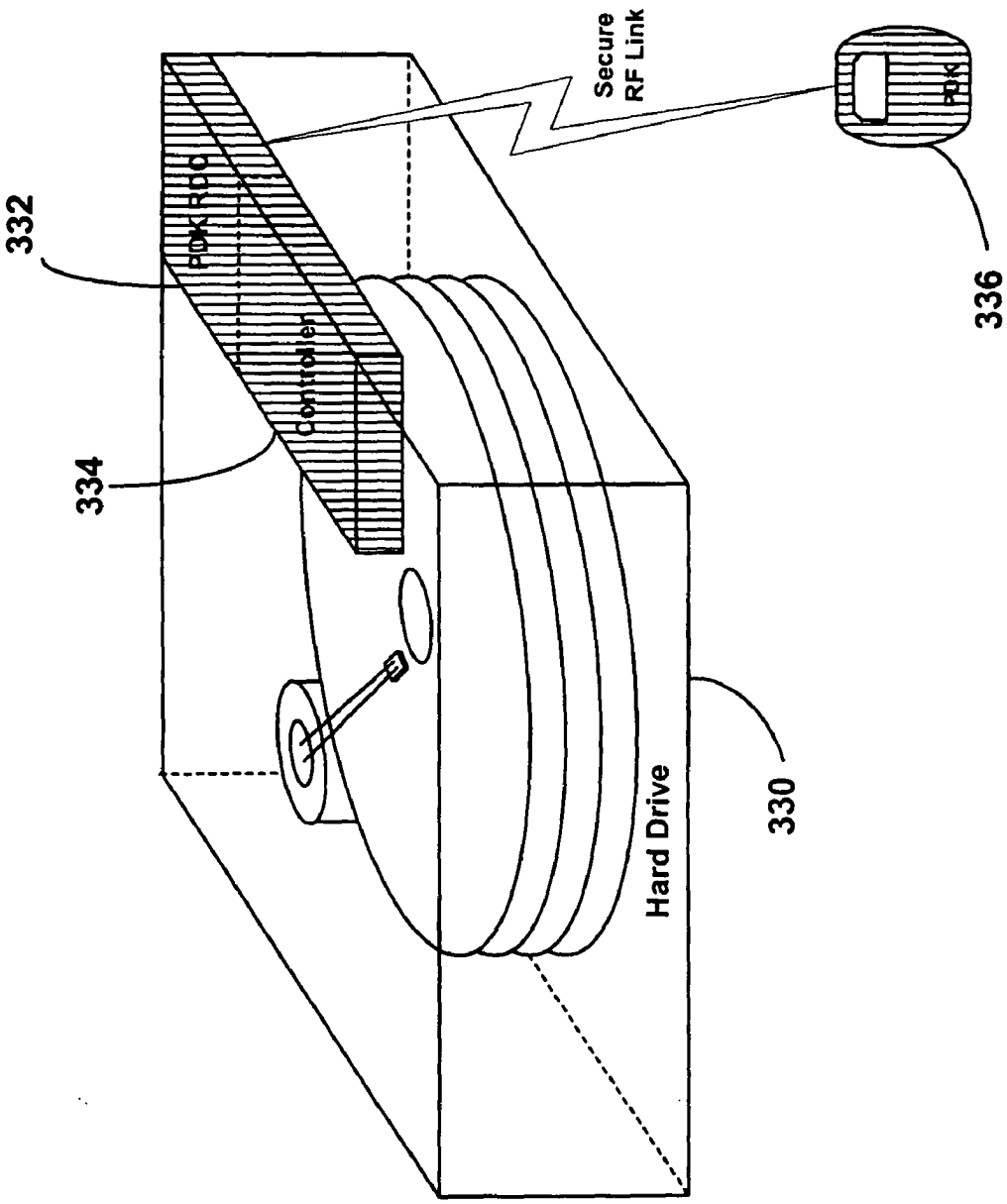

332
334
330
336
POK RDO
Controller
Hard Drive
Secure
RF Link
POK

FIG. 11

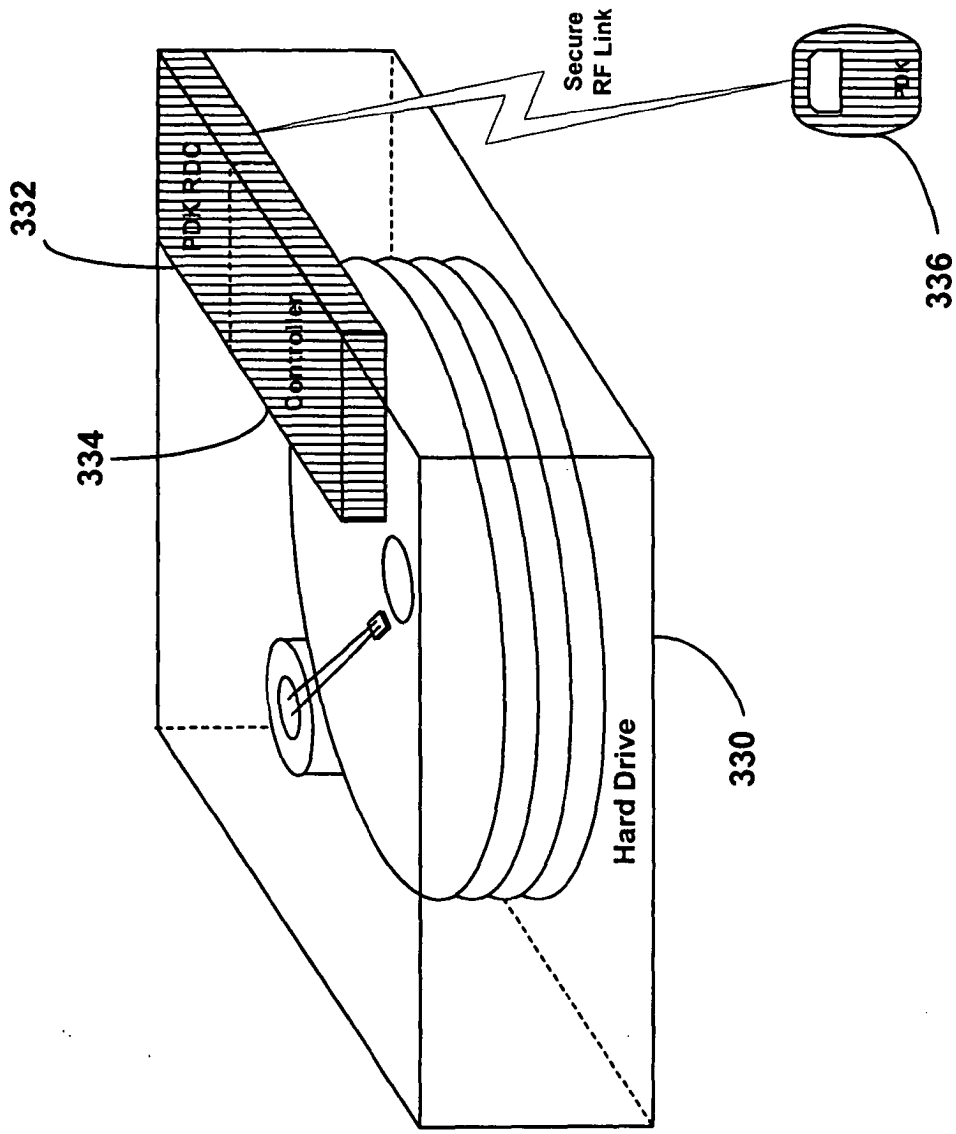

332
334
PDK RPC
Controller
Hard Drive
330
Secure
RF Link
PDK
336

FIG. 12

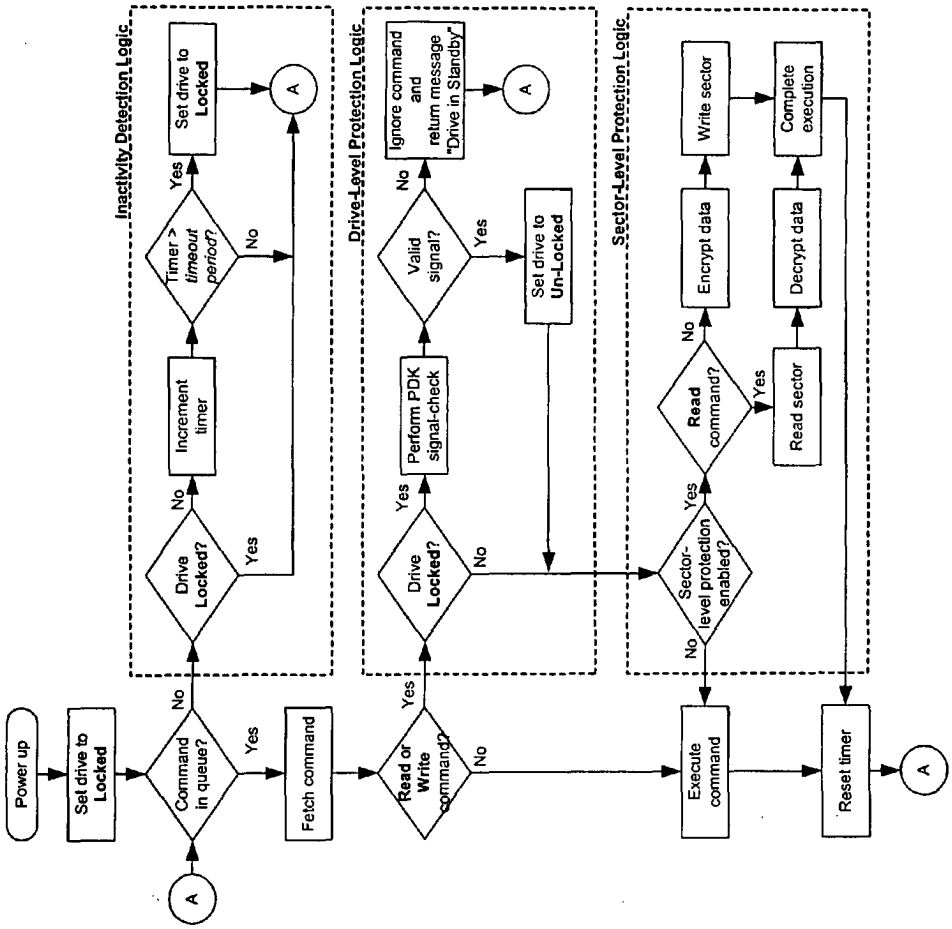

Power up
Set drive to Locked
Command in queue?
No
Yes
A
Fetch command
Inactivity Detection Logic
Drive Locked?
No
Yes
Increment timer
Timer > timeout period?
Yes
No
Set drive to Locked
A
Drive-Level Protection Logic
Read or Write command?
Yes
No
Drive Locked?
Yes
No
Perform PDK signal-check
Valid signal?
No
Yes
Ignore command and return message "Drive in Standby"
A
Set drive to Un-Locked
Sector-Level Protection Logic
Execute command
Sector-level protection enabled?
No
Yes
Read command?
No
Yes
Encrypt data
Write sector
Read sector
Decrypt data
Complete execution
Reset timer
A

FIG. 13

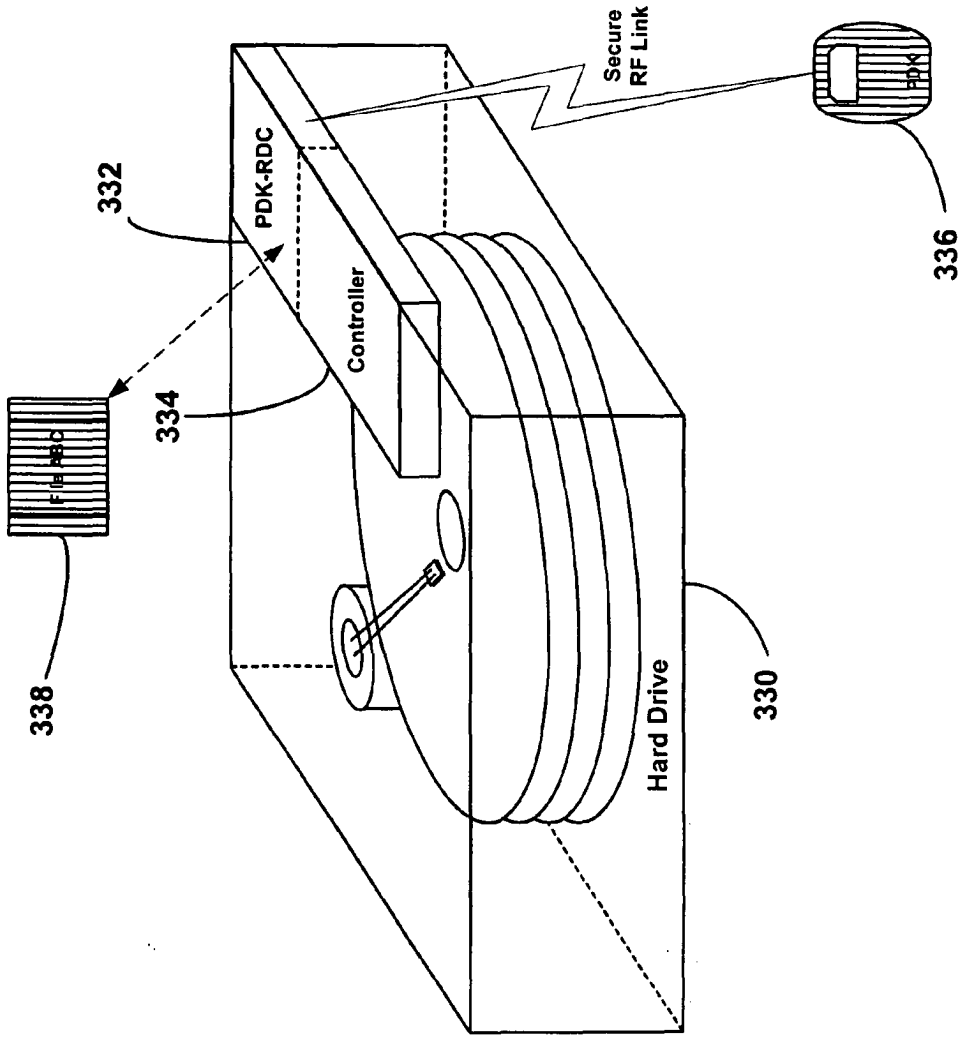

332
PDK-RDC
Controller
334
338
Secure
RF Link
PDK
336
Hard Drive
330

FIG. 14

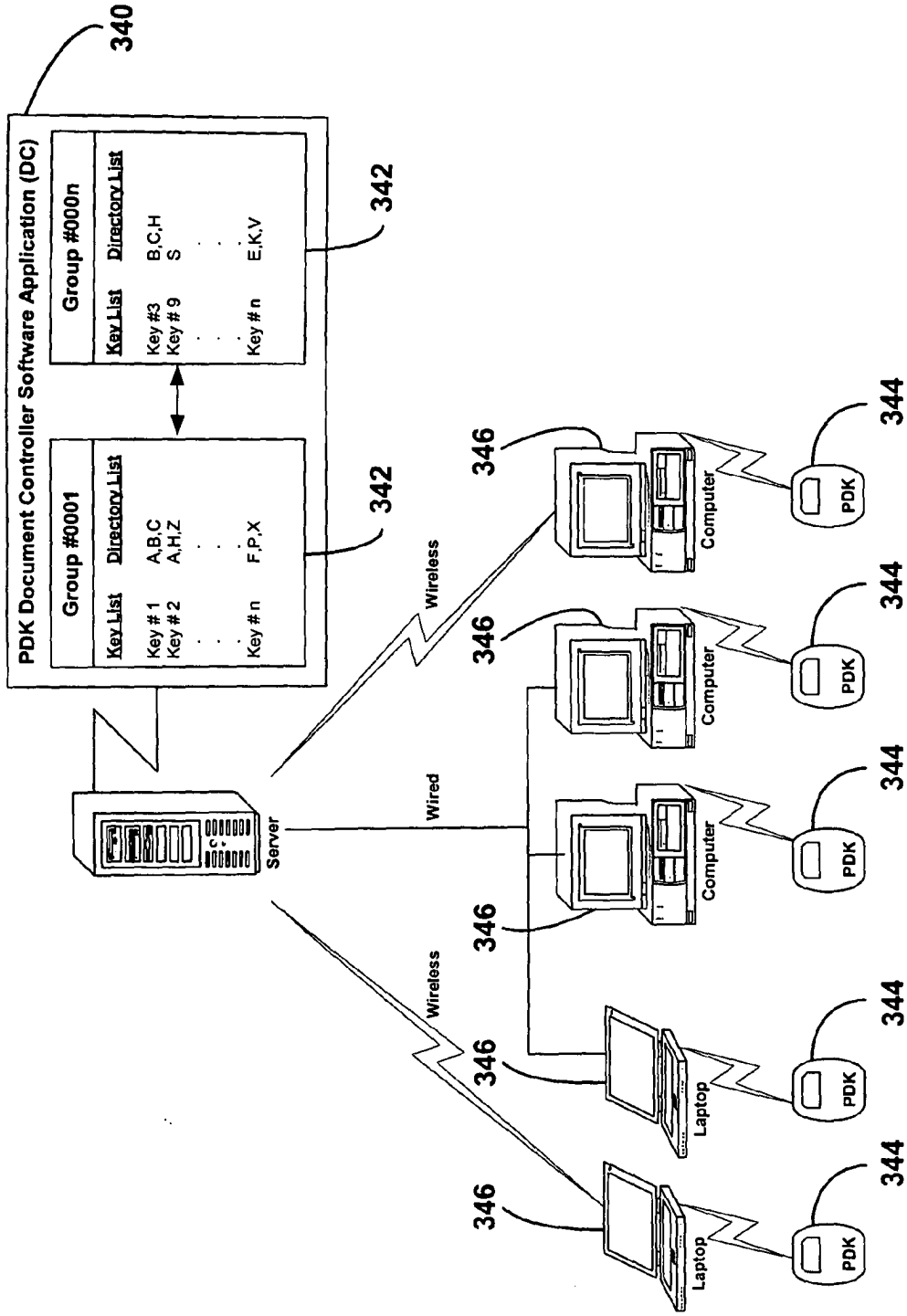

340
PDK Document Controller Software Application (DC)
Group #0001
Key List
Directory List
Key # 1
A,B,C
Key # 2
A,H,Z
Key # n
F,P,X
Group #000n
Key List
Directory List
Key #3
B,C,H
Key # 9
S
Key # n
E,K,V
342
342
Server
Wireless
Wired
Wireless
346
346
346
346
346
Laptop
Laptop
Computer
Computer
Computer
PDK
PDK
PDK
PDK
PDK
344
344
344
344
344

FIG. 15

DIGITAL CONTENT SECURITY SYSTEM

REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of U.S. patent application Ser. No. 10/715,035 filed Nov. 17, 2003, which is a continuation-in-part of U.S. patent application Ser. No. 10/153,979 filed May 23, 2002, which is a continuation-in-part of U.S. patent application Ser. No. 09/750,487 filed Dec. 27, 2000 and Ser. No. 10/016,857 filed Dec. 14, 2001, all of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] 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

[0003] 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.

[0004] 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.

[0005] 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.

[0006] 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.

[0007] 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.

[0008] 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.

[0009] 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

[0010] 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

[0011] 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:

[0012] **FIG. 1** is a flow chart of a method of managing digital rights in accordance with the present invention;

[0013] **FIGS. 2, 3**, and **4** are block diagrams of portions of a DRM system for implementing the method in **FIG. 1**;

[0014] **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;

[0015] **FIG. 6** is a block diagram for implementing a core acquisition option of downloaded content;

[0016] **FIG. 7** is a block diagram for implementing a core acquisition option of store-bought content;

[0017] **FIG. 8** is a block diagram for implementing a core acquisition option of broadcast content;

[0018] **FIGS. 9***a* and **9***b* are block diagrams for implementing a core playback option of stand-alone devices;

[0019] **FIG. 10** is a block diagram for implementing a core playback option of networked devices;

[0020] **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;

[0021] **FIG. 12** is a block diagram for implementing Drive-Level protection and Sector-Level protection in connection with the computer hard drive;

[0022] **FIG. 13** is a flow chart of the logic executed by the PDK-RDC for implementing Drive-Level protection and Sector-Level protection;

[0023] **FIG. 14** is a block diagram for implementing File-Level protection in connection with the computer hard drive; and

[0024] **FIG. 15** is a block diagram for implementing Network-Level protection by expanding File-Level protection to a network environment.

[0025] 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

[0026] 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.

[0027] 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.

[0028] 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**.

[0029] **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**.

[0030] 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.

[0031] 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.

[0032] 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.

[**0033**] 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.

[**0034**] **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**.

[**0035**] 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.

[**0036**] 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.

[**0037**] 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.

[**0038**] **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**.

[**0039**] 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.

[**0040**] 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 802.11b. 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.

[0041] 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.

[0042] 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.

[0043] 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.

[0044] 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.

[0045] 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.

[0046] 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.

[0047] 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):

[0048] identification number of enhanced receiver/decoder circuit used for downloading and transmit-

ted by the receiver/decoder circuit to the key provider's web site at the time of content purchase;

[0049] hour stamp (i.e., the hour in which the content was downloaded; and

[0050] life hours (i.e., number of hours content remains valid, such as perpetual, one hour, 24 hours, 48 hours, etc.).

[0051] 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.

[0052] 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.

[0053] 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.

[0054] 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.

[0055] 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.

[0056] 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.

[**0057**] 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**.

[**0058**] Referring to **FIGS. 9***a* and **9***b* 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.

[**0059**] Referring to the specifics of **FIGS. 9***a* and **9***b*, 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. 9***a*) or a stereo amplifier (**FIG. 9***b*) 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. 9***a* or integrated into the playback device **220** as in **FIG. 9***b*. 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.

[**0060**] 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 hand-held 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.

[**0061**] 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**.

[**0062**] 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.

[**0063**] 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.

[**0064**] 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**.

[**0065**] 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** serves 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 audio-visual 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 **324***c*.

[**0066**] 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**.

[**0067**] 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.

[**0068**] 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.

[**0069**] 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 **324***a* or computer hard disk **324***b* 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.

[**0070**] 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**.

[**0071**] 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.

[**0072**] 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**.

[**0073**] 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).

[**0074**] The PDK-Key and RDC technology is utilized to provide two categories of protection:

[**0075**] 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.

[**0076**] 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.

[**0077**] 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.

[**0078**] 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.).

[**0079**] 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.

[**0080**] **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.

[**0081**] 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.

[**0082**] 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.

[**0083**] 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.

[**0084**] 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** running 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.

[**0085**] 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.

[**0086**] 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.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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.

[0091] 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).

[0092] 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:

[0093] 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).

[0094] 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.

[0095] 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.

[0096] This built-in (firmware-based) PDK-Key configuration/management capability greatly enhances PDK's overall flexibility and ease of setup/use.

[0097] 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.

[0098] 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.

[0099] Each of these embodiments and obvious variations thereof is contemplated as falling within the spirit and scope of the claimed invention, which is set forth in the following claims.

1. A method of securing a storage device, comprising:

detecting a portable, physical 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 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 digital content stored on the storage device 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 link.

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 method 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 method of claim 14, wherein the key associated with the storage device is assigned thereto by a user.

* * * * *