(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2008 (03.01.2008)

PCT

(10) International Publication Number
WO 2008/002916 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2007/072127

(22) International Filing Date: 26 June 2007 (26.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/476,999 27 June 2006 (27.06.2006) US

(71) Applicant *(for all designated States except US)*: **APPLE INC.** [US/US]; 1 Infinite Loop, MS 3-PAT, Cupertino, California 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NOVOTNEY, Donald J.** [US/US]; 1 Infinite Loop, MS 3-PAT, Cupertino, California 95014 (US). **FILSON, John B.** [US/US]; 1 Infinite Loop, MS 3-PAT, Cupertino, California 95014 (US). **TUPMAN, David** [GB/US]; 1 Infinite Loop, MS 3-PAT, Cupertino, California 95014 (US). **LYDON, Gregory T.** [US/US]; 1 Infinite Loop, MS 3-PAT, Cupertino, California 95014 (US).

(74) Agents: **CRETSINGER, Cathy E.** et al.; TOWNSEND and TOWNSEND and CREW LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

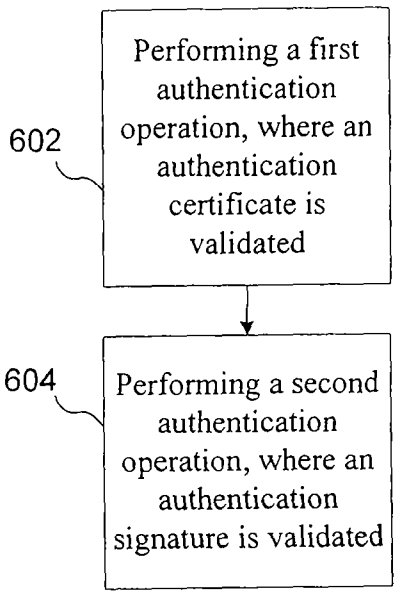
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHOD AND SYSTEM FOR AUTHENTICATING AN ACCESSORY



(57) **Abstract:** A method, system, and connector interface for authenticating an accessory. A method includes performing an authentication operation and allowing the accessory to access the media player during the authentication operation; if the authentication operation fails, the accessory is locked out from any further access to the media player. The authentication operation can include, e.g., validating authentication information included in an authentication certificate provided by the accessory and/or validating a digital signature provided by the accessory. The media player and accessory may utilize a plurality of commands in a variety of environments such as within a connector interface system environment to control access to the media player.

WO 2008/002916 A2

METHOD AND SYSTEM FOR AUTHENTICATING AN ACCESSORY

FIELD OF THE INVENTION

[0001] The present invention relates generally to electrical devices and more particularly to electronic devices such as media players that communicate with accessory devices.

BACKGROUND OF THE INVENTION

[0002] A media player stores media assets, such as audio tracks or photos that can be played or displayed on the media player. One example of a media player is the iPod™ media player, which is available from Apple Inc. of Cupertino, CA. Often, a media player acquires its media assets from a host computer that serves to enable a user to manage media assets. As an example, the host computer can execute a media management application to manage media assets. One example of a media management application is iTunes®, version 6.0, produced by Apple Inc.

[0003] A media player typically includes one or more connectors or ports that can be used to interface to the media player. For example, the connector or port can enable the media player to couple to a host computer, be inserted into a docking system, or receive an accessory device. There are today many different types of accessory devices that can interconnect to the media player. For example, a remote control can be connected to the connector or port to allow the user to remotely control the media player. As another example, an automobile can include a connector and the media player can be inserted onto the connector such that an automobile media system can interact with the media player, thereby allowing the media content on the media player to be played within the automobile.

[0004] Numerous third parties have developed accessories for use with media players. An accessory may be used with the media player as long as a compatible connector or port is utilized. Accessories interact with the media player using an accessory protocol. One example of an accessory protocol is referred to as iPod Accessory Protocol (iAP), which is available from Apple Inc. of Cupertino, CA. The accessory protocol includes commands which have been typically been made freely accessible to accessory developers. A problem with the commands being freely accessible is that they can be used by unauthorized or counterfeit accessory devices.

[0005] One solution is to perform authentication operations on an accessory device. Accordingly, the accessory devices would not have any access to the media player until after the authentication process is complete.

[0006] Thus, there is a need for improved techniques to control the nature and extent to which accessory devices can be utilized with other electronic devices.

BRIEF SUMMARY OF THE INVENTION

[0007] A method, system, and connector interface for authenticating an accessory are disclosed. In one aspect, the method includes performing an authentication operation and allowing the accessory to access the media player during the authentication operation; if the authentication operation fails, the accessory is locked out from any further access to the media player. The authentication operation can include, e.g., validating authentication information included in an authentication certificate provided by the accessory and/or validating a digital signature provided by the accessory.

[0008] According to the system and method disclosed herein, the media player and accessory may utilize a plurality of commands in a variety of environments such as within a connector interface system environment to control access to the media player.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] Figures 1A and 1B illustrate a docking connector in accordance with the present invention.

[0010] Figure 2A is a front and top view of a remote connector in accordance with the present invention.

[0011] Figure 2B illustrates a plug that can be utilized in the remote connector of Figure 2A.

[0012] Figure 2C illustrates the plug of Figure 2B inserted into the remote connector of Figure 2A.

[0013] Figure 3A illustrates connector pin designations for the docking connector.

[0014] Figure 3B illustrates connection pin designations for the remote connector.

[0015] Figure 4A illustrates a typical FireWire connector interface for the docking connector.

[0016] Figure 4B illustrates a reference schematic diagram for an accessory power source.

[0017] Figure 4C illustrates a reference schematic diagram for a system for detecting and identifying accessories for the docking connector.

[0018] Figure 4D is a reference schematic of an electret microphone that may be connected to the remote connector.

[0019] Figure 5A illustrates a media player coupled to different accessories.

[0020] Figure 5B illustrates the media player coupled to a computer.

[0021] Figure 5C illustrates the media player coupled to a car or home stereo system.

[0022] Figure 5D illustrates the media player coupled to a dongle that communicates wirelessly with other accessories.

[0023] Figure 5E illustrates the media player coupled to a speaker system.

[0024] Figure 6 is a flow chart that illustrates a process for controlling access to a media player.

[0025] Figure 7 is a flow chart that illustrates a process for authenticating an accessory.

DETAILED DESCRIPTION OF THE INVENTION

[0026] The present invention relates generally to electrical devices and more particularly to electrical devices such as media players that communicate with accessory devices. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment and the generic principles and features described herein will be readily apparent to those skilled in the art. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

[0027] A method in accordance with the present invention for authenticating an accessory includes performing a first authentication operation on the accessory by the media player, wherein an authentication certificate is validated. In one embodiment, the authentication operations are handled in the background such that the media player is operative to process commands after authentication has begun but before the authentication has completed. This allows the media player and the accessory to interact immediately rather than waiting until

after the authentication process has completed successfully. The method also includes performing a second authentication operation on the accessory by the media player, wherein an authentication signature is validated. In one embodiment, the media player verifies the authentication signature using a public key provided in the certificate. The media player and accessory may utilize a plurality of commands in a variety of environments to facilitate controlling access to the media player. One such environment is within a connector interface system environment such as described in detail hereinbelow.

[0028] Although the authentication of an accessory is described hereinbelow, one of ordinary skill in the art recognizes that the procedures described below may be applied to the authentication of the media player and such application would be within the spirit and scope of the present invention.

Connector Interface System Overview

[0029] To describe the features of the connector interface system in accordance with the present invention in more detail, refer now to the following description in conjunction with the accompanying drawings.

Docking Connector

[0030] Figures 1A and 1B illustrate a docking connector 100 in accordance with the present invention. Referring first to Figure 1A, the keying features 102 are of a custom length 104. In addition, a specific key arrangement is used where one set of keys is separated by one length at the bottom of the connector and another set of keys is separated by another length at the top of the connector. The use of this key arrangement prevents noncompliant connectors from being plugged in and causing potential damage to the device. The connector for power utilizes a Firewire specification for power. The connector includes a first make/last break contact to implement this scheme. Figure 1B illustrates the first make/last break contact 202 and also illustrates a ground pin and a power pin related to providing an appropriate first make/last break contact. In this example, the ground pin 204 is longer than the power pin 206. Therefore, the ground pin 204 would contact its mating pin in the docking accessory before the power pin 206, minimizing internal electrical damage of the electronics of the device.

[0031] In addition, a connector interface system in accordance with the present invention uses universal serial bus (USB), universal asynchronous receiver-transmitter (UART), and Firewire interfaces as part of the same docking connector alignment, thereby making the

design more compatible with different types of interfaces, as will be discussed in detail hereinafter. In so doing, more remote accessories can interface with the media player.

Remote Connector

[0032] The connection interface system also includes a remote connector which provides for the ability to output and input audio, provides I/O serial protocol, and provides an output for video. Figure 2A is a front and top view of a remote connector 200 in accordance with the present invention. As is seen, the remote connector 200 includes a top headphone receptacle 202, as well as a second receptacle 204 for remote devices. Figure 2B illustrates a plug 300 to be utilized in the remote connector. The plug 300 allows the functions to be provided via the remote connector. Figure 2C illustrates the plug 300 inserted into the remote connector 200. Heretofore, all of these features have not been implemented in a remote connector. Therefore, a standard headphone cable can be plugged in, but also special remote control cables, microphone cables, and video cables could be utilized with the remote connector.

[0033] To describe the features of the connector interface system in more detail, please find below a functional description of the docking connector, remote connector and a command set in accordance with the present invention.

Docking and Remote Connector Specifications

[0034] For an example of the connector pin designations for both the docking connector and for the remote connector for a media player such as an iPod™ device by Apple Inc., refer now to Figures 3A and 3B. Figure 3A illustrates the connector pin designations for the docking connector. Figure 3B illustrates the connection pin designations for the remote connector.

Docking Connector Specifications

[0035] Figure 4A illustrates a typical Firewire connector interface for the docking connector. The following are some exemplary specifications: Firewire power (8V – 30V DC IN, 10W Max). In one embodiment, Firewire may be designed to the IEEE 1394 A Spec (400 Mb/s).

USB Interface

[0036] The media player provides two configurations, or modes, of USB device operation: mass storage and media player USB Interface (MPUI). The MPUI allows the media player to be controlled using a media player accessory protocol (MPAP) which will be described in

detail later herein, using a USB Human Interface Device (HID) interface as a transport mechanism.

Accessory 3.3 V Power

[0037] Figure 4B illustrates the accessory power source. The media player accessory power pin supplies voltages, for example, 3.0 V to 3.3V+/-5% (2.85 V to 3.465 V) over the docking connector and remote connector (if present). A maximum current is shared between the docking and remote connectors.

[0038] By default, the media player supplies a particular current such as 5mA. Proper software accessory detection is required to turn on high power (for example, up to 100 mA) during active device usage. When devices are inactive, they must consume less than a predetermined amount of power such as 5mA current.

[0039] Accessory power is grounded through the Digital GND pins.

[0040] Figure 4C illustrates a reference schematic diagram for a system for detecting and identifying accessories for the docking connector. The system comprises a resistor to ground that allows the device to determine what has been plugged into the docking connector. There is an internal pullup on Accessory Identify within the media player. Two pins (Accessory Identify & Accessory Detect) are used.

[0041] Figure 4D is a reference schematic of an electret microphone that may be connected to the remote connector.

[0042] Serial Protocol Communication:

[0043] a) Two pins used to communicate to and from device (Rx & Tx)

[0044] b) Input & Output (0V=Low, 3.3V=High)

[0045] As mentioned previously, media players connect to a variety of accessories. Figures 5A-5E illustrate a media player 500 coupled to different accessories. Figure 5A illustrates a media player 500 coupled to a docking station 502. Figure 5B illustrates the media player 500' coupled to a computer 504. Figure 5C illustrates the media player 500" coupled to a car or home stereo system 506. Figure 5D illustrates the media player 500"'coupled to a dongle 508 that communicates wirelessly with other devices. Figure 5E illustrates the media player 500"" coupled to a speaker system 510. As is seen, what is meant by accessories includes but

is not limited to docking stations, chargers, car stereos, microphones, home stereos, computers, speakers, and accessories which communicate wirelessly with other accessories.

[0046] As mentioned previously, this connector interface system could be utilized with a command set for authenticating an accessory. In one embodiment, the accessory may be a host computer or any other electronic device or system that may communicate with the media player. It should be understood by one of ordinary skill in the art that although the above-identified connector interface system could be utilized with the command set, a variety of other connectors or systems could be utilized and they would be within the spirit and scope of the present invention.

[0047] As described above, accessories interact with the media player using a media player accessory protocol. An example of such a media player accessory protocol is the iPod Accessory Protocol (iAP). The media player accessory protocol refers to the software component executing on the media player that communicates with accessories over a given transport layer. The application of the media player may be, for example, a media player application framework that presents menus/screens to the user. Media player commands are associated with the processing of voice, video, and other data between the media player and the accessory. For example, commands may be associated with read operations and write operations to transfer and store information between the media player and the accessory. Accordingly, in one embodiment, for each command related to the media player, there is a reciprocal command for the accessory. In one embodiment, commands may be grouped and associated with specific accessory functionality.

Command Functionality

[0048] Although a plurality of commands is described hereinbelow, one of ordinary skill in the art recognizes that many other commands could be utilized and their use would be within the spirit and scope of the present invention. Accordingly, the list of commands below is representative, but not exhaustive, of the types of commands that could be utilized to authenticate an accessory. Furthermore, it is also readily understood by one of ordinary skill in the art that a subset of these commands could be utilized by a media player or an accessory and that use would be within the spirit and scope of the present invention. A description of the functionality of some of these commands is described below.

Authentication of an Accessory

[0049] In previous authentication methods, the accessory transmits an identification message to the media player, where the identification message indicates that the accessory supports certain commands and supports authentication. The media player then transmits an acknowledgment message to the accessory. The media player blocks access by the accessory until the entire authentication process completes. The media player may display a "Connecting..." screen. The media player then confirms that the authentication version number that the accessory provides is the correct version number. If so, the media player transmits a challenge to be signed by the device. The media player then validates the authentication signature using a public key based on a device ID from the accessory. The following describes improvements over the previous authentication methods, in accordance with the present invention.

[0050] Figure 6 is a flow chart that illustrates a process for controlling access to a media player in accordance with the present invention. As Figure 6 illustrates, the process begins in step 602 where the media player performs a background authentication operation on the accessory, in which the authentication certificate is validated. More specifically, during the background authentication operation, the accessory transmits authentication information to the media player, and the media player receives and validates the certificate contained in the authentication information. In one embodiment, the authentication information may also include an authentication version number. Authentication certificates are described in more detail below. As described in more detail below, the media player does not wait until the entire authentication process completes but instead allows certain access before the authentication process completes. Next, in step 604, the media player performs a second authentication operation on the accessory, in which an authentication signature is validated. More specifically, during the second authentication operation, the accessory transmits an authentication signature to the media player, and the media player receives and validates the authentication signature. In one embodiment, the media player verifies the authentication signature using a public key. More detailed embodiments of the background authentication and second authentication operations are described below with reference to Figure 7.

[0051] Although the authentication of an accessory is described herein, one of ordinary skill in the art recognizes that the procedures described herein may be applied to the authentication of the media player and such application would be within the spirit and scope

of the present invention. For example, the same or similar steps described in Figure 6 above and/or in Figure 7 below may be utilized by an accessory to authenticate the media player.

Authentication Certificates

[0052] Standard authentication certificates function as containers for data such as the certificate creator (issuer, country, etc.), certificate type, valid certificate date ranges, and other metadata. Authentication certificates, also referred to as certificates or certs, are generated and signed by one or more certificate authorities (CAs) and have a unique serial number. In one embodiment, the certificate may be stored in an authentication coprocessor chip on the accessory. Authentication certificates in accordance with the present invention contain not only the metadata as in a standard authentication certificate but also device class information and a public key, which are described in more detail below.

[0053] As described in more detail below, the media player verifies certificates using a public key that is issued by the CA. The media player may also use the public key to verify a signed challenge. Certificates are used to transfer the public key and other accessory-specific information to the media player. Such accessory-specific information may contain, for example, device class information about the accessory. The device class determines what commands the accessory is permitted to use with respect to the media player. In one embodiment, the media player may add permissible commands to existing classes or add new device classes by means of a media player firmware update. New accessories may be supported by the media player when the CA issues new certificates to the accessory vendor.

[0054] In one embodiment, if a certificate is somehow compromised and cloned in counterfeit devices, the compromised serial number may be added to a certificate revocation list (or CRL) on the media player to prevent devices using the certificate from authenticating successfully. If the certificate parser of the media player does not recognize the cert's device class, the media player rejects the certificate. In one embodiment, a certificate to be used for device authentication may have a preset lifespan (e.g., in the range of 1-5 years, etc.), which may be set, for example, by a date. In one embodiment, certificate expiration could be accomplished by adding device serial numbers to the CRL after the expiration date has passed.

[0055] Figure 7 is a flow chart that illustrates a process for authenticating an accessory in accordance with the present invention. As Figure 7 illustrates, the process begins in step 702 where the media player and accessory exchange messages to determine whether the accessory

supports certain commands and supports immediate authentication. More specifically, in one embodiment, the accessory transmits an identification message to the media player. The identification message includes a device identification (ID) and an indication that the accessory supports certain commands and supports authentication. In some embodiments, support for immediate authentication is required. The media player then transmits an acknowledgment message to the accessory. In one embodiment, the media player notifies the application of the media player that the accessory is attempting to access the media player.

[0056] As described above, in one embodiment, the authentication operations are handled in the background to allow multiple cryptography options (e.g., RSA or SFEE) with/without hardware acceleration to be used. As a result, the media player is operative to process device commands after authentication has begun, before the authentication has completed, and through its successful completion. When device authentication fails (e.g., retry count and/or maximum time has been exhausted), the media player can lockout processing of incoming commands and prevent the device from interacting with media player. Media player applications can permit non-risky device use once authentication has started. Risky behavior is defined as anything that could permanently alter the media player behavior or download unsafe media. Examples of risky behavior to be avoided include download executable media or firmware updates to the media player. If authentication fails at some later point, the application of the media player could cancel any device-related activities and possibly report an error message to the user (e.g., "Device is not supported").

[0057] Referring still to Figure 7, in step 704, during the background authentication operation, the media player transmits an authentication information request to the accessory. In one embodiment, the media player starts a timeout timer. Next, in step 706, the accessory transmits the authentication information to the media player. In one embodiment, the authentication information includes an authentication major version, an authentication minor version, and a public certificate, where the certificate may be divided up into sections if it is large (e.g., greater than 500 bytes). If the certificate is divided up into sections, upon receipt of the authentication information the media player reassembles the certificate. When the certificate is fully assembled, the certificate is parsed for device class information. The media player then converts a class number from the device class information into an allowed command mask. This mask is used to validate that the commands identified by the device are allowed by the certificate. In other words, the media player validates the certificate based at least in part on the device class information.

[0058] Next, in step 708, the media player validates the authentication information. The authentication information may be invalid for a number of reasons. For example, the authentication information may be invalid if the authentication version is not valid, if the public certificate has expired, or if the public certificate is on the certificate revocation list (CRL). If any of the authentication information is invalid, the background authentication operation fails. A failure will restart the authentication process (if a retry count and timeout limits have not been exceeded). The background authentication operation passes if the authentication version is validated and if the certificate class commands have been determined to match or exceed those requested by an identify command of the media player, and if a certification chain has been verified. In one embodiment, non-risky media player command application functions and command processing are enabled while authentication process continues. In one embodiment, the media player may transmit a message to the accessory indicating a version information status.

[0059] Next, in step 710, during a second authentication operation, the media player transmits an authentication signature request to the accessory. The authentication signature request includes a random nonce/challenge to be signed by the device. The specific nonce/challenge length may vary and will depend on the specific implementation. Next, in step 712, the accessory transmits an authentication signature (i.e., a message with a signed challenge/signature) to the media player. Next, in step 714, upon receipt of the authentication signature, the media player validates the authentication signature (i.e., the signed challenge). In one embodiment, the media player verifies the signed nonce/challenge using a public key based on a device ID from the accessory. In a preferred embodiment, the media player verifies the signed nonce/challenge using a public key from the certificate provided by the accessory.

[0060] In one embodiment, an accessory authentication process is based on a public key/private key system where the accessory has a private key and the media player has the associated public key. The accessory authentication process is closely integrated with accessory protocol commands.

[0061] Before completing the authentication process, the media player transmits an authentication status message to the accessory indicating signature status and authentication process completion. The authentication passes if the media player verifies the authentication

signature. Otherwise, the authentication process fails. If authentication passes, the application of the media player unblocks to allow user access to the device.

[0062] If the authentication process fails, the device port of the media player will lock out the accessory. Also, upon a failure, the media player de-authorizes the accessory to prevent the accessory from utilizing the media player resources. In one embodiment, the media player may also transmit an authentication status to the application of the media player. For example, if the authentication fails, the application of the media player may display a "Connection Failed" message.

[0063] In one embodiment, the authentication operations may utilize a retry count and maximum timeout. Accordingly, in one embodiment, the authentication can also fail if the retry counter or maximum timeout is exceeded. Locking out a port prevents an accessory from simulating a detach or re-identifying in order to reset the authentication retry/timeout counters. In one embodiment, incoming packets may be deleted if a device port authentication state is set to "lockout." This will prevent any locked out device packets from being processed. In one embodiment, if the failure is due to an accessory identifying more commands than allowed by the certificate, the device lockout is not activated at authentication failure and the accessory may be permitted to re-identify.

[0064] A method, system, and connector interface for authenticating an accessory has been disclosed. The method includes performing a first authentication operation on the accessory by the media player, where an authentication certificate is validated. The method also includes performing a second authentication operation on the accessory by the media player, where an authentication signature is validated. According to the system and method disclosed herein, the media player and accessory may utilize a plurality of commands in a variety of environments such as within a connector interface system environment to control access to the media player.

[0065] Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. For example, the present invention can be implemented using hardware, software, a computer readable medium containing program instructions, or a combination thereof. Software written according to the present invention is to be either stored in some form of computer-readable medium such as memory or CD-ROM, or is to be

transmitted over a network, and is to be executed by a processor. Consequently, a computer-readable medium is intended to include a computer readable signal, which may be, for example, transmitted over a network. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

WHAT IS CLAIMED IS:

1. A method usable by a media player to interact with accessory, the method comprising:

executing an authentication operation to authenticate the accessory;

during the authentication operation, allowing the accessory to access the media player;

determining whether the authentication operation completed successfully or failed;

in the event that the authentication operation completed successfully, continuing to allow the accessory to access the media player; and

in the event that the authentication operation failed, locking out the accessory from any further access to the media player.

2. The method of claim 1 wherein executing the authentication operation includes:

obtaining an authentication certificate from the accessory; and

validating authentication information included in the authentication certificate.

3. The method of claim 2 further comprising:

receiving a device identification message from the accessory, the device identification message including an indication of a command set supported by the accessory;

determining an allowed command set for the accessory based on the authentication information included in the authentication certificate; and

comparing the allowed command set to the supported command set,

wherein the authentication operation fails in the event that the allowed command set does not match the supported command set.

4. The method of claim 2 wherein executing the authentication operation further comprises:

transmitting a digital signature request to the accessory, the digital signature request including a random challenge;

receiving from the accessory a digitally signed version of the random challenge; and

validating the digital signature.

5. The method of claim 4 wherein the digitally signed version of the random nonce is signed by the accessory using a private key and wherein validating the digital signature includes:

extracting a public key from the authentication certificate; and

using the public key to validate the digital signature.

6. The method of claim 1 further comprising:

receiving a device identification message from the accessory, the device identification message including an indication of a command set supported by the accessory,

wherein during the authentication operation, the accessory is allowed to access the media player using any of the commands in the command set supported by the accessory.

7. The method of claim 1 further comprising:

receiving a device identification message from the accessory, the device identification message including an indication of a command set supported by the accessory, wherein the command set includes a first command that relates to a risky behavior and a second command that relates to a non-risky behavior,

wherein during the authentication operation, the accessory is allowed to access the media player using the second command but not allowed to access the media player using the first command.

8. The method of claim 1 wherein determining whether the authentication operation completed successfully or failed includes:

detecting when a timeout period measured from a starting time of the authentication operation ends,

wherein the authentication operation fails in the event that the authentication operation does not complete successfully before the timeout period ends.

9. The method of claim 8 wherein executing the authentication operation includes:

in the event that an error occurs during the authentication operation, retrying the authentication operation if the timeout period has not ended.

10. The method of claim 9 wherein retrying the authentication includes updating a count of retries and wherein the authentication operation fails in the event that the count of retries exceeds a retry limit.

11. The method of claim 1 further comprising:

in the event that the authentication operation fails, generating a notification for a user.

12. The method of claim 11 wherein the notification includes a message displayed on a display screen of the media player.

13. A method usable by an accessory to interact with a media player, the method comprising:

executing an authentication operation to authenticate the media player;

during the authentication operation, allowing the media player to access the accessory;

determining whether the authentication operation completed successfully or failed;

in the event that the authentication operation completed successfully, continuing to allow the media player to access the accessory; and

in the event that the authentication operation failed, locking out the media player from any further access to the accessory.

14. A media player comprising:

a storage device configured to store media assets;

a control module configured to execute at least one application for accessing the stored media assets;

an interface configured to exchange commands and associated data with an accessory; and

a command module coupled to the interface and the control module and configured to operate the interface to exchange commands and data with the accessory,

wherein the commands exchanged with the accessory include one or more authentication commands usable in an authentication operation to authenticate the accessory and one or more application commands usable to control execution of at least one of the applications by the control module, and

wherein the command module is configured to deliver application commands to the control module while the authentication operation is in progress and to cease delivering application commands to the control model in the event that the authentication operation ends in failure to authenticate the accessory.

15. The media player of claim 14 wherein the authentication commands include:

a command from the media player to the accessory requesting an authentication certificate; and

a command from the accessory to the media player returning the authentication certificate.

16. The media player of claim 15 wherein the authentication commands further include:

a command from the media player to the accessory requesting that the accessory digitally sign a random challenge, wherein the random challenge is provided as data associated with the command; and

a command from the accessory to the media player returning the digitally signed random challenge.

17. The media player of claim 14 wherein the command module is further configured to delete any application commands received from the accessory in the event that the authentication operation ends in failure to authenticate the accessory.

18. The media player of claim 14 wherein the command module is further configured to signal the control module to cancel processing of an application command received from the accessory during the authentication operation, wherein processing is canceled in the event that the authentication operation ends in failure to authenticate the accessory.

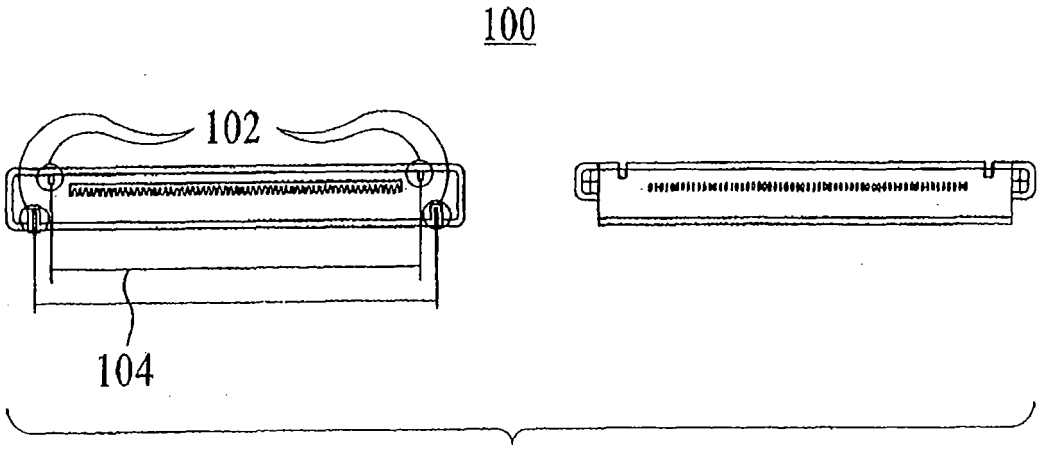


FIG.1A

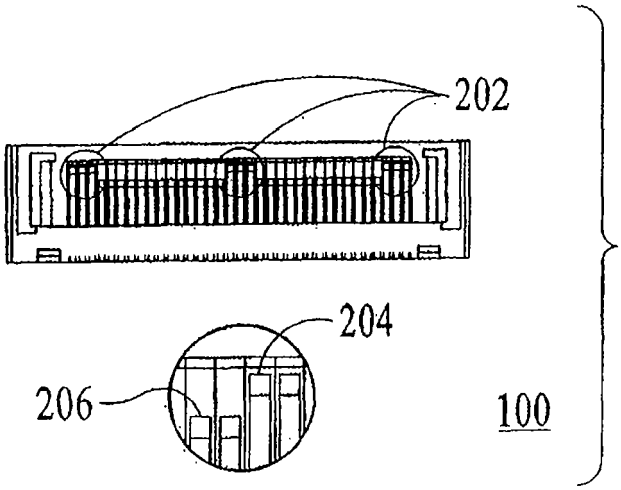


FIG.1B

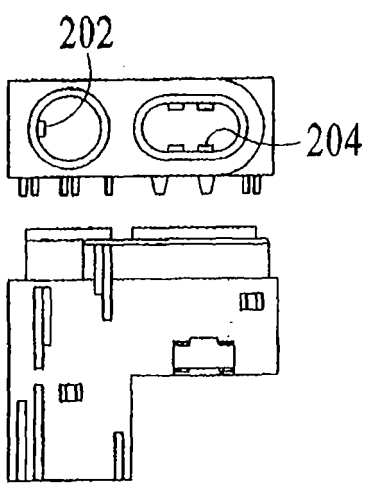


FIG.2A

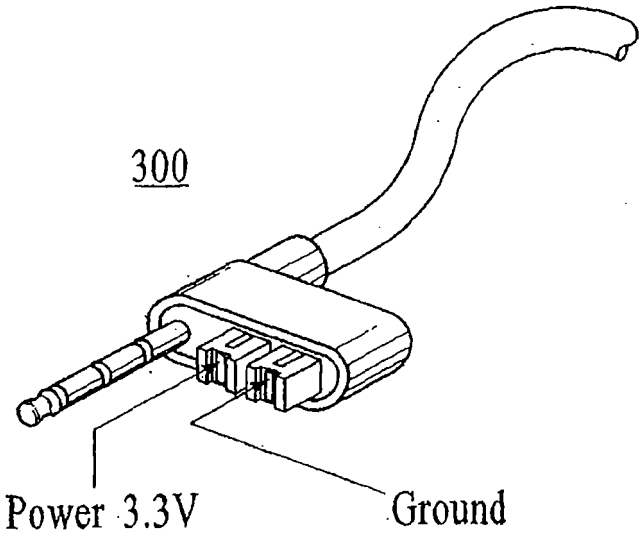


FIG.2B

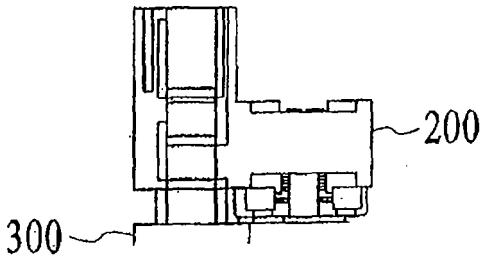


FIG.2C

PIN	Signal Name	I/O	Function
1	DGND	GND	Digital Ground
2	DGND	GND	Digital Ground
3	TPA+	I/O	FireWire signal
4	USB D+	I/O	USB signal
5	TPA-	I/O	FireWire signal
6	USB D-	I/O	USB signal
7	TPB+	I/O	FireWire signal
8	USB PWR	I	USB power in; used to detect USB hub
9	TPB-	I/O	FireWire signal
10	Accessory Identify	I	Connection for accessory identification resistor
11	F/W PWR+	I	Firewire and charger input power (8V to 15V dc)
12	F/W PWR+	I	Firewire and charger input power (8V to 15V dc)
13	Accessory Pwr	O	Nominal 3.3V output; current limited to 100 mA
14	Reserved		
15	DGND	GND	Digital Ground
16	DGND	GND	Digital Ground
17	Reserved		
18	RX	I	Serial protocol input to media player
19	TX	O	Serial protocol output from media player
20	Accessory Detect	I	Connection for accessory identification resistor
21	S Video Y	O	Luminance component for S-video
22	S Video C	O	Chrominance component for S-video
23	Composite Video	O	Composite video signal
24	Remote sense	I	Detect remote
25	LINE-IN L	I	Line level input for left audio channel
26	LINE-IN R	I	Line level input for right audio channel
27	LINE-OUT L	O	Line level output to left audio channel
28	LINE-OUT R	O	Line level output to right audio channel
29	Audio Return	---	Signal, not to be grounded in accessory
30	DGND	GND	Digital ground
31	Chassis		Chassis ground for connector shell
32	Chassis		Chassis ground for connector shell

FIG. 3A

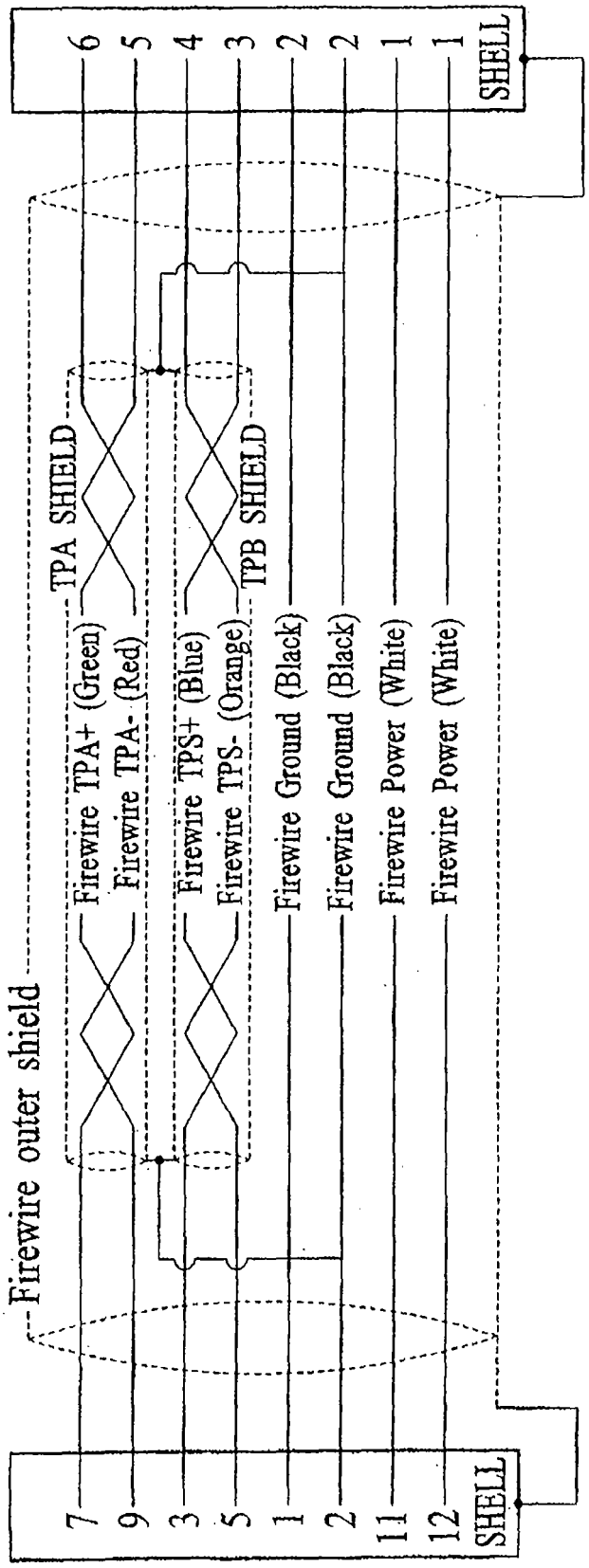

Firewire outer shield
TPA SHIELD
TPB SHIELD
Firewire TPA+ (Green)
Firewire TPA- (Red)
Firewire TPS+ (Blue)
Firewire TPS- (Orange)
Firewire Ground (Black)
Firewire Ground (Black)
Firewire Power (White)
Firewire Power (White)
SHELL
SHELL
7
9
3
5
1
2
11
12
6
5
4
3
2
2
1
1

FIG.4A

Pin	Signal name	I/O	Function
1	Audio Out Left / Mono Mic In	I/O	30mW audio out left channel, also doubles as mono mic in
2	HP Detect	I	Internal Switch to detect plug insertion
3	Audio Return	GND	Audio return for left and right audio
4	Audio Out Right	O	30mW audio out right channel
5	Composite Video	O	Video Signal
6	Accessory 3.3V	O	3.3V Accessory power 100mA max
7	Tx	O	Serial protocol (Data from iPod to Device)
8	Rx	I	Serial protocol (Data to iPod from Device)
9	D GND	GND	Digital ground for accessory

FIG.3B

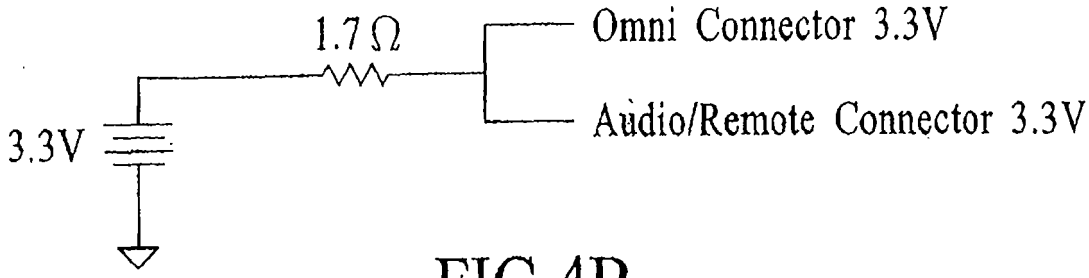


FIG.4B

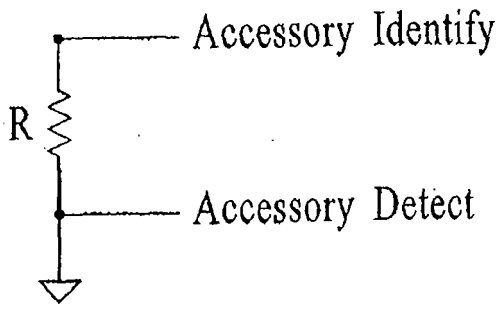


FIG.4C

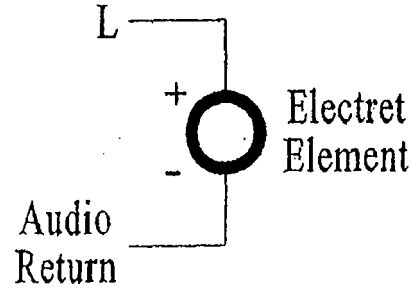


FIG.4D

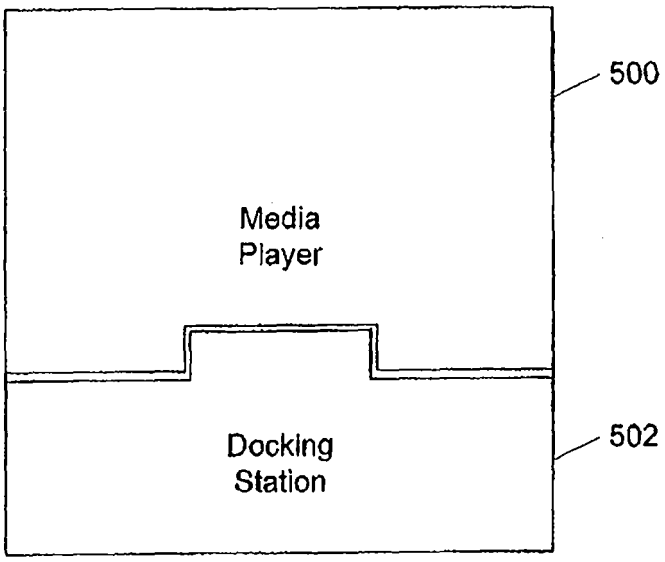


Fig. 5A

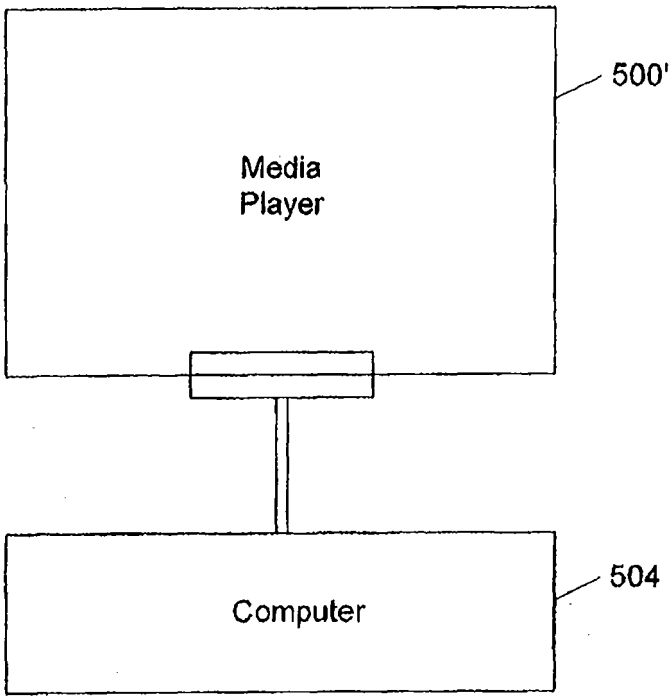


Fig. 5B

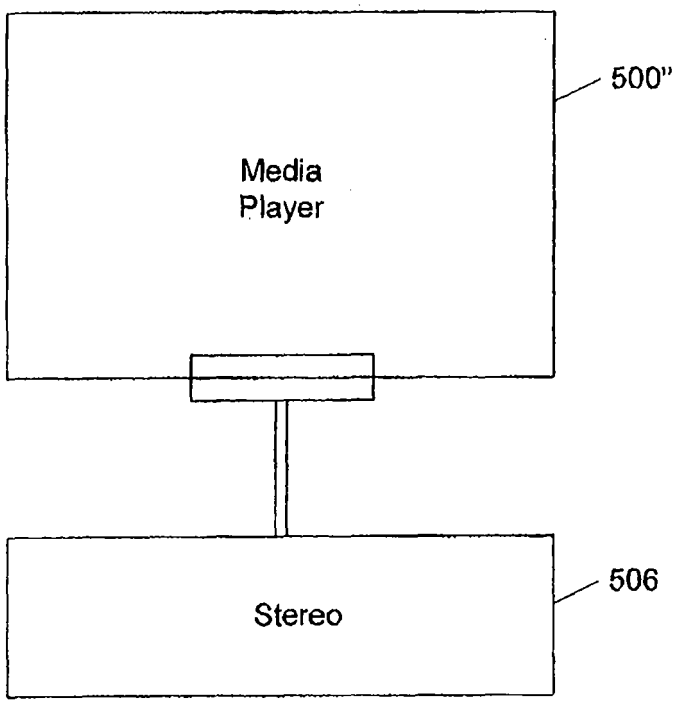


Fig. 5C

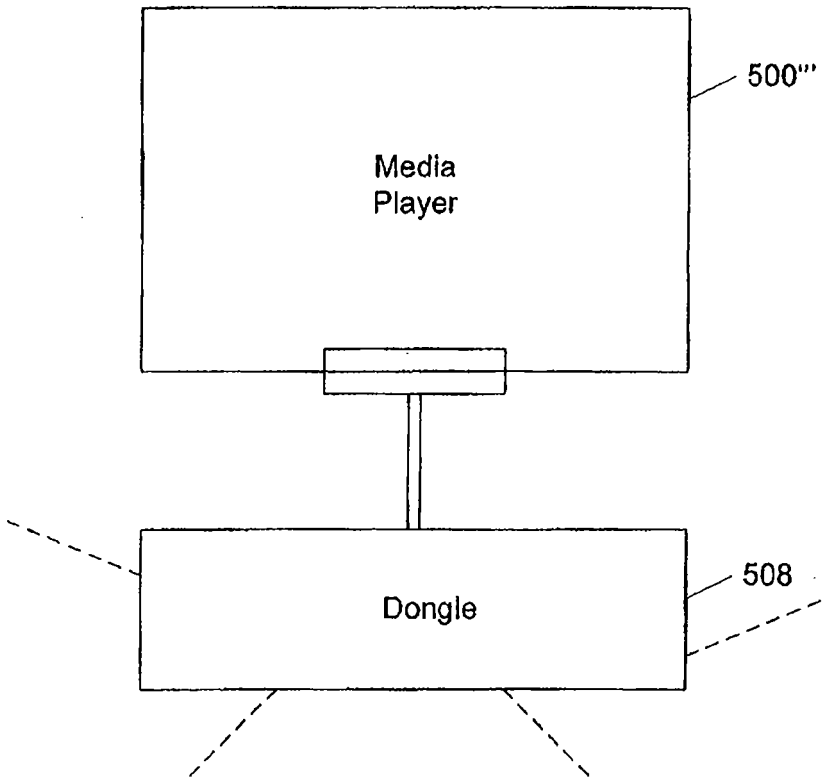


Fig. 5D

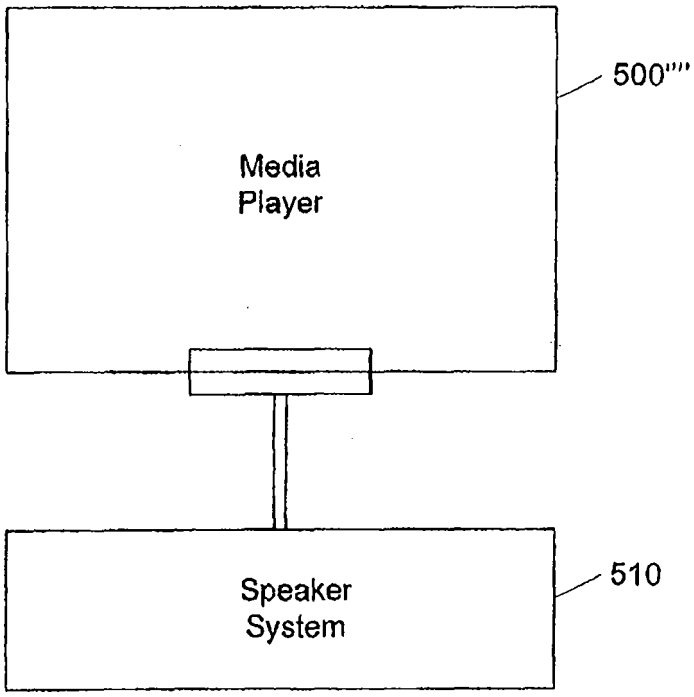


Fig. 5E

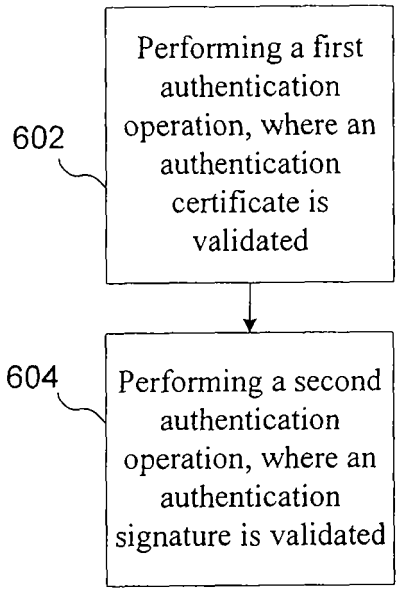

602
Performing a first authentication operation, where an authentication certificate is validated
604
Performing a second authentication operation, where an authentication signature is validated

FIG. 6

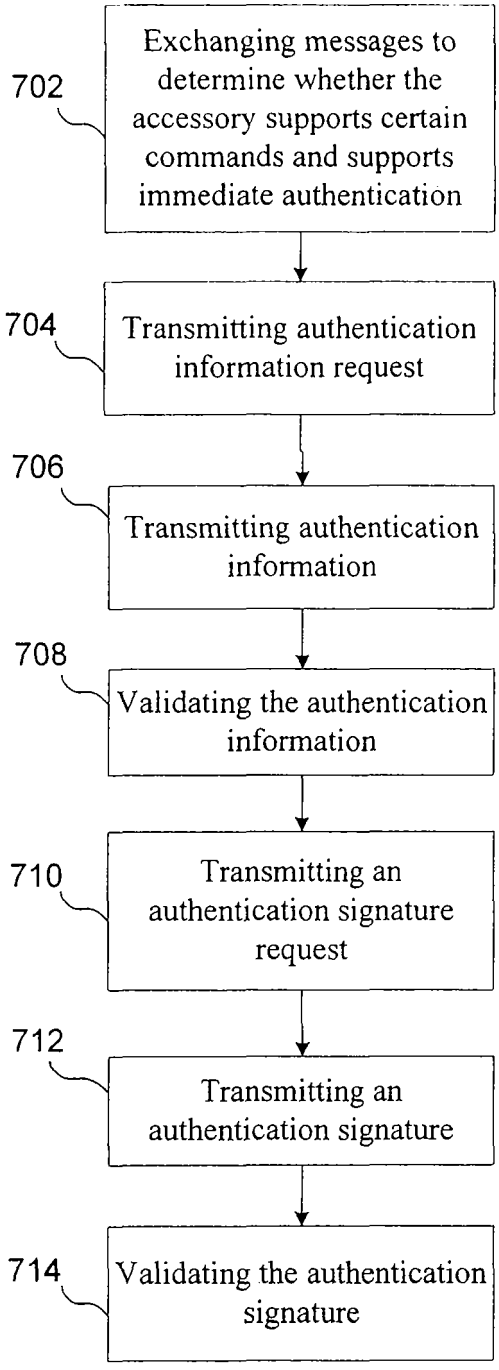

702
Exchanging messages to determine whether the accessory supports certain commands and supports immediate authentication
704
Transmitting authentication information request
706
Transmitting authentication information
708
Validating the authentication information
710
Transmitting an authentication signature request
712
Transmitting an authentication signature
714
Validating the authentication signature

FIG. 7