



- (51) International Patent Classification:
B60R 25/10 (2006.01) *B60R 25/34* (2013.01)
- (21) International Application Number:
PCT/US2018/016610
- (22) International Filing Date:
02 February 2018 (02.02.2018)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/454,462 03 February 2017 (03.02.2017) US
- (71) Applicant: FASETTO, LLC [US/US]; 1401 Tower Avenue, Suite 307, Superior, WI 54880 (US).
- (72) Inventors: CHRISTMAS, Coy; P.O. Box 2036, Superior, WI 54880 (US). MALPASS, Luke; 156 Bagnall Road, Stoke On Trent ST2 7LW (GB).
- (74) Agent: ASHCRAFT, Damon, A.; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren Street, Phoenix, AZ 85004-2202 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— with international search report (Art. 21(3))

(54) Title: SYSTEMS AND METHODS FOR DATA STORAGE IN KEYED DEVICES

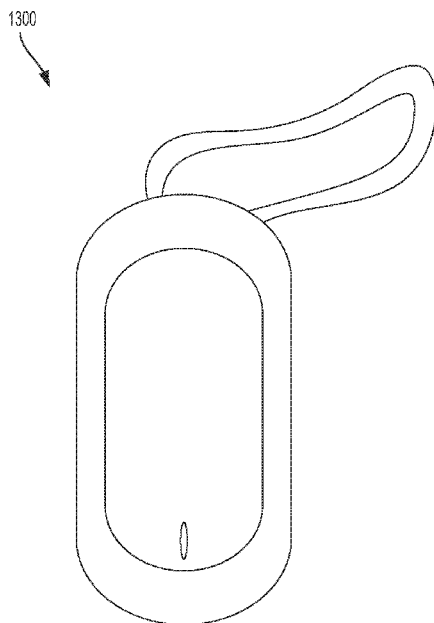


FIG. 13

(57) Abstract: A content storage system integrates with locking, engine, and other control systems in a vehicle. The system includes a portable storage device comprising a processor, a storage module in electronic communication with the processor, and a wireless communication module. A wireless device is in electronic communication with the wireless communication module of the portable storage device. A transponder is installed in a vehicle configured to transmit a signal on a wire. The wireless device detects the signal on the wire from the transponder and stores the signal. The wireless device is transmits the signal on the wire in response to a command from the portable storage device.



Title: **SYSTEMS AND METHODS FOR DATA STORAGE IN KEYED DEVICES**

Inventors: Coy Christmas
Luke Malpass

5 **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority to, and the benefit of, U.S. Provisional Patent Application No. 62/454,462 filed on February 3, 2017 entitled “SYSTEMS AND METHODS FOR DATA STORAGE IN KEYED DEVICES.” The content of the foregoing application is hereby incorporated by reference for all purposes.

10 **FIELD**

[0002] The present disclosure generally relates to portable storage devices, and more particularly to systems and methods for integrating data storage into keyed devices.

BACKGROUND

15 [0003] Communication between devices is typically performed over a network, such as the internet or a local area network. However, networks may not always be available for communication between devices and additionally may expose communications to security breaches on the network. Devices enabled with Bluetooth® may communicate directly. However, Bluetooth® enabled devices must be within a limited range, and communication
20 speeds may be relatively slow. Consumers may have files stored on one device and wish to access the files from another device. It may be difficult to transfer the file without an internet connection or using data on a data plan. Additionally, transferring the information may expose the information to hackers and security breaches.

[0004] Carrying storage devices can also be cumbersome even without concerns regarding
25 data transfer. Most people are conditioned to check for a few items such as their keys, wallets, and phones when leaving a location. But USB sticks, for example, are easily misplaced and left behind. Losing storage devices is a security risk in addition to being inconvenient. Physical copies of data retained on a storage device get exposed when the device is recovered by a third party.

30 [0005] Motor vehicles, particularly older vehicles, have limited computing capacity. Electronic control units (ECUs) age and may not have processing power suitable to support modern electronic conveniences. Older ECUs may thus not provide, for example, traction

control, automatic braking, engine performance programming, or other operations dependent on processing power. Additionally, as ECUs and other controllers in the vehicle age there is limited capacity to upgrade an ECU.

SUMMARY

5 [0006] A content storage system integrates with locking, engine, and other control systems in a vehicle. The system includes a portable storage device comprising a processor, a storage module in electronic communication with the processor, and a wireless communication module. A wireless device is in electronic communication with the wireless communication module of the portable storage device. A transponder is installed in a vehicle configured to transmit a
10 signal on a wire. The wireless device detects the signal on the wire from the transponder and stores the signal. The wireless device transmits the signal on the wire in response to a command from the portable storage device.

[0007] In certain embodiments, the content storage system described herein is meant to incorporate the system set forth and described in U.S. Patent Application Serial No. 14/745,100
15 entitled "System and Methods for Portable Storage Devices" filed on June 19, 2015 which is incorporated by reference in its entirety.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] A more complete understanding may be derived by referring to the detailed description and claims when considered in connection with the Figures, wherein like reference
20 numbers refer to similar elements throughout the Figures, and:

[0009] FIG. 1 illustrates a schematic diagram of a system for transmitting messages according to various embodiments of the disclosure;

[0010] FIG. 2 illustrates a process for transmitting data between devices according to various
embodiments;

25 [0011] FIG. 3 illustrates a process for a file send protocol according to various embodiments;

[0012] FIG. 4 illustrates a discovery protocol according to various embodiments;

[0013] FIG. 5 illustrates a definition for a discovery protocol according to various
embodiments;

[0014] FIG. 6 illustrates a definition for a file transfer request according to various
30 embodiments;

[0015] FIG. 7 illustrates a definition for a response to a file transfer request according to
various embodiments;

[0016] FIG. 8 illustrates a portable storage device according to various embodiments;

[0017] FIG. 9 illustrates a portable storage device communicating with a device according to various embodiments;

[0018] FIG. 10 illustrates a portable storage device syncing with a server according to various embodiments;

5 [0019] FIG. 11 illustrates a portable storage device operable to interface with electronics systems in a motor vehicle according to various embodiments;

[0020] FIG. 12 illustrates an electronic key system having a portable storage device configured to monitor and/or control electronic systems in a motor vehicle according to various embodiments; and

10 [0021] FIG. 13 illustrates an electronic key fob having a portable storage device configured to monitor and/or control electronic systems in a motor vehicle according to various embodiments.

DETAILED DESCRIPTION

[0022] The detailed description of exemplary embodiments herein makes reference to the accompanying drawings and pictures, which show various embodiments by way of illustration. While these various embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the disclosure. Thus, the detailed description herein is presented for purposes of illustration only and not of limitation. For example, the steps recited in any of the method or process descriptions may be executed in any order and are not limited to the order presented. Moreover, any of the functions or steps may be outsourced to or performed by one or more third parties. Furthermore, any reference to singular includes plural embodiments, and any reference to more than one component may include a singular embodiment.

25 [0023] The present disclosure relates to systems, methods, and computer program products. In the detailed description herein, references to “various embodiments,” “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to implement such feature, structure, or characteristic in

30

connection with other embodiments whether or not explicitly described. After reading the description, it will be apparent to one skilled in the relevant art(s) how to implement the disclosure in alternative embodiments.

[0024] Systems and methods are disclosed herein for communication between a portable content repository and computing devices. A portable storage device may serve as a content repository by retaining content for access by other devices. Various computing devices may read, write, and/or execute content stored on the portable storage device. Although the portable storage device may “permanently” store the content, the various computing devices accessing content on the portable storage device retain the content temporarily and/or with access controls in place. The portable storage device may thus be described as a content repository device. Content repository devices of the present disclosure may use a standardized communication system (“SCS”) as described herein.

[0025] The systems and methods disclosed herein may enable communication between devices without connection to the Internet or other networks using an SCS. A standardized communication system (“SCS”) may be operable on the computing devices of the present disclosure. The SCS may comprise any combination of hardware and/or software. The SCS may utilize existing physical components of the device, such as 802.11 or 802.2(2) wireless chips and Bluetooth® systems in order to communicate with other devices. The SCS may be suitable for any communication protocol, such as IP, TCP/UDP, Bluetooth®, raw Manchester encoding, and any other form of wireless communication.

[0026] The SCS may allow communication between devices of varying types and platforms. Additionally, as communication may be directly between devices without transmitting data across a network, communication may be available when networks are unavailable, and communications may be protected from eavesdroppers on a network. Furthermore, direct communication between devices may avoid data charges on cellular data plans.

[0027] Referring to FIG. 1, a system 100 for transmitting messages is illustrated according to various embodiments. A first device 110 comprising an SCS 112 and a second device 120 comprising an SCS 122 are illustrated according to various embodiments. In various embodiments, SCS 112 and SCS 122 may be aftermarket software programs installed on first device 110 and second device 120. For example, a user may download an SCS app onto a smartphone or other device. However, in various embodiments, SCS 112 and SCS 122 may be embedded into a chip, such as an 802.11 wireless chip, in first device 110 and/or second device 120.

[0028] In various embodiments, the SCS may implement a standardized communication protocol (“SCP”) on a device. SCP may attach an SCP header 152 to a packet in order to identify a datagram 150 as an SCP datagram. First device 110 may communicate with second device 120 via SCP. The SCS may recognize the SCP header and may follow the SCP. The SCP may define the ability for devices to discover one another, to request the transfer of raw data, to transmit confirmations on receipt of data, and to perform any other steps involved with transmitting data.

[0029] In various embodiments, the SCS may be implemented at the network layer in the Open Systems Interconnection (“OSI”) model (or the Internet layer in the TCP/IP model). Regardless of the protocol being used at the transport layer (e.g. TCP, UDP, SCTP, DCCP), the SCP header may allow devices comprising an SCS to communicate via SCP.

[0030] In various embodiments, at least one of first device 110 and second device 120 may comprise a smartphone. However, in various embodiments, first device 110 and second device 120 may comprise any type of device capable of transmitting and/or receiving data.

[0031] Referring to FIG. 2, a process 200 for transmitting data between devices is illustrated according to various embodiments. In various embodiments, a first user may wish to transmit data from first device 110 to second device 120. The data may comprise any type of data, such as a text message, image, video, text document, or any other type of file.

[0032] First device 110 may discover available devices (step 210). First device 110 may attempt to discover other devices by a variety of methods. In various embodiments, first device 110 may discover other devices via a camera or other optical device. In various embodiments, second device 120 may display a symbol, such as a QR-code, a barcode, or text. The symbol may comprise identifying characteristics about second device 120. For example, in various embodiments the identifying characteristics may comprise at least one of a device name, an IP address of the device, an owner name, an endpoint of the device, and the available transport layers on the device. First device 110 may scan the symbol using a camera. First device 110 may obtain the identifying characteristics from the symbol and use the identifying characteristics in order to transmit data to second device 120.

[0033] In various embodiments, the SCS on first device 110 may search for other devices using a wireless chip in first device 110. Devices comprising an SCS may transmit a broadcast message. The broadcast message may comprise the identifying characteristics of the device. In various embodiments, first device 110 may be within transmission range of second device 120. The transmission range may depend on the specific type of wireless chips in first device 110 and

second device 120. However, in various embodiments, the transmission range may be up to about 200 feet – 300 feet. The SCS may open a socket on first device 110 to listen for broadcast messages. The broadcast message may be sent by a variety of hardware. For example, the broadcast message may be transmitted via an 802.11 wireless chip, Bluetooth® chip, or NFC.

5 [0034] In various embodiments, first device 110 and second device 120 may not be within transmission range of each other. However, an intermediary device, such as a smartphone equipped with hotspot technology, may be within transmission range of first device 110. First device 110 may search for available devices by transmitting a message to intermediary device, instructing intermediary device to look for available devices. Intermediary device may receive a
10 broadcast message from second device 120, and intermediary device may transmit the broadcast message to first device 110. Thus, first device 110 may discover second device 120 without connecting to the internet or a cellular network even though first device 110 may not be within transmission range of second device 120. In various embodiments, any number of intermediary devices may be daisy-chained, such that first device 110 may discover second device 120 from
15 miles apart by transmitting data via a series of intermediary devices.

[0035] First device 110 may display a list of all discovered devices to the user. The user may select second device 120 in order to transmit data to second device 120. The user may select a file or message to be transmitted to second device 120.

[0036] The SCS 112 on first device 110 may determine the transmission hardware to utilize
20 for the transmission (step 220). In various embodiments, first device 110 and second device 120 may each have only one type of transmission hardware, such as an 802.11 wireless chip, and the SCS 112 may thus select the 802.11 wireless chip to transmit the data. However, in various embodiments, multiple transmission paths may be available between first device 110 and second device 120. For example, first device 110 and second device 120 may each comprise an 802.11
25 wireless chip and a Bluetooth® chip. In various embodiments, the SCS 112 may determine the fastest transmission path, and may select the fastest transmission path to transmit the data. In various embodiments, the transmission path may be selected by default settings. For example, SCS 112 may always select an 802.11 wireless path for transmission when available, and if the 802.11 wireless path is not available, SCS 112 may select a Bluetooth® path. However, in
30 various embodiments, the SCS 112 on first device 110 may transmit a speed test message to second device 120 via each available transmission path, and the SCS 112 may select the fastest transmission path based on the speed test results.

[0037] In various embodiments, the SCS 112 may instruct first device 110 to send the data to second device 120 via multiple transmission paths. A message may be divided into multiple packets. SCS 112 may analyze the available transmissions paths, and send the message over multiple transmission paths in order to expedite transmission of the entire message. For example, SCS 112 may determine that the fastest method of transmitting the message may be to transmit 90% of the packets via an 802.11 wireless path, and 10% of the packets over a Bluetooth® path. SCS 112 may attach an SCP header to each packet being transmitted to second device 120, whether via 802.11 wireless or Bluetooth®. Thus, SCS 122 on second device 120 may recognize the packets as being received by SCP, and SCS 122 may reassemble the packets in order to recreate the entire message. In various embodiments, SCS 112 may analyze all transmission paths available, including but not limited to multiple 802.11 wireless chips, Bluetooth® chips, NFC, PDQ, or any other transmission paths in order to select the fastest transmission method. The SCS on first device 110 may initiate a file send protocol and transmit the data to second device 120 (step 230).

[0038] In various embodiments, first device 110 and second device 120 may be connected to the same local network. First device 110 may transmit a link, such as a QR-code, over a cellular network or the local network to second device 120. In various embodiments, the link may comprise 10kb or less of data. Second device 120 may use the link to request or accept a file transfer. First device 110 may transmit a file over the local network. In various embodiments, the file may be transferred using TCP/IP directly over the local network.

[0039] In various embodiments, second device 120 may have access to an internet connection. First device 110 may transmit a link over a cellular transmission path to second device 120, and second device 120 may use the link to download a file stored on the cloud and/or on a server over the internet. In various embodiments, second device 120 may download the file using TCP/IP.

[0040] In various embodiments, first device 110 may sync its contents with a cloud database. In various embodiments, first device 110 may comprise an SCS folder, and only files stored in the SCS folder may be synced with the database. First device 110 may transmit a link over a cellular transmission path to second device 120 identifying a file stored on the database. In various embodiments, second device 120 may not have access to an 802.11 wireless network at the time second device 120 receives the link. Second device 120 may use the link to access the file whenever second device 120 gains access to an 802.11 wireless network in order to prevent cellular data charges. In various embodiments, second device 120 may use the link to access the

file over the cellular network. In various embodiments, second device 120 may stream all or part of the file over either the cellular network or an 802.11 wireless network.

[0041] In various embodiments, first device 110 may share an online folder with second device 120. First device 110 may indicate that second device 120 may have access to an online folder. First device 110 may sync with the online folder to upload files stored on first device 110 to the online folder. Second device 120 may sync with the online folder to download files stored in the online folder to second device 120.

[0042] Referring to FIG. 3, a process 300 for a file send protocol is illustrated according to various embodiments. First device 110 may transmit a request to establish a connection with second device 120 (step 310). In various embodiments the connection may comprise a TCP connection. However, in various embodiments, the connection may comprise any type of connection for transmitting data between devices. Second device 120 may accept the connection request (step 320). In various embodiments, the connection may be between secure sockets on first device 110 and second device 120.

[0043] In various embodiments, first device 110 may transmit a message comprising a cypher book to second device 120 (step 330). The cypher book may comprise a list of one-time cyphers, and may allow second device 120 to decrypt data sent to second device 120 over the secure socket connection using one time cyphers. In various embodiments, first device 110 may encrypt the message comprising the cypher book using known encryption methods, such as Advanced Encryption Standard (“AES”) or RSA encryption. However, subsequent messages during the transfer session may be encrypted using the one-time cyphers contained in the cypher book. The messages encrypted using the one-time cyphers may be encrypted and decrypted using significantly less processing power and time than messages encrypted with AES or RSA. Additionally, the messages sent using the one-time cyphers may be indecipherable to parties not containing the cypher book.

[0044] First device 110 may send a file transfer request (step 340). For an example of a file transfer request, refer to FIG. 5. Second device 120 may accept the file transfer request (step 350). In response to second device 120 accepting the file transfer request, first device 110 may break the file into segments, and begin transmitting the segments to second device 120 (step 360). After first device 110 has transmitted all segments of the file, first device 110 may wait for confirmation that second device 120 has received all segments. Second device 120 may transmit a confirmation message to first device 110 indicating that all segments have been received (step

370). Second device 120 may decrypt and reassemble the segments according to SCP in order to recreate the file (step 380).

[0045] Referring to FIG. 4, an example of a discovery protocol 400 is illustrated according to various embodiments. Discovery protocol 400 may be implemented on the transport layer using TCP/UDP. However, in various embodiments, discovery protocols may be implemented using a Bluetooth® serial port, RS-232, or may be sent entirely over datagrams or a Windows® Socket API (“WSA”). The LocalClient in the illustrated embodiment may be a new instance of an IDiscoveredClient (defined in FIG. 5) class filled in with the device’s identifying characteristics, such as device name, user name, preview image, and endpoint (in this case an IP address and port). First device 110 may open a new socket for a broadcast message (410). First device 110 may transmit the IP address that first device 110 is listening on for a response to the broadcast message (420). First device 110 may open a new datagram socket to listen for a response message (430). After receiving a response message, first device 110 may decipher the response message into the original IDiscoveredClient message that first device 110 sent (440).

[0046] Referring to FIG. 5, a definition for an example discovery protocol 500 is illustrated according to various embodiments. The definition may be a single common class called IDiscoveredClient that may be implemented by a transmitting device and a receiving device. In various embodiments, the definition may be expanded to include custom fields and any other information that users may desire. In various embodiments, the definition may comprise a name of the device (510), an IP address of the device (520), an owner of the device (530), and endpoint of the device (540), and a transport layer on which the device was discovered (550). However, one skilled in the art will appreciate that the particular fields used may be altered to any desired fields.

[0047] Referring to FIG. 6, a definition for an example file transfer request protocol 600 is illustrated according to various embodiments. The definition may be called “IFileTransferRequest.” In various embodiments, the definition may comprise the name of the device transmitting a file (610), the filename to be sent (620), the size of the file (630), the device receiving the file (640), a unique identification for the file transfer (650), and the transport layer associated with the file transfer (660).

[0048] Referring to FIG. 7, a definition for a response to a file transfer request 700 is illustrated according to various embodiments. The receiving device may respond with a definition called IFileTransferResponse to indicate that the receiving device is willing to accept the file transfer. In various embodiments, IFileTransferResponse may comprise the response

from the user (710) and the unique identification for the file transfer (720). The transmitting device may receive the response from the receiving device, and the transmitting device may proceed to transmit the file to the receiving device. Once a complete file transfer has occurred, the receiving device may transmit a confirmation to the transmitting device (730).

5 [0049] Referring to FIG. 8, a portable storage device (“PSD”) 800 is illustrated according to various embodiments. The PSD 800 may be a wearable device, such as a wrist band or bracelet as illustrated in FIG. 8. However, PSDs may be any type of portable device which is capable of storing information. For example, a PSD may comprise a watch, necklace, phone case, smartphone, implanted chips, clothing item, wallet, etc.

10 [0050] The PSD 800 may comprise a storage module 810, a communication module 820, a processor 830, and a battery 840. The storage module 810 may comprise a memory card. For example, the storage module 810 may comprise an SD card, an xD card, a CompactFlash card, or any other suitable memory card. The storage module 810 may comprise an internal memory, such as iSSD, SSD, iNAND, or flash SD. The communication module 820 may comprise one or
15 more components capable of wireless communication. For example, the communication module may comprise an 802.11 or 802.2(2) wireless chip, a Bluetooth® chip, an NFC chip, etc. The processor 830 may comprise any combination of hardware and/or software capable of providing instructions to the storage module 810 and the communication module 820. In various
20 embodiments, the storage module 810, the communication module 820, and the processor 830 may be embedded within the PSD 800, such that the PSD 800 does not have any visible electronic components. In various embodiments, the PSD 800 may comprise a waterproof coating, such as rubber or silicone.

[0051] The PSD 800 may comprise a standard communication system (“SCS”) as previously described herein. The SCS may be any combination of hardware and/or software which is
25 capable of communicating via a standard communication protocol (“SCP”) as previously described herein. In various embodiments, the SCS may be implemented on at least one of the storage module 810, the communication module 820, or the processor 830.

[0052] The PSD 800 may wirelessly receive and transmit files and communications from other devices, such as smartphones, televisions, game consoles, tablets, personal computers,
30 printers, etc. Due to the SCS, the PSD 800 may not be limited to communicating with any particular brand or manufacturer of device. In contrast, the PSD 800 may communicate across platforms, such as with Apple® devices, Android® devices, Windows® devices, UNIX® devices, or any other suitable devices.

[0053] In various embodiments, the PSD 800 may allow a user to access their files wherever the user goes. For example, a user may have a document stored on a laptop computer. The user may transmit the document from the laptop computer to the PSD 800 using the SCS. The PSD 800 may store the document in the storage module 810. The user may then transmit the document from the PSD 800 to another device, such as a smartphone, using the SCS.

[0054] In various embodiments, the PSD 800 may communicate directly with other devices without using a network. Thus, information may be transmitted securely between the PSD 800 and other devices. However, in various embodiments, the PSD 800 may communicate over a network using a wireless chip in the communication module 820. The communication module 820 may comprise two wireless chips, allowing the PSD 800 to simultaneously communicate over a network on a first wireless chip and directly to another device on a second wireless chip.

[0055] In various embodiments, the PSD 800 may allow data to be transferred from a device to the PSD 800 without storing the data on the device. For example, a smartphone may capture a picture and transmit the picture directly to the PSD 800 using the smartphone's RAM without storing the picture on the hard drive of the smartphone. Thus, the smartphone may be lost, stolen, sold, or donated without risk of a third-party obtaining the picture, or other data which is stored on the PSD 800 and not the smartphone. Similarly, a user may initiate an SCS on a device, such as a laptop, and open a file stored on the PSD 800 using the device. The user may edit the file on the device and save the edited file directly on the PSD 800 without saving the edited file on the device.

[0056] A user may use the PSD 800 to store all of the user's files. Regardless of what device a user is using to access the files on the PSD 800, the user may create, edit, and delete files directly on the PSD 800 using another device, such as a personal computer.

[0057] In various embodiments, the PSD 800 may emulate a network drive. Thus, the PSD 800 may be able to communicate with devices which are not capable of downloading or installing custom software. For example, the PSD 800 may emulate a DLNA media service, or a Windows® network. The PSD 800 may require a password to be entered on the device, and the device may then access files stored on the PSD 800.

[0058] Referring to FIG. 9, a PSD 910 and a device 920 comprising an SCS 922 are illustrated according to various embodiments. In various embodiments, the device 920 may be the first device 110 described with reference to FIG. 1. However, the device 920 may comprise any device capable of communicating with the PSD 910 using an SCP. A user may login to the SCS 922, and the device 920 may request an access key. In various embodiments, the device

920 may request the access key from a server over an internet or cellular connection. However, in various embodiments, the PSD 910 may have one or more stored access keys on the PSD 910, and the device 920 may request the stored access key from the PSD 910. The PSD 910 may transmit the stored access key to the device 920, and the device 920 may use the stored access key to encrypt and/or decrypt data transmitted between the device 920 and the PSD 910. In various embodiments, the access key may be a temporary key which may expire after a set amount of time. The user may view the files stored on the PSD 910, and the user may upload or download files between the PSD 910 and the device 920. In various embodiments, the PSD 910 may stream a file, such as an audio or video file, to the device 920. Once a file is stored on the PSD 910, the user may access the file with any device within communication range of the PSD 910. In various embodiments, a file may be streamed cross-platform. For example, a user may purchase an audio file via iTunes® on an Apple® device. The user may transmit the audio file to the PSD 910 using the SCP. The PSD 910 may stream the audio file from the PSD 910 to a non-Apple® device, regardless of the operating system, using the SCP.

[0059] Referring to FIG. 10, a system 1000 for backing up data on a PSD 1010 is illustrated according to various embodiments. The PSD 1010 may establish a connection with a device 1020. In various embodiments, the device 1020 may comprise any type of device capable of communicating with a server 1030. For example, the device 1020 may comprise a personal computer, a smartphone, or a wireless router. The device 1020 may communicate with the server 1030 over a network. In various embodiments, the server 1030 may comprise a cloud computing system.

[0060] The device 1020 may comprise an SCS. The PSD 1010 may communicate with the device 1020 utilizing the SCS. A user may log into the SCS on the device 1020, and instruct the PSD 1010 to sync with the server 1030. The PSD 1010 may transmit any new or edited files to the server 1030 via the device 1020. The files may be associated with a user account and stored on the server 1030. In various embodiments, any new or edited files associated with the user account may be downloaded from the server 1030 and transmitted to the PSD 1010 via the device 1020. Once the PSD 1010 is synced with the server 1030, a user may access a file by either logging into the user account with any device over the internet, or the user may access the file by accessing the PSD 1010 with a device.

[0061] In various embodiments, the PSD 1010 may automatically sync when charging, and may charge wirelessly or on a charging cable. The PSD 1010 may reach a predefined battery level prior to initiating the sync. For example, when placed on a charger, the PSD 1010 may

initiate a sync in response to the battery level reach at least 50%, or at least 90%. The PSD 1010 may sync to any location specified by a user, such as the server 1030, a local device, or another PSD.

[0062] With reference to FIG. 11 a portable storage device 1100 is shown, in accordance with various embodiments. Portable storage device 1100 may variously include features and functionality described herein. Portable storage device 1100 may have a protective outer housing 1102. Protective outer housing 1102 may be made from materials including metals, plastics, and/or rubbers. For example, protective outer housing 1102 may be made from aluminum.

[0063] Protective outer housing 1102 may include a surface 1104 having rectangular geometry with rounded corners. The surface 1104 may also include a protruding perimeter 1106 and a sunken central portion 1108. The length of each side of surface 1104 may be approximately 48 mm, for example. A tie loop 1110 may also be removably coupled to portable storage device 1100 to facilitate portability.

[0064] Surface 1112 and surface 1114 may meet surface 1104 along tapered surface 1110. Surface 1112 and surface 1114 may include ribbed features 1116 to augment strength with minimal weight increase. The side surfaces may be approximately 48 mm by 23 mm with a rectangular geometry. The rectangular geometry of portable storage device 1100 may thus comprise 6 sides with each side having edges less than 0.5 cm in length.

[0065] Surface 104 may include i/o panel 1118. I/o panel 1118 may include buttons 1120 and 1122 to switch portable storage device 1100 between power configurations including on, off, and standby. Buttons 1120 and/or 1122 may also be used for wireless pairing with computing devices or addition to a wireless LAN, for example. I/o panel 1118 may also include lights 1124 that illuminate to shine through the surface of i/o panel 1118. The lights may serve as status indicators for power, pairing, network activity, cellular activity, etc. and may vary in color, brightness, flashing, solid, and other light characteristics to indicate device status. Portable storage device 1100 may include additional surfaces having ribbed features 1116 and similar rectangular geometry to surface 1112 and surface 1114. Portable storage device 1100 may also include another square surface opposite surface 1104 having a similar geometry with a protruding perimeter 1106 and sunken central portion 1108. One or more surface of protective outer housing 1102 may be removable to expose a changeable battery. One or more surface of protective outer housing 1102 may also include a coil electronically coupled to the battery to facilitate wireless charging.

[0066] A base 1126 may be removable from protective outer housing 1102. Base 1126 may retain and/or cover operational components such as a battery or wireless communication device. For example, base 1126 may include an RFID chip configured to broadcast an RFID for detection by RFID transponders to lock doors, unlock doors, and/or open doors. In such a configuration, on or more button such as button 1122 may be configured to broadcast a signal in response to depression.

[0067] With reference to FIGS. 12 and 13 an electronic key system 1200 is shown, in accordance with various embodiments. Electronic key system 1200 may control locking mechanisms and other mechanisms in automobiles. For example, electronic key system 1200 may actuate door locks remotely and engage or disengage an immobilizer to prevent or allow the engine to start. Electronic key system may operate using a portable storage device 1202. A portable storage device as described herein may be integrated into portable storage device 1202. Portable storage device 1202 may also be a portable storage device as described herein.

[0068] Electronic key system 1200 may accommodate lock actuation based on proximity and/or a button press. The remote unlocking is done via transponders 1206 that read the RFID transmitted by RFID chip 1204 in portable storage device 1202 (For example, the same RFID may be used for the immobilizer). Although the term portable storage device is used, a portable storage device such as portable storage device 1100 may be integrated into a key fob as shown in FIG. 13 or wireless key.

[0069] The RFID chip 1204 may be keyed to a vehicle having one or more transponders 1206 capable of detecting and matching the RFID. The RFID may be detectable at a predetermined range such as about 12 inches, 18 inches, 24 inches, or another suitable range in proximity to an automobile or door thereof. Although RFID is used as an exemplary technology, those skilled in the art will appreciate that other wireless protocols may be used by equipping portable storage device 1202 and transponders 1206 with appropriate wireless chips. For example, electronic key system 1200 may also operate using an ISO 802.11 wireless standard or Bluetooth® low energy (BLE), for example.

[0070] Transponders 1206 may be disposed in the doors and/or handles at the trunk, hood, passenger doors, gas doors, glove box, or other doors or handles on a vehicle. Doors on an automobile may thus be unlocked and open by placing a hand near a door handle, for example. Electronic key system 1200 may power a transponder 1206 keyed with an RFID in response to detecting an object nearby. The transponder 1206 may determine whether a portable storage device 1202 is in range with an RFID matching that stored in transponder 1206. Transponder

1206 may be coupled to an actuator to actuate door locks and/or latches. The door may thus unlock and/or open in response to portable storage device 1202 being in proximity to transponder 1206. Transponder 1206 may also be coupled via electronic connection 1208 (wireless or wired) to other systems of a vehicle.

5 [0071] Portable storage device 1202 may include an RFID reader/write capable of cloning a vehicle key. In that regard, portable storage device 1202 may have RFID chip 1204 with a cloned RFID identical to that of an existing key. Portable storage device 1202 may thus enable access to the car without the manufacturer-issued car key. Vehicle manufacturers may also key portable storage device 1202 for delivery along with a vehicle, or for purchase for an identifiable
10 vehicle, to replace the typical key fob. FIG 13 shows an exemplary key fob.

[0072] In various embodiment, electronic key system 1200 may comprise wireless devices 1291, 1292, 1293 such as, for example, Bluetooth®, RF, NFC, and/or a low-level Wi-Fi devices such as that commercially available under the trade names Artik or NXP. Wireless devices 1291 and 1293 may be capable of electronic communication with one another via wireless
15 transmission to match an ID. A wireless key protocol may be implemented between the wireless communication devices to facilitate authentication and actuation of locks and latches. The wireless device 1291 in the remote unlocking may be located remote from the ignition coil. For example, the wireless device at 1291 may be located at an electromagnetic solenoid disposed in the door handle. The wireless device 1291 may be configured to intercept transmissions on the
20 wire 1210. A user may be prompted to lock and/or unlock their door with their original key. The wireless device 1291 may intercept one or more transmission and store the signal in a reproducible manner. In response to detecting an ID from wireless device 1293, wireless device 1291 may be configured to reproduce the signal on wire 1210 to trigger the action in the vehicle associated with the signal such as locking, unlocking, or opening a door.

25 [0073] Wireless device 1291 may be positioned at a location on wire 1210 suitable to detect an ID. In that regard, the signal may not be a rolling code or any other complexities/security that may be introduced later. The system may thus be secure by restricting the ability to hack into electronic key system 1200 installed in a vehicle. Integrating portable storage device 1202 in this manner may also extend the range of lock/unlock commands to about 200 feet rather than a
30 more restrictive distance such as 18 inches.

[0074] In various embodiments, portable storage device 1202 may also be configured to lock and/or unlock doors at range in response to depressing a button. Portable storage device 1202 may be configured to clone a signal transmitted by an existing key, as described above. Portable

storage device 1202 may also be configured to intercept a signal using the configuration with paired wireless communication devices 1293 and 1291, as described above. Portable storage device 1202 may thus replace the transmitter and receiver lines. Portable storage device 1202 may perform its own authentication to confirm a valid signals associated with lock/unlock commands between wireless devices 1291 and 1293. In response to successful authentication, wireless device 1291 may send the information (the ID that is static and in a vehicle electronic control unit (ECU)) to the ECU 1212 through the wire 1210.

[0075] Wireless device 1291 may be installed in an automobile using standard wireless installation techniques. For example, wireless device 1291 may be installed in a simple configuration using three or fewer wires for each transponder 1206 in the vehicle and a 12 volt and ground pair to power a transponder 1206. Wireless device 1291 may thus be installed by splicing existing wires with push-fit connectors, for example, to facilitate tool-less installation. Wireless device 1293 may include a wireless communication chip or module that connects to portable storage device 1202 (e.g., in base 1126 of FIG. 11) and/or is directly embedded into portable storage device 1202.

[0076] Electronic key system 1200 may also integrate with an immobilizer installed in an automobile to disable/enable engine operation. Vehicle ECU 1212 may store a set of keys (e.g., RFID or other ID codes) that correspond to keys with which portable storage devices 1202 are programmed. In response to an attempt to start the vehicle, the wireless communication device 1291 may transmit the ID code to the transponder key ECU 1214. Transponder key ECU 1214 may validate and/or authenticate the ID code by matching the ID code to a value stored in its memory. In response to a match, transponder key ECU 1214 may send an OK signal to the engine ECU 1216.

[0077] Electronic key system 1200 may also use a similar approach to cloning an ID code configured to operate an immobilizer as the described above. Electronic key system 1200 may also incorporate a wireless device 1292 (similar to the above described wireless device 1291) electronically coupled to at least one of the transponder key ECU 1214 and/or engine ECU 1216. Wireless device 1292 may optionally replace wireless device 1291 and/or operate in conjunction with wireless device 1291. Installing into a vehicle wireless device 1292 may enable electronic key system 1200 to bypass any limitation in the vehicle ECU such as the number of keys, the level of security, or other ECU limitations and/or controls. Wireless device 1292 may thus replace and/or duplicate transponder key ECU 1214 if the transponder key ECU is a separate device and not part of the vehicle ECU 1212 directly. Wireless device 1292 may send basic

transmissions directly to the engine ECU 1216. Wireless device 1292 may also act as a controller of the transponder key ECU 1214 and thereby use transponder key ECU 1214 to lock, unlock, and/or demobilize the engine.

[0078] Electronic key system 1200 may also be configured to program vehicle ECU 1212 in various embodiments. For example, electronic key system 1200 may interface with an onboard diagnostic system (e.g., OBD II) in communication with engine ECU 1216 by a wireless device 1292 (or another suitably placed wireless device) to control, program, or otherwise interact with spark plugs, fuel injectors, fuel pumps, or other components of a vehicle subject to electronic control.

[0079] In various embodiments, a wireless device 1292 may sit atop the engine ECU 1216 to intercept and/or control electronic traffic to and from the engine ECU 1216. For example, wireless device 1292 may monitor and/or transmit to portable storage device 1202 the user's driving habits, learn from the driving habits, identify driver inefficiencies, and/or program the engine ECU 1216 to auto-correct by overriding detrimental driving habits of the user. For example, electronic key system 1200 may be configured to improve fuel economy. A driver may apply too much gas while the clutch is engaging a manual transmission, thereby wasting fuel and burning the clutch. Electronic key system 1200 may program engine ECU 1216 to apply a cap on the throttle during clutch engagement from a stand still. Similarly, electronic key system 1200 may program engine ECU 1216 to correct other uneconomical habits that would not endanger the driver.

[0080] In various embodiments, electronic key system 1200 may also be configured to interact with safety features by appropriately placing a wireless device similar to wireless devices 1291 and 1292. For example, an older vehicle with limited processing may have safety features augmented by electronic key system 1200. A wireless device may read proximity sensors, detect a possible collision or icy conditions, or otherwise integrate with various sensors and controllers in a vehicle and then transmit signals to and/or receive signals from portable storage device 1202. Portable storage device 1202 may be programmed to evaluate the signals and transmit commands back to the wireless device to effectively and appropriately engage brakes, steering, audio signals, or otherwise protect the driver and vehicle. Processing power may be enhanced by replacing and/or upgrading portable storage device 1202 (e.g., by replacing base 1126 with a more powerful base).

[0081] In various embodiments, electronic key system 1200 may be integrated into an infotainment system by placing wireless devices similar to wireless devices 1291 and 1292 in

suitable locations. The wireless devices, in conjunction with portable storage devices 1202, may perform operations such as, for example, adjusting seat position, adjusting climate control to preselected settings, playing media, controlling a garage door, adjusting mirrors.

[0082] Portable storage device 1202 may also leverage modern computing power to operate as an anti-theft device. Portable storage device 1202 may be programmed to learn the driver's habits, driver characteristics (e.g., weight or body temperature) to detect theft attempts. A person entering the car would, for example, sit on the seat fitted with a basic load cell coupled to a wireless device similar to 1291 or 1292. Portable storage device 1202 would receive from the wireless device a signal indicating the driver weighs 6 lbs more than the last time they drove 6 hours ago. Portable storage device 1202 may thus immobilize the vehicle. Portable storage device 1202 may then transmit a message to the user's cell phone asking them to authorize ignition of the engine. In response to a "no" answer, for example, portable storage device 1202 may be configured to notify a security firm of an attempted theft. Further security could be added, such as if a car is attempted to be started ever outside of a set time period like after 8 pm and before 6 am, or leaves a GPS field and has the power to safely gradually slow the car to a stop and send full GPS tracking information and audio/video to the owner and security company.

[0083] Portable storage device 1202 may effectively act as the "brain" of the vehicle, listening, controlling and reporting every aspect where it has access to receive/send appropriate signals. The processing power and feature list may be easily upgraded as time passes by replacing or upgrading portable storage device 1202. In addition to the vehicle-centric features described with reference to FIG. 12, portable storage device 1202 may have additional functionality including that described herein.

[0084] Referring to FIG. 13, an electronic key fob 1300 having a portable storage device configured to monitor and/or control electronic systems in a motor vehicle is illustrated according to various embodiments. The electronic key fob 1300 may comprise a portable storage device such as portable storage device 1202 described with respect to FIG. 12. The electronic key fob 1300 may come in a variety of shapes and sized as is known in the art.

[0085] In various embodiments, the methods described herein are implemented using the various particular machines described herein. The methods described herein may be implemented using the below particular machines, and those hereinafter developed, in any suitable combination, as would be appreciated immediately by one skilled in the art. Further, as is unambiguous from this disclosure, the methods described herein may result in various transformations of certain articles.

[0086] For the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical system.

[0087] The various system components discussed herein may include one or more of the following: a host server or other computing systems including a processor for processing digital data; a memory coupled to the processor for storing digital data; an input digitizer coupled to the processor for inputting digital data; an application program stored in the memory and accessible by the processor for directing processing of digital data by the processor; a display device coupled to the processor and memory for displaying information derived from digital data processed by the processor; and a plurality of databases. Various databases used herein may include: client data; merchant data; financial institution data; and/or like data useful in the operation of the system. As those skilled in the art will appreciate, user computer may include an operating system (e.g., Windows NT, Windows 95/98/2000, Windows XP, Windows Vista, Windows 7, OS2, UNIX, Linux, Solaris, MacOS, etc.) as well as various conventional support software and drivers typically associated with computers.

[0088] A network may include any cloud, cloud computing system or electronic communications system or method which incorporates hardware and/or software components. Communication among the parties may be accomplished through any suitable communication channels, such as, for example, a telephone network, an extranet, an intranet, Internet, point of interaction device (point of sale device, personal digital assistant (e.g., iPhone®, Palm Pilot®, Blackberry®, cellular phone, kiosk, etc.), online communications, satellite communications, off-line communications, wireless communications, transponder communications, local area network (LAN), wide area network (WAN), virtual private network (VPN), networked or linked devices, keyboard, mouse and/or any suitable communication or data input modality. Moreover, although the system is frequently described herein as being implemented with TCP/IP communications protocols, the system may also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI, any tunneling protocol (e.g. IPsec, SSH), or any number of existing or future protocols. If the network is in the nature of a public network, such as the Internet, it may be advantageous to presume the network to be insecure and open to eavesdroppers. Specific information related to

the protocols, standards, and application software utilized in connection with the Internet is generally known to those skilled in the art and, as such, need not be detailed herein. See, for example, DILIP NAIK, INTERNET STANDARDS AND PROTOCOLS (1998); JAVA 2 COMPLETE, various authors, (Sybex 1999); DEBORAH RAY AND ERIC RAY, MASTERING HTML 4.0 (1997); and LOSHIN, TCP/IP CLEARLY EXPLAINED (1997) and DAVID GOURLEY AND BRIAN TOTTY, HTTP, THE DEFINITIVE GUIDE (2002), the contents of which are hereby incorporated by reference.

[0089] The various system components may be independently, separately or collectively suitably coupled to the network via data links which includes, for example, a connection to an Internet Service Provider (ISP) over the local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods, see, e.g., GILBERT HELD, UNDERSTANDING DATA COMMUNICATIONS (1996), which is hereby incorporated by reference. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network. Moreover, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

[0090] Any communication, transmission and/or channel discussed herein may include any system or method for delivering content (e.g. data, information, metadata, etc.), and/or the content itself. The content may be presented in any form or medium, and in various embodiments, the content may be delivered electronically and/or capable of being presented electronically. For example, a channel may comprise a website, a uniform resource locator ("URL"), a document (e.g., a Microsoft Word document, a Microsoft Excel document, an Adobe .pdf document, etc.), an "ebook," an "emagazine," an application or microapplication (as described below), an SMS or other type of text message, an email, Facebook, twitter, MMS and/or other type of communication technology. In various embodiments, a channel may be hosted or provided by a data partner. In various embodiments, the distribution channel and/or the may comprise at least one of a merchant website, a social media website, affiliate or partner websites, an external vendor, a mobile device communication, social media network and/or location based service. Distribution channels may include at least one of a merchant website, a social media site, affiliate or partner websites, an external vendor, and a mobile device communication. Examples of social media sites include Facebook®, foursquare®, Twitter®,

MySpace®, LinkedIn®, and the like. Moreover, examples of mobile device communications include texting, email, and mobile applications for smartphones.

[0091] The present system or any part(s) or function(s) thereof may be implemented using hardware, software or a combination thereof and may be implemented in one or more computer systems or other processing systems. However, the manipulations performed by embodiments were often referred to in terms, such as matching or selecting, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein. Rather, the operations may be machine operations. Useful machines for performing the various embodiments include general purpose digital computers or similar devices.

[0092] In fact, in various embodiments, the embodiments are directed toward one or more computer systems capable of carrying out the functionality described herein. The computer system includes one or more processors. The processor is connected to a communication infrastructure (e.g., a communications bus, cross over bar, or network). Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement various embodiments using other computer systems and/or architectures. Computer system can include a display interface that forwards graphics, text, and other data from the communication infrastructure (or from a frame buffer not shown) for display on a display unit.

[0093] Computer system also includes a main memory, such as for example random access memory (RAM), and may also include a secondary memory. The secondary memory may include, for example, a hard disk drive and/or a removable storage drive, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive reads from and/or writes to a removable storage unit in a well known manner. Removable storage unit represents a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive. As will be appreciated, the removable storage unit includes a computer usable storage medium having stored therein computer software and/or data.

[0094] In various embodiments, secondary memory may include other similar devices for allowing computer programs or other instructions to be loaded into computer system. Such devices may include, for example, a removable storage unit and an interface. Examples of such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable read only memory (PROM)) and associated socket, and other

removable storage units and interfaces, which allow software and data to be transferred from the removable storage unit to computer system.

[0095] Computer system may also include a communications interface. Communications interface allows software and data to be transferred between computer system and external devices. Examples of communications interface may include a modem, a network interface (such as an Ethernet card), a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface are in the form of signals which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface. These signals are provided to communications interface via a communications path (e.g., channel). This channel carries signals and may be implemented using wire, cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, wireless and other communications channels.

[0096] The terms “computer program medium” and “computer usable medium” are used to generally refer to media such as removable storage drive and a hard disk installed in hard disk drive. These computer program products provide software to computer system.

[0097] Computer programs (also referred to as computer control logic) are stored in main memory and/or secondary memory. Computer programs may also be received via communications interface. Such computer programs, when executed, enable the computer system to perform the features as discussed herein. In particular, the computer programs, when executed, enable the processor to perform the features of various embodiments. Accordingly, such computer programs represent controllers of the computer system.

[0098] In various embodiments, software may be stored in a computer program product and loaded into computer system using removable storage drive, hard disk drive or communications interface. The control logic (software), when executed by the processor, causes the processor to perform the functions of various embodiments as described herein. In various embodiments, hardware components such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

[0099] In various embodiments, the server may include application servers (e.g. WEB SPHERE, WEB LOGIC, JBOSS). In various embodiments, the server may include web servers (e.g. APACHE, IIS, GWS, SUN JAVA SYSTEM WEB SERVER).

[00100] As those skilled in the art will appreciate, a device may include but is not limited to an operating system (e.g., Windows NT, 95/98/2000/CE/Mobile, OS2, UNIX, Linux, Solaris,

MacOS, PalmOS, etc.) as well as various conventional support software and drivers typically associated with computers. A device may include but is not limited to any suitable personal computer, network computer, workstation, personal digital assistant, cellular phone, smart phone, minicomputer, mainframe or the like. A device can be in a home or business environment with
5 access to a network. In various embodiments, access is through a network or the Internet through a commercially available web-browser software package. A device may implement security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). A device may implement several application layer protocols including http, https, ftp, and sftp.

[00101] In various embodiments, components, modules, and/or engines of system 100 may be
10 implemented as micro-applications or micro-apps. Micro-apps are typically deployed in the context of a mobile operating system, including for example, a Palm mobile operating system, a Windows mobile operating system, an Android Operating System, Apple iOS, a Blackberry operating system and the like. The micro-app may be configured to leverage the resources of the larger operating system and associated hardware via a set of predetermined rules which govern
15 the operations of various operating systems and hardware resources. For example, where a micro-app desires to communicate with a device or network other than the mobile device or mobile operating system, the micro-app may leverage the communication protocol of the operating system and associated device hardware under the predetermined rules of the mobile operating system. Moreover, where the micro-app desires an input from a user, the micro-app
20 may be configured to request a response from the operating system which monitors various hardware components and then communicates a detected input from the hardware to the micro-app.

[00102] “Cloud” or “Cloud computing” includes a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,
25 storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing may include location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. For more information regarding cloud computing, see the NIST’s (National Institute of Standards and Technology) definition of cloud computing at
30 <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> (last visited February 4, 2011), which is hereby incorporated by reference in its entirety.

[00103] As used herein, “transmit” may include sending electronic data from one system component to another. Additionally, as used herein, “data” may include encompassing

information such as commands, queries, files, data for storage, and the like in digital or any other form.

[00104] The system contemplates uses in association with web services, utility computing, pervasive and individualized computing, security and identity solutions, autonomic computing, cloud computing, commodity computing, mobility and wireless solutions, open source, biometrics, grid computing and/or mesh computing.

[00105] Any databases discussed herein may include relational, hierarchical, graphical, or object-oriented structure and/or any other database configurations. Common database products that may be used to implement the databases include DB2 by IBM (Armonk, NY), various database products available from Oracle Corporation (Redwood Shores, CA), Microsoft Access or Microsoft SQL Server by Microsoft Corporation (Redmond, Washington), MySQL by MySQL AB (Uppsala, Sweden), or any other suitable database product. Moreover, the databases may be organized in any suitable manner, for example, as data tables or lookup tables. Each record may be a single file, a series of files, a linked series of data fields or any other data structure. Association of certain data may be accomplished through any desired data association technique such as those known or practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, using a key field in the tables to speed searches, sequential searches through all the tables and files, sorting records in the file according to a known order to simplify lookup, and/or the like. The association step may be accomplished by a database merge function, for example, using a “key field” in pre-selected databases or data sectors. Various database tuning steps are contemplated to optimize database performance. For example, frequently used files such as indexes may be placed on separate file systems to reduce In/Out (“I/O”) bottlenecks.

[00106] One skilled in the art will also appreciate that, for security reasons, any databases, systems, devices, servers or other components of the system may consist of any combination thereof at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, decryption, compression, decompression, and/or the like.

[00107] Encryption may be performed by way of any of the techniques now available in the art or which may become available—e.g., Twofish, RSA, El Gamal, Schorr signature, DSA, PGP, PKI, GPG (GnuPG), and symmetric and asymmetric cryptosystems.

[00108] The computing unit of the device may be further equipped with an Internet browser connected to the Internet or an intranet using standard dial-up, cable, DSL or any other Internet protocol known in the art. Transactions originating at a device may pass through a firewall in order to prevent unauthorized access from users of other networks. Further, additional firewalls
5 may be deployed between the varying components of the system to further enhance security.

[00109] The computers discussed herein may provide a suitable website or other Internet-based graphical user interface which is accessible by users. In various embodiments, the Microsoft Internet Information Server (IIS), Microsoft Transaction Server (MTS), and Microsoft SQL Server, are used in conjunction with the Microsoft operating system, Microsoft NT web
10 server software, a Microsoft SQL Server database system, and a Microsoft Commerce Server. Additionally, components such as Access or Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase, etc., may be used to provide an Active Data Object (ADO) compliant database management system. In various embodiments, the Apache web server is used in conjunction with a Linux operating system, a MySQL database, and the Perl, PHP, and/or
15 Python programming languages.

[00110] Any of the communications, inputs, storage, databases or displays discussed herein may be facilitated through a website having web pages. The term “web page” as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. For example, a typical website might include, in addition to standard HTML
20 documents, various forms, Java applets, JavaScript, active server pages (ASP), common gateway interface scripts (CGI), extensible markup language (XML), dynamic HTML, cascading style sheets (CSS), AJAX (Asynchronous Javascript And XML), helper applications, plug-ins, and the like. A server may include a web service that receives a request from a web server, the request including a URL (<http://yahoo.com/stockquotes/ge>) and an IP address (123.56.789.234). The
25 web server retrieves the appropriate web pages and sends the data or applications for the web pages to the IP address. Web services are applications that are capable of interacting with other applications over a communications means, such as the internet. Web services are typically based on standards or protocols such as XML, SOAP, AJAX, WSDL and UDDI. Web services methods are well known in the art, and are covered in many standard texts. See, e.g., ALEX
30 NGHIEM, IT WEB SERVICES: A ROADMAP FOR THE ENTERPRISE (2003), hereby incorporated by reference.

[00111] Middleware may include any hardware and/or software suitably configured to facilitate communications and/or process transactions between disparate computing systems.

Middleware components are commercially available and known in the art. Middleware may be implemented through commercially available hardware and/or software, through custom hardware and/or software components, or through a combination thereof. Middleware may reside in a variety of configurations and may exist as a standalone system or may be a software component residing on the Internet server. Middleware may be configured to process transactions between the various components of an application server and any number of internal or external systems for any of the purposes disclosed herein. WebSphere MQ™ (formerly MQSeries) by IBM, Inc. (Armonk, NY) is an example of a commercially available middleware product. An Enterprise Service Bus (“ESB”) application is another example of middleware.

5

10

[00112] Practitioners will also appreciate that there are a number of methods for displaying data within a browser-based document. Data may be represented as standard text or within a fixed list, scrollable list, drop-down list, editable text field, fixed text field, pop-up window, and the like. Likewise, there are a number of methods available for modifying data in a web page such as, for example, free text entry using a keyboard, selection of menu items, check boxes, option boxes, and the like.

15

20

25

30

[00113] The system and method may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the system may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the system may be implemented with any programming or scripting language such as C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, assembly, PERL, PHP, awk, Python, Visual Basic, SQL Stored Procedures, PL/SQL, any UNIX shell script, and extensible markup language (XML) with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the system may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the system could be used to detect or prevent security issues with a client-side scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography and network security, see any of the following references: (1) “Applied Cryptography: Protocols, Algorithms, And Source Code In C,” by Bruce Schneier,

published by John Wiley & Sons (second edition, 1995); (2) “Java Cryptography” by Jonathan Knudson, published by O’Reilly & Associates (1998); (3) “Cryptography & Network Security: Principles & Practice” by William Stallings, published by Prentice Hall; all of which are hereby incorporated by reference.

5 [00114] As will be appreciated by one of ordinary skill in the art, the system may be embodied as a customization of an existing system, an add-on product, a processing apparatus executing upgraded software, a stand alone system, a distributed system, a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, any portion of the system or a module may take the form of a processing apparatus
10 executing code, an internet based embodiment, an entirely hardware embodiment, or an embodiment combining aspects of the internet, software and hardware. Furthermore, the system may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical
15 storage devices, magnetic storage devices, and/or the like.

[00115] The system and method is described herein with reference to screen shots, block diagrams and flowchart illustrations of methods, apparatus (e.g., systems), and computer program products according to various embodiments. It will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of functional
20 blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions.

[00116] These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions that execute on the computer or other
25 programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which
30 implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions

which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

[00117] Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-based computer systems which perform the specified functions or steps, or suitable combinations of special purpose hardware and computer instructions. Further, illustrations of the process flows and the descriptions thereof may make reference to user windows, webpages, websites, web forms, prompts, etc. Practitioners will appreciate that the illustrated steps described herein may comprise in any number of configurations including the use of windows, webpages, web forms, popup windows, prompts and the like. It should be further appreciated that the multiple steps as illustrated and described may be combined into single webpages and/or windows but have been expanded for the sake of simplicity. In other cases, steps illustrated and described as single process steps may be separated into multiple webpages and/or windows but have been combined for simplicity.

[00118] The term “non-transitory” is to be understood to remove only propagating transitory signals per se from the claim scope and does not relinquish rights to all standard computer-readable media that are not only propagating transitory signals per se. Stated another way, the meaning of the term “non-transitory computer-readable medium” and “non-transitory computer-readable storage medium” should be construed to exclude only those types of transitory computer-readable media which were found in *In Re Nuijten* to fall outside the scope of patentable subject matter under 35 U.S.C. § 101.

[00119] Benefits, other advantages, and solutions to problems have been described herein with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any elements that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of the disclosure. Reference to an element in the singular is not intended to mean “one and only one” unless explicitly so stated, but rather “one or more.” Moreover, where a phrase similar to ‘at least one of A, B, and C’ or ‘at least one of A, B, or C’ is used in the claims or specification, it is intended that the phrase be interpreted to mean that A alone may be present in an embodiment, B

alone may be present in an embodiment, C alone may be present in an embodiment, or that any combination of the elements A, B and C may be present in a single embodiment; for example, A and B, A and C, B and C, or A and B and C. Although the disclosure includes a method, it is contemplated that it may be embodied as computer program instructions on a tangible computer-readable carrier, such as a magnetic or optical memory or a magnetic or optical disk. All structural, chemical, and functional equivalents to the elements of the above-described exemplary embodiments that are known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present disclosure, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. 112(f) unless the element is expressly recited using the phrase "means for." As used herein, the terms "comprises", "comprising", or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.

CLAIMS

1. A content storage system comprising:
a portable storage device comprising a processor, a storage module configured to store
5 files for reading by a first device comprising at least one of a personal computer, a laptop, a
smartphone, or a tablet in electronic communication with the processor, and a wireless
communication module;
a transponder electronically coupled to a door lock of a vehicle and in communication
with the wireless communication module, wherein the transponder is configured to unlock the
10 door lock in response to receiving a signal from the portable storage device.
2. The content storage system of claim 1, wherein the portable storage device further
comprises:
a protective housing containing the processor and the storage module; and
a removable base coupled to the protective housing, wherein the removable base contains
15 the wireless communication module.
3. The content storage system of claim 1, further comprising:
a second wireless communication module;
an electronic control unit of the vehicle in electronic communication with the second
20 wireless communication module, wherein the second wireless communication module allows an
engine of the vehicle to start by communicating with the electronic control unit in response to
receiving a second signal from the portable storage device.
4. The content storage system of claim 1, wherein the portable storage device comprises an
25 RFID chip.
5. The content storage system of claim 1, wherein the portable storage device is configured
to clone a manufacturer-issued key for the vehicle.
- 30 6. The content storage system of claim 1, further comprising an electronic control unit,
wherein the electronic control unit is configured to store a first key corresponding to a second
key stored on the portable storage device.

7. The content storage system of claim 1, wherein the portable storage device is configured to store a driving habit of a driver of the vehicle.

8. A content storage system comprising:

5 a portable storage device comprising a processor, a storage module configured to store files for reading by a first device comprising at least one of a personal computer, a laptop, a smartphone, or a tablet in electronic communication with the processor, and a wireless communication module; and

10 a wireless device in electronic communication with the wireless communication module of the portable storage device;

a transponder installed in a vehicle configured to transmit a signal on a wire,

wherein the wireless device is configured to detect the signal on the wire from the transponder and store the signal, and

15 wherein the wireless device is configured to transmit the signal on the wire in response to receiving a command from the portable storage device.

9. The content storage system of claim 8, wherein the portable storage device further comprises:

a protective housing containing the processor and the storage module; and

20 a removable base coupled to the protective housing, wherein the removable base contains the wireless communication module.

10. The content storage system of claim 8, wherein the signal comprises an instruction to unlock a door or start an engine.

25

11. The content storage system of claim 8, wherein the transponder is coupled to a door lock.

12. The content storage system of claim 8, wherein the wireless device is configured to transmit a driver characteristic to the portable storage device.

30

13. The content storage system of claim 12, further comprising a load cell configured to measure the driver characteristic.

14. The content storage system of claim 8, wherein the portable storage device is configured to transmit a message to a cell phone to authorize a vehicle command.

15. A method of controlling a vehicle from a portable storage device, comprising:

5 keying the portable storage device comprising a storage module configured to store files for reading by a first device comprising at least one of a personal computer, a laptop, a smartphone, or a tablet in electronic communication with the processor to a transponder by programming the portable storage device with an ID;

10 transmitting, from the portable storage device and to a wireless device, the ID in response to the transponder being within range of the portable storage device;

matching, by the wireless device, the ID from the portable storage device to a stored ID of the wireless device; and

15 transmitting, by the wireless device, a signal to at least one of a door lock or an electronic control unit in response to matching the ID to the stored ID.

16. The method of claim 15, further comprising unlocking the door lock in response to the matching.

17. The method of claim 15, further comprising cloning a manufacturer-issued car key and
20 storing a cloned RFID on the portable storage device.

18. The method of claim 15, further comprising receiving, by the portable storage device, a driver characteristic.

25 19. The method of claim 18, further comprising determining, by the portable storage device, that the driver characteristic has changed.

20. The method of claim 19, further comprising transmitting, by the portable storage device, a message to a cell phone in response to the change in the driver characteristic.

30

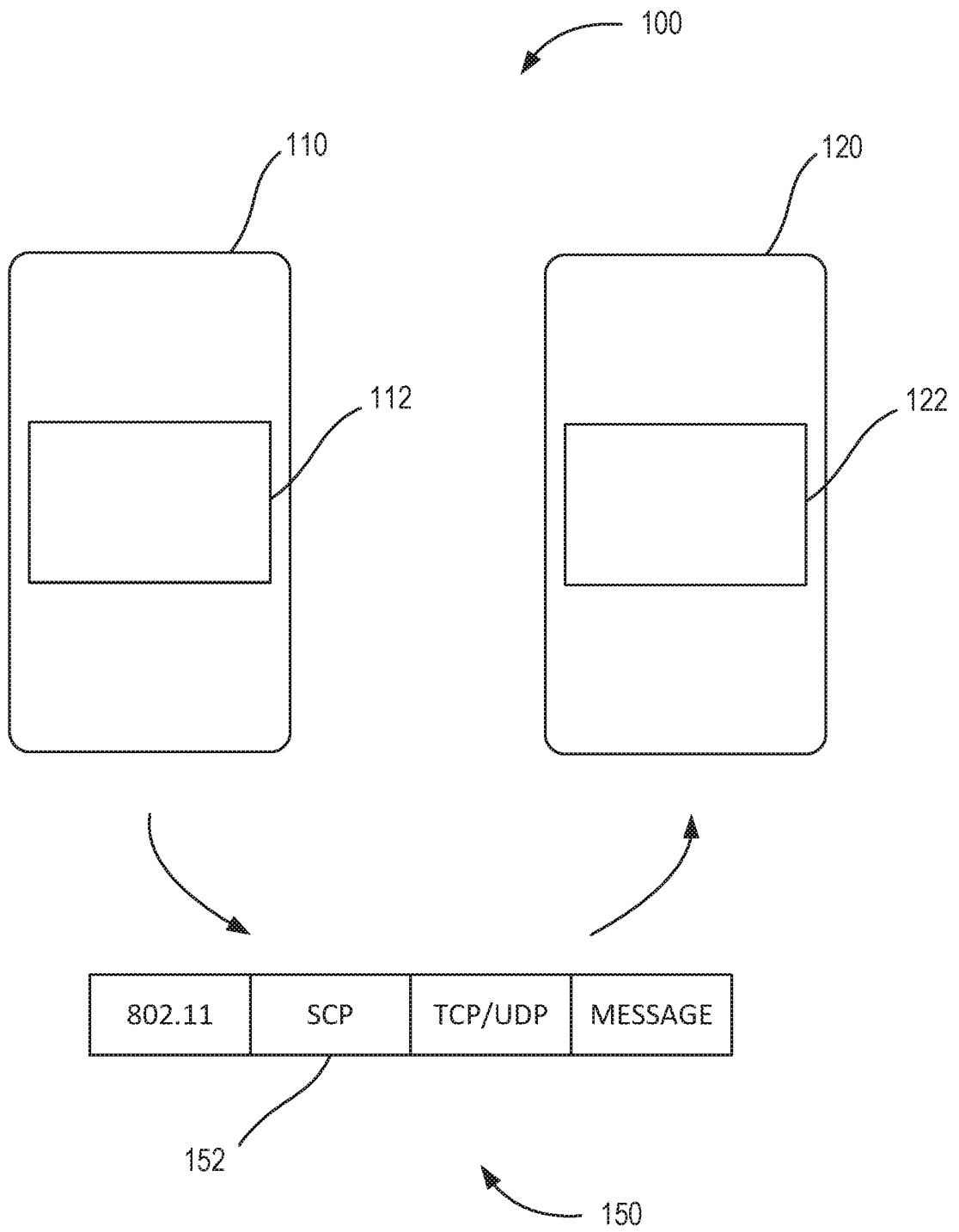


FIG. 1

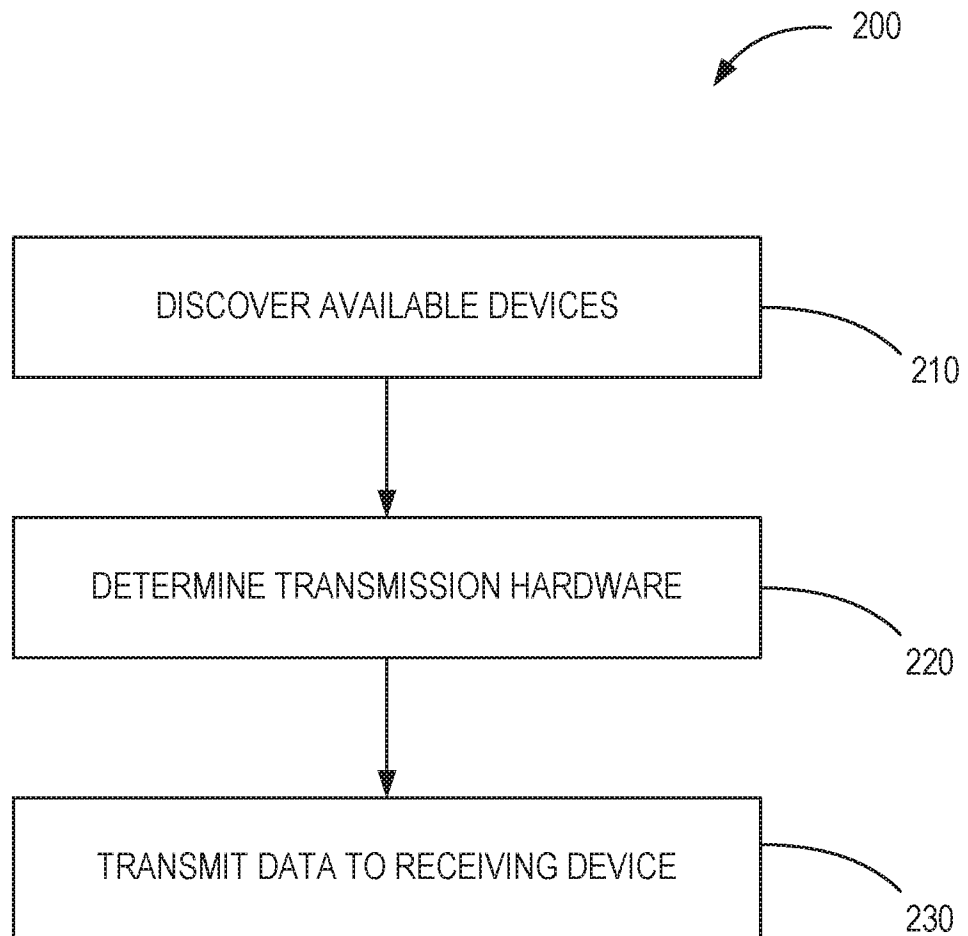


FIG. 2

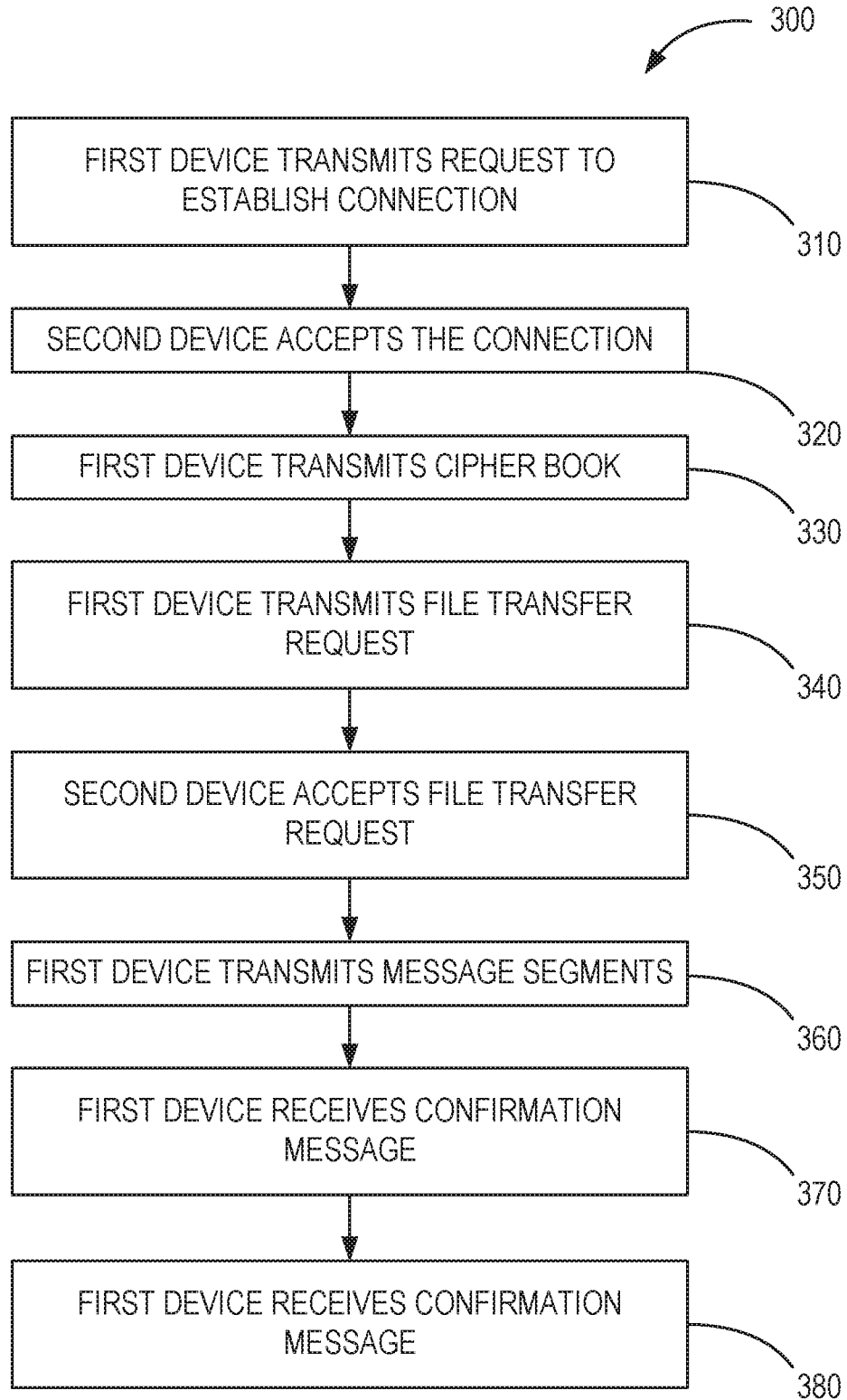


FIG. 3

400

```
mBroadcastingSocket = new Socket(AddressFamily.InterNetwork,
SocketType.Dgram, ProtocolType.Udp);
mBroadcastingSocketEventArgs = new SocketAsyncEventArgs();
mBroadcastingSocket.Ttl = 255;

var broadcastaddress = GetBroadcastAddress();
mBroadcastingSocketEventArgs.RemoteEndPoint = new
IPEndPoint(broadcastaddress, UDPPort);

// Send the IP address we are listening on
string packetData = JsonConvert.SerializeObject(LocalClient);
byte[] payload = Encoding.UTF8.GetBytes(packetData);
mBroadcastingSocketEventArgs.SetBuffer(payload, 0, payload.Length);

// Make an asynchronous Send request over the socket
mBroadcastingSocket.SendToAsync(mBroadcastingSocketEventArgs);

mDiscoverySocket = new DatagramSocket();
// This is the TTL but on datagram socket the default of 128 is more than
enough
mDiscoverySocket.Control.OutboundUnicastHopLimit = 255;
mDiscoverySocket.MessageReceived += DiscoverySocketNewMessage;

Await mDiscoverySocket.BindServiceNameAsync(UDPPort.ToString()); // Port
mDiscoverySocket.JoinMulticastGroup(new HostName(MULTICAST_ADDRESS));

var writer = new DataWriter(await
socket.GetOutputStreamAsync(eventArguments.RemoteAddress,
eventArguments.RemotePort));
await writer.StoreAsync();

var reader = eventArguments.GetDataReader();
var data = new byte[reader.UnconsumedBufferLength];
reader.ReadBytes(data);

// Get info from it
var userDetails =
JsonConvert.DeserializeObject<IDiscoveredClient>(Encoding.UTF8.GetString(data, 0,
data.Length));
```

410
420
430
440

FIG. 4

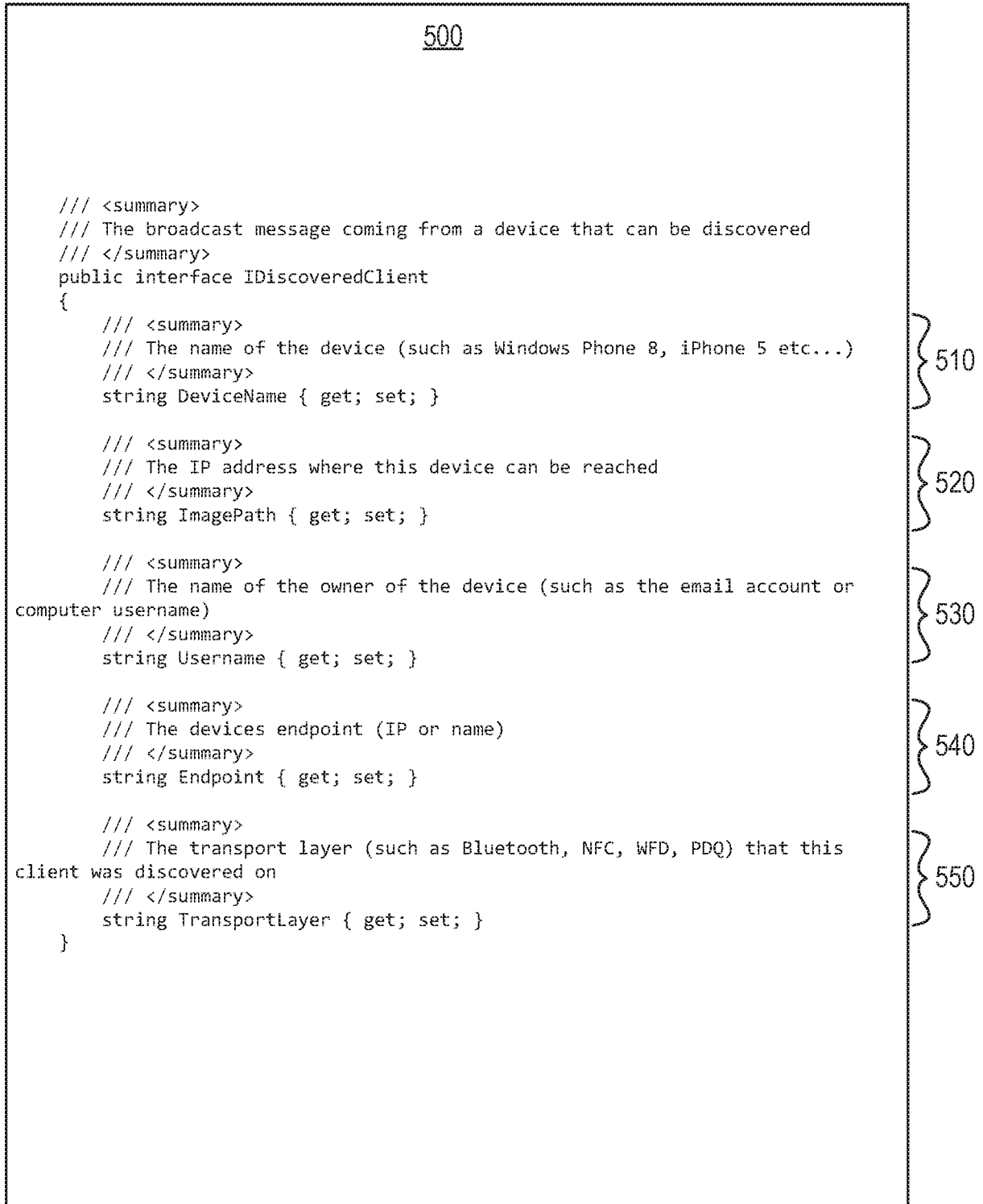


FIG. 5

600

```
/// <summary>
/// The broadcast message coming from a device that can be discovered
/// </summary>
public interface IFileTransferRequest
{
    /// <summary>
    /// The client wishing to share the file with you
    /// </summary>
    IDiscoveredClient Client { get; set; }

    /// <summary>
    /// The filename of the file wanting to be sent
    /// </summary>
    string Filename { get; set; }

    /// <summary>
    /// The size of the file wanting to be sent
    /// </summary>
    long Filesize { get; set; }

    /// <summary>
    /// The client that will be receiving the file from you
    /// </summary>
    IDiscoveredClient ReceivingClient { get; set; }

    /// <summary>
    /// The unique ID for this file transfer
    /// </summary>
    Guid UniqueID { get; set; }

    /// <summary>
    /// The transport layer associated with this request
    /// </summary>
    string TransportName { get; set; }
}
```

610
620
630
640
650
660

FIG. 6

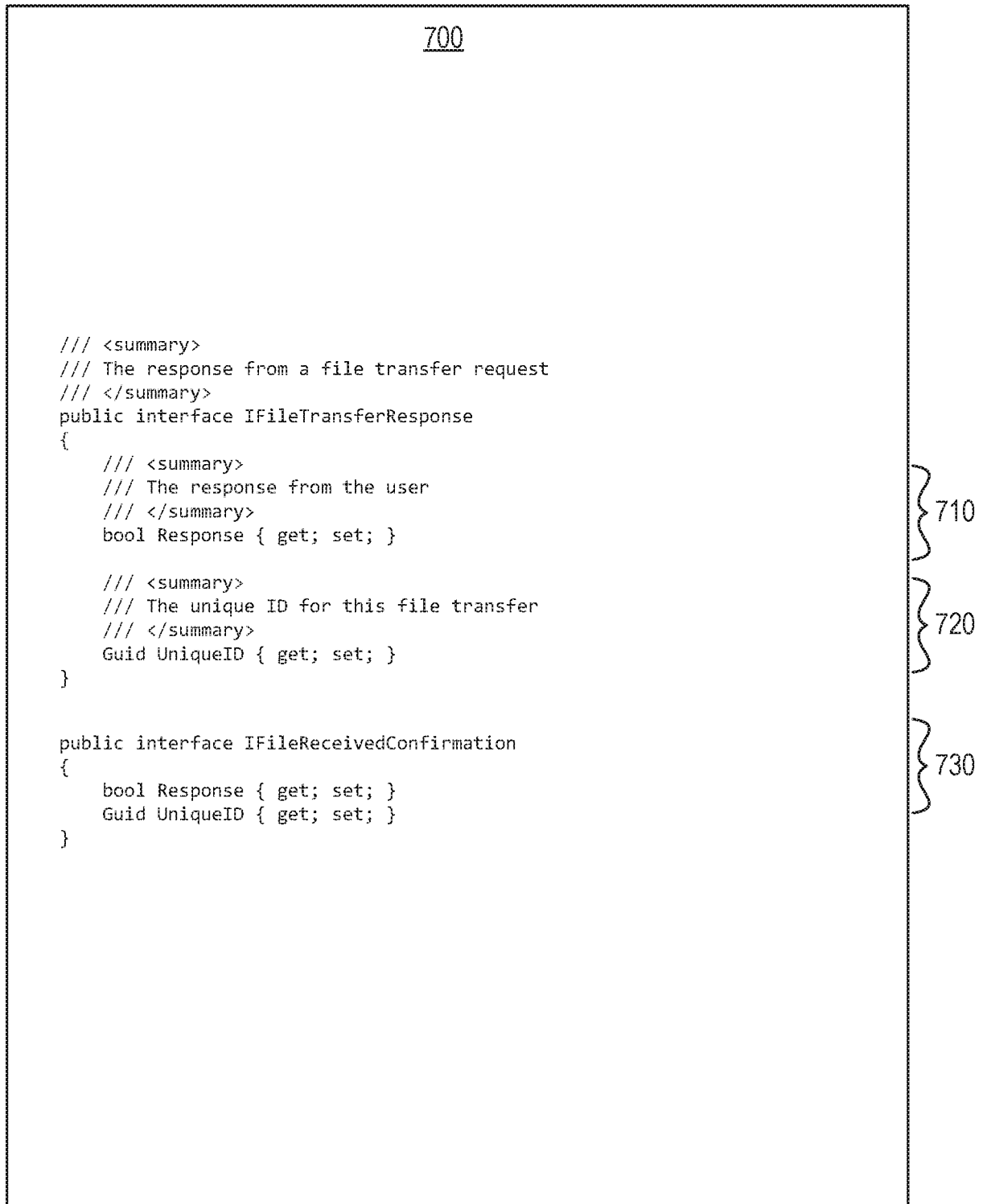


FIG. 7

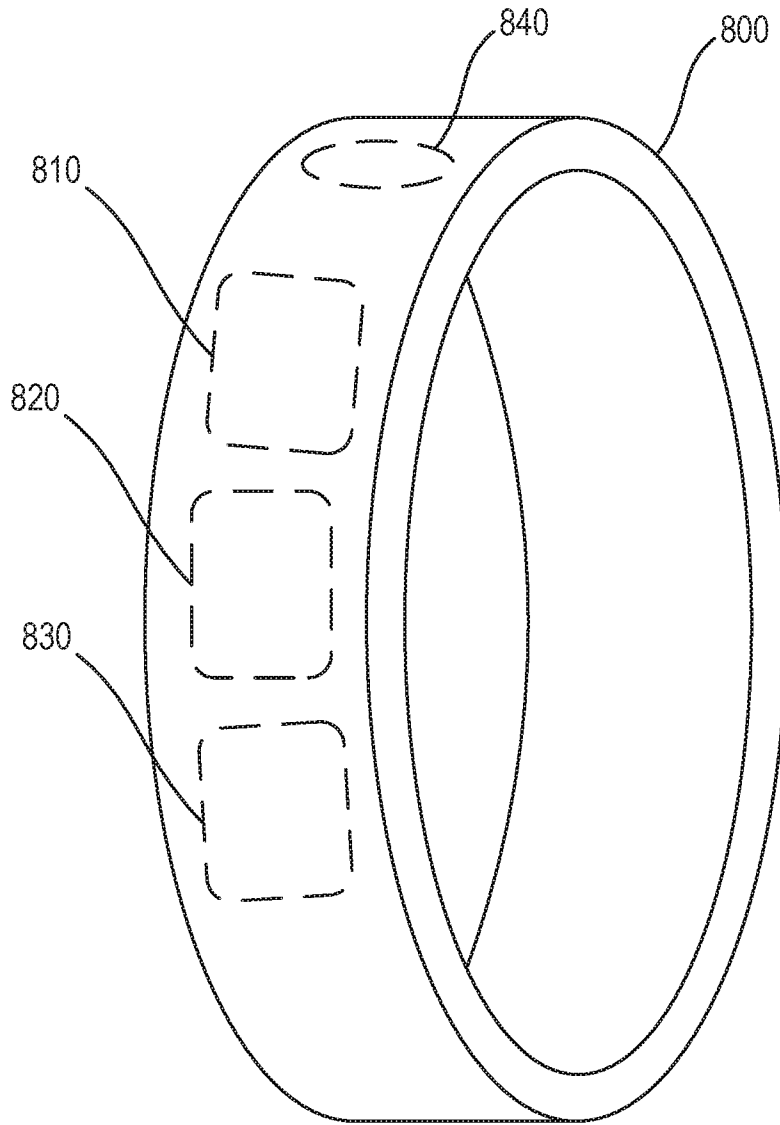


FIG. 8

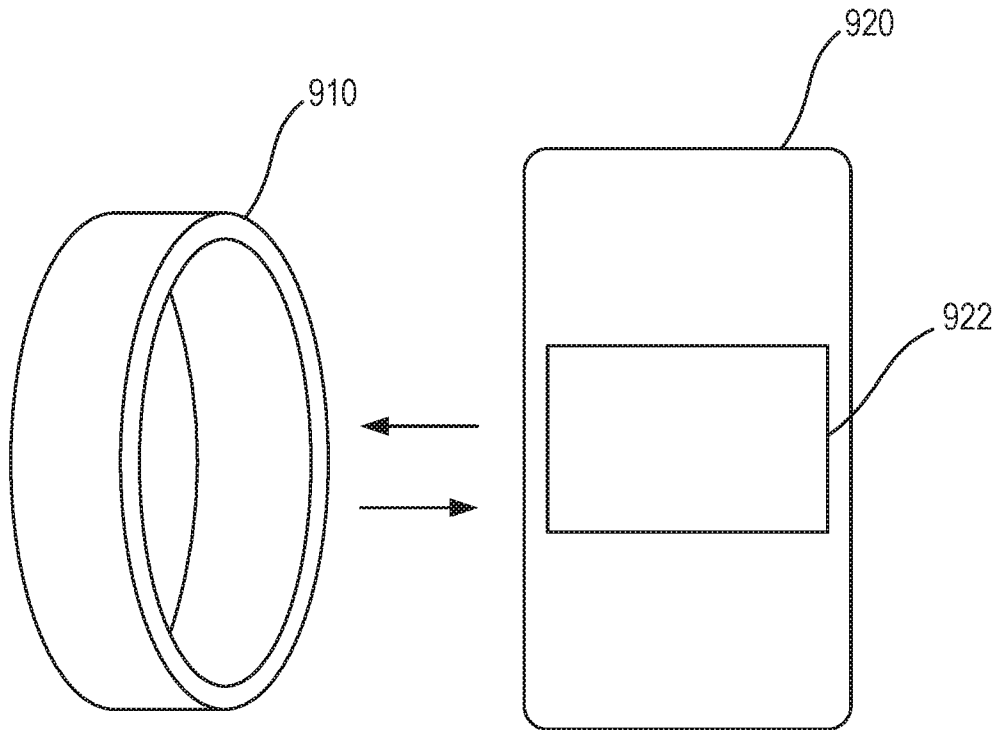


FIG. 9

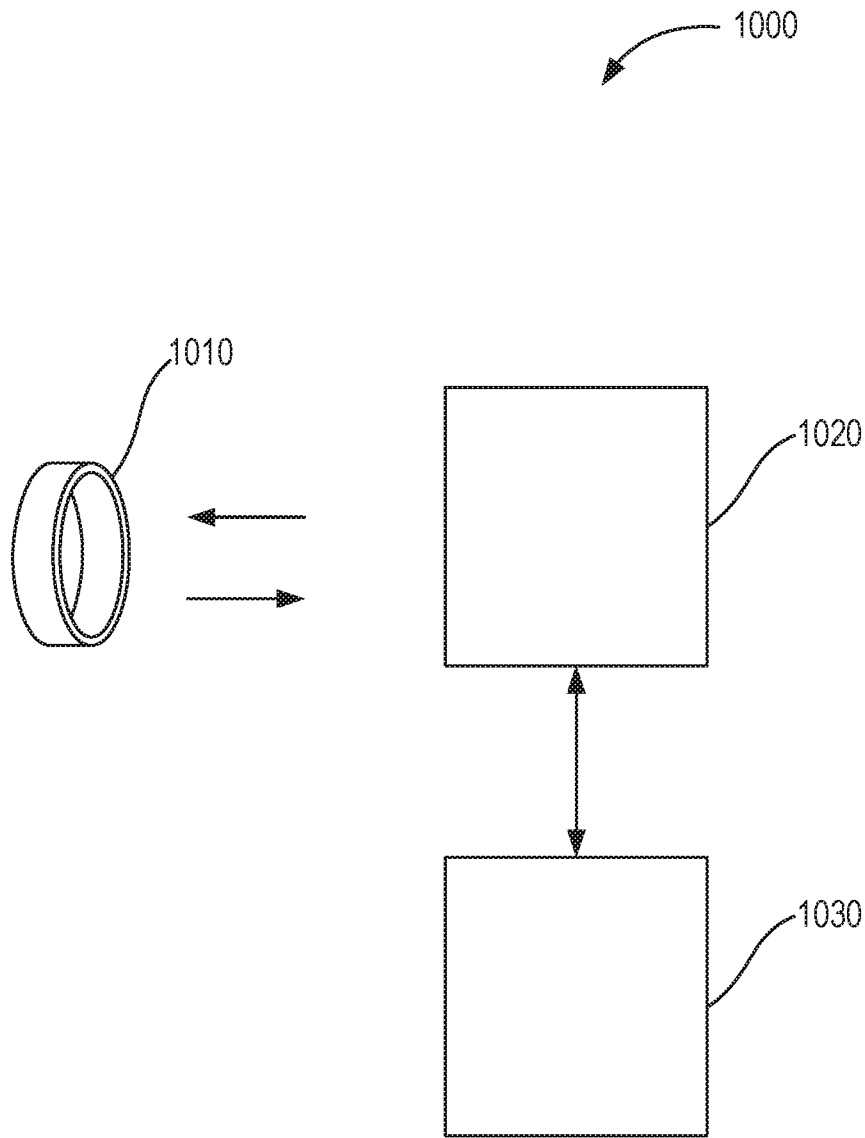


FIG. 10

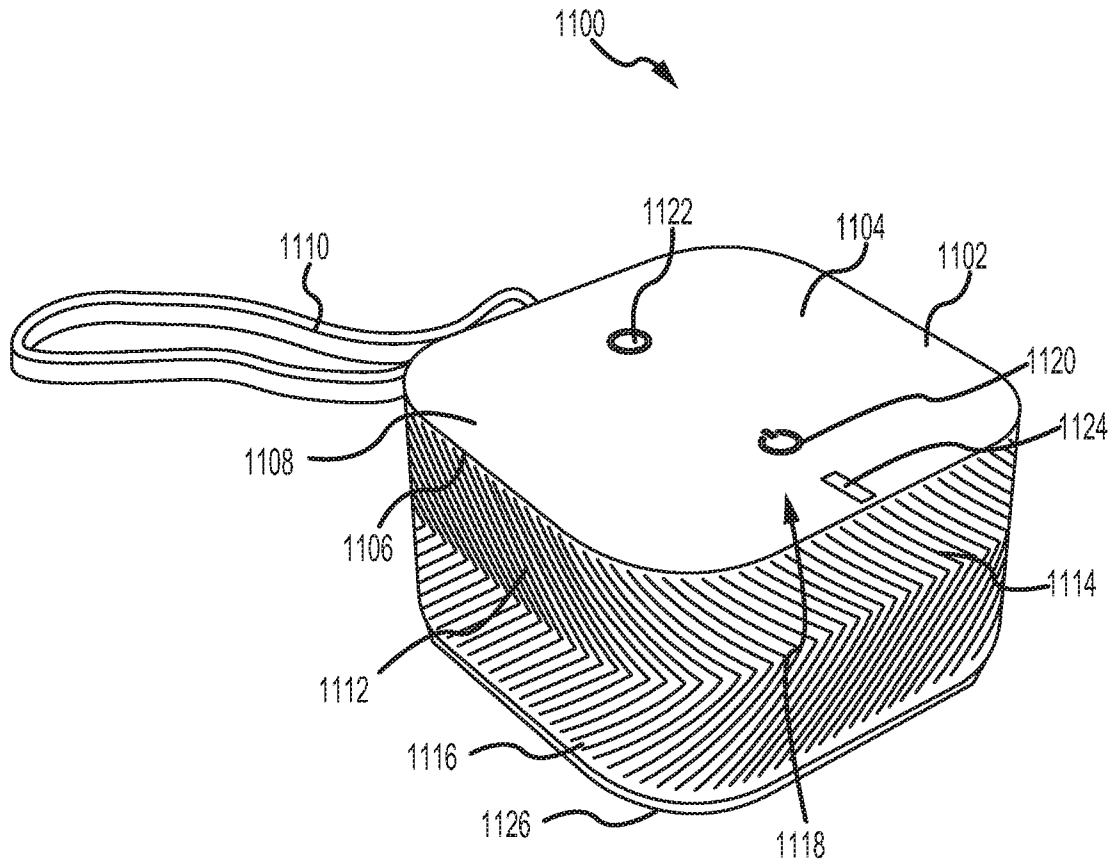


FIG.11

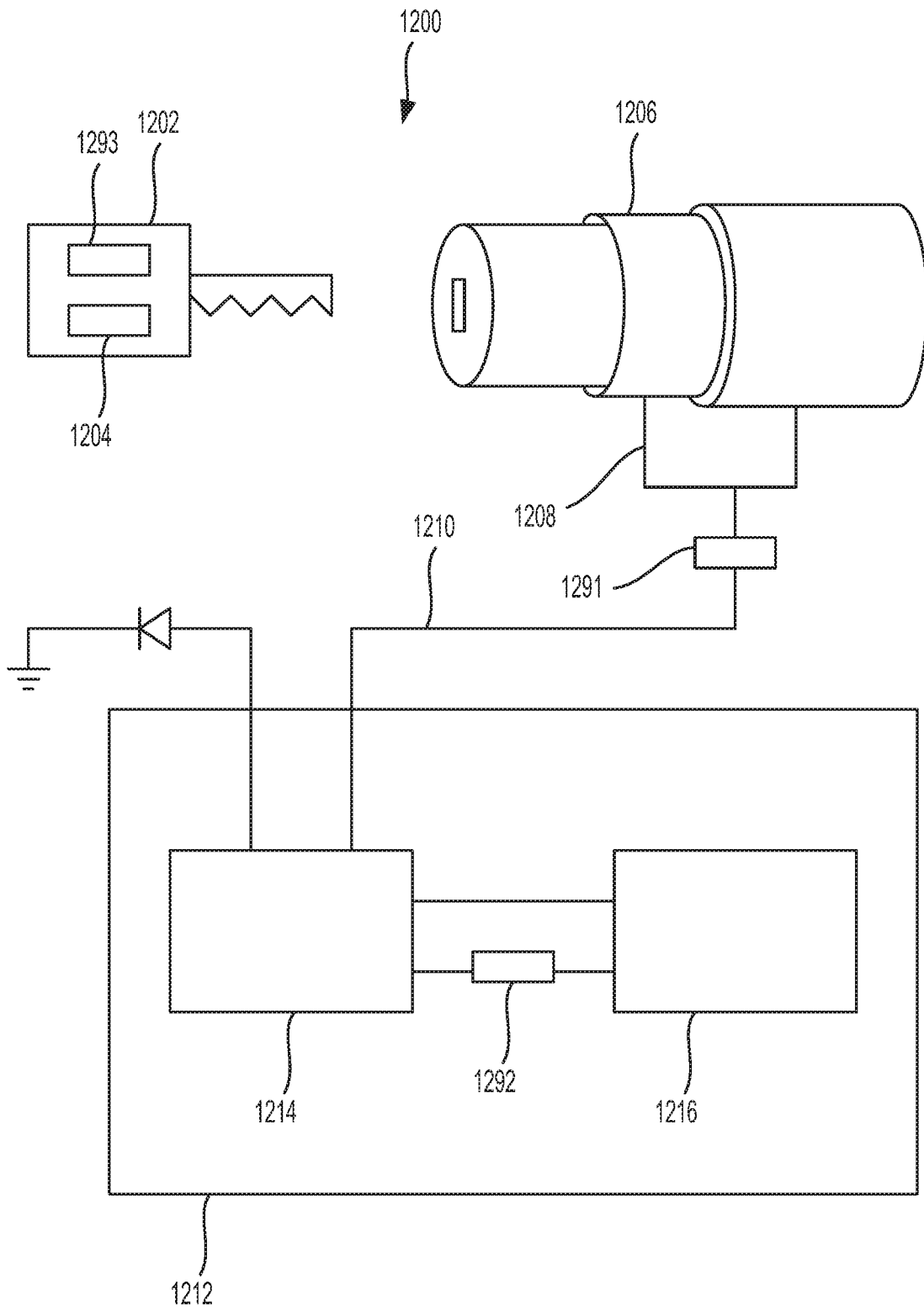


FIG. 12

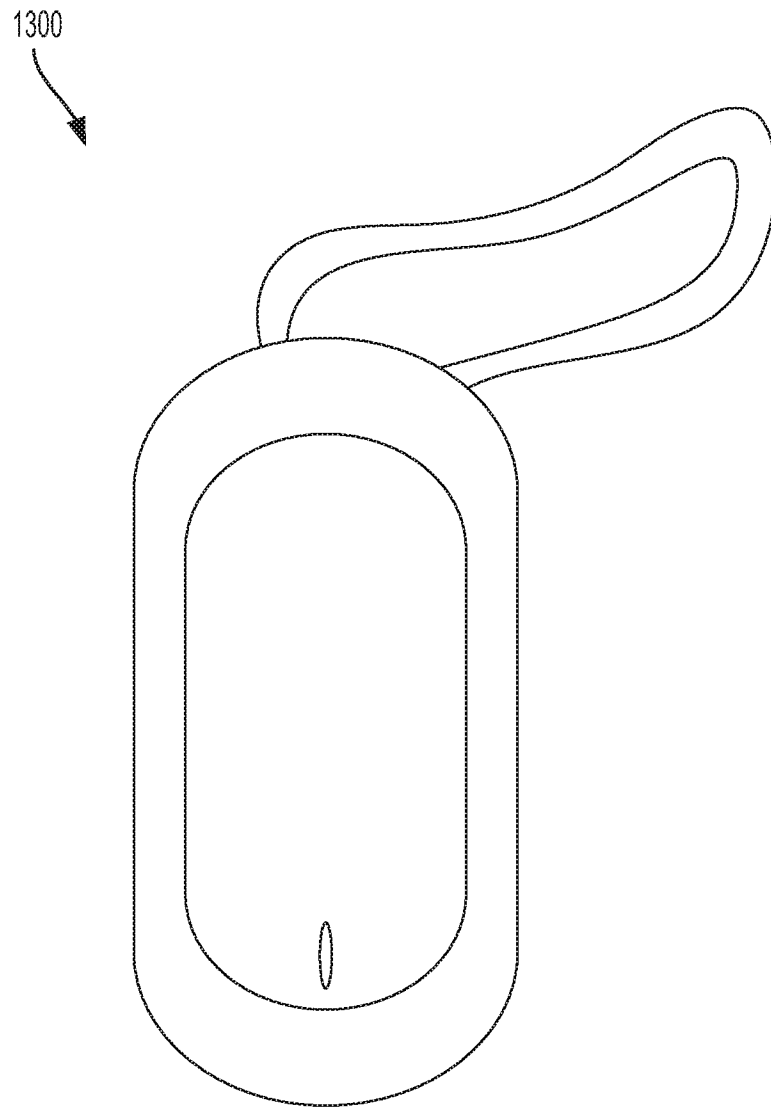


FIG. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/016610**A. CLASSIFICATION OF SUBJECT MATTER****B60R 25/10(2006.01)i, B60R 25/34(2013.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

B60R 25/10; H04L 9/08; G07D 7/00; B60R 25/24; H04W 8/00; B60R 25/0215; H04W 4/00; H04Q 5/22; H04W 12/04; B60R 25/34

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: content, portable storage device, communication module, vehicle, key, ECU, transponder

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016-0100279 A1 (CHRISTMAS et al.) 07 April 2016 See paragraphs [0002], [0047]; claim 1; and figure 8.	1-20
A	US 6160488 A (HONDA, TAKAYOSHI) 12 December 2000 See claims 1-28; and figures 1, 4-9.	1-20
A	US 5982295 A (GOTO et al.) 09 November 1999 See column 3, line 15 - column 7, line 15; and figures 1-2, 3A-3C, 4.	1-20
A	US 2014-0355761 A1 (KABUSHIKI KAISHA TOKAI RIKA DENKI SEISAKUSHO) 04 December 2014 See paragraphs [0023]-[0069]; and figures 1, 7.	1-20
A	KR 10-2009-0059672 A (HYUNDAI MOTOR COMPANY) 11 June 2009 See paragraphs [0004]-[0020]; and figures 1-3.	1-20

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

15 May 2018 (15.05.2018)

Date of mailing of the international search report

15 May 2018 (15.05.2018)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

HWANG, Chan Yoon

Telephone No. +82-42-481-3347



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2018/016610

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016-0100279 A1	07/04/2016	AU 2015-328723 A1 CA 2963079 A1 CN 107006063 A EP 3205176 A1 JP 2018-501679 A KR 10-2017-0067807 A MX 2017004463 A SE 1551071 A1 WO 2016-057091 A1	20/04/2017 14/04/2016 01/08/2017 16/08/2017 18/01/2018 16/06/2017 18/08/2017 20/08/2015 14/04/2016
US 6160488 A	12/12/2000	EP 0835790 A2 EP 0835790 A3 EP 0835790 B1 JP 10-175512 A	15/04/1998 13/09/2000 10/12/2003 30/06/1998
US 5982295 A	09/11/1999	GB 2308405 A JP 09-170366 A JP 3580923 B2	25/06/1997 30/06/1997 27/10/2004
US 2014-0355761 A1	04/12/2014	CN 104081716 A CN 104081716 B EP 2811689 A1 EP 2811689 B1 JP 2013-157900 A JP 5922419 B2 US 9392448 B2 WO 2013-114971 A1	01/10/2014 24/05/2017 10/12/2014 24/08/2016 15/08/2013 24/05/2016 12/07/2016 08/08/2013
KR 10-2009-0059672 A	11/06/2009	None	