

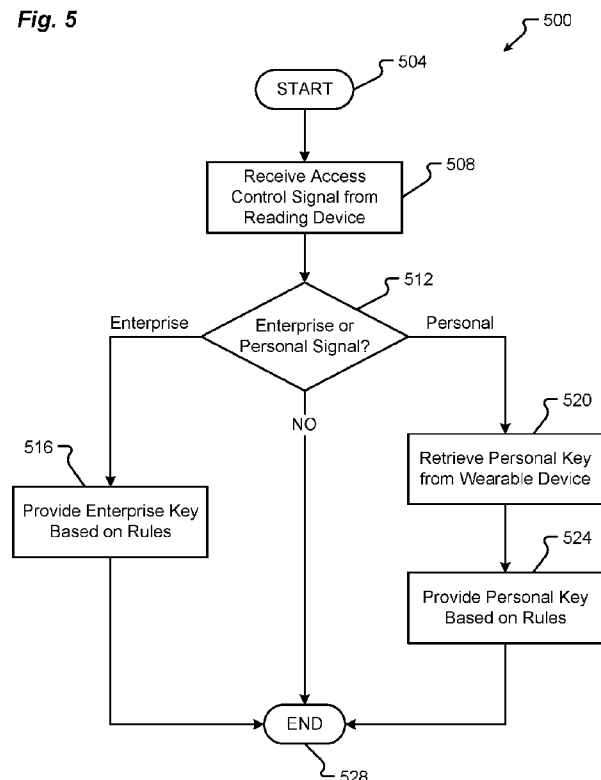


- (51) **International Patent Classification:**
- | | | | | |
|-----------------------------|-----------------------------|------------|---------------------------|----|
| <i>H04W 12/06</i> (2009.01) | <i>G06F 21/34</i> (2013.01) | 62/197,945 | 28 July 2015 (28.07.2015) | US |
| <i>H04M 1/725</i> (2006.01) | <i>H04L 29/06</i> (2006.01) | 62/197,985 | 28 July 2015 (28.07.2015) | US |
| <i>H04W 4/04</i> (2009.01) | <i>H04W 4/00</i> (2009.01) | 62/198,240 | 29 July 2015 (29.07.2015) | US |
| <i>H04W 12/08</i> (2009.01) | <i>H04W 12/04</i> (2009.01) | | | |
- (21) **International Application Number:** PCT/EP2016/059753
- (22) **International Filing Date:** 2 May 2016 (02.05.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
- | | | |
|------------|--------------------------|----|
| 62/156,035 | 1 May 2015 (01.05.2015) | US |
| 62/156,030 | 1 May 2015 (01.05.2015) | US |
| 62/161,640 | 14 May 2015 (14.05.2015) | US |
| 62/162,273 | 15 May 2015 (15.05.2015) | US |
| 62/164,099 | 20 May 2015 (20.05.2015) | US |
| 62/167,172 | 27 May 2015 (27.05.2015) | US |
| 62/167,136 | 27 May 2015 (27.05.2015) | US |
- (71) **Applicant:** ASSA ABLOY AB [SE/SE]; P.O. Box 70340, 107 23 Stockholm (SE).
- (72) **Inventors:** EINBERG, Fredrik; Klyftvägen 8, 141 41 Huddinge (SE). HOYER, Philip; 43 Manor Road, Richmond TW9 1YA (GB).
- (74) **Agent:** KRANSELL & WENNBORG KB; P.O. Box 27834, 115 93 Stockholm (SE).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[Continued on next page]

(54) **Title:** SPLIT-PROVISIONING OF PERSONAL WEARABLE AND ENTERPRISE PHONE

Fig. 5



(57) **Abstract:** Methods, devices, and systems are provided for separating the storage of access control keys based on an operational environment associated with each of the keys and access control systems. In particular, the keys may be separated based on a use context and stored on separate devices, such as a wearable device and a mobile device. The wearable device may be associated with a first operational environment such as a personal or non-enterprise environment. The mobile device may be associated with a second operational environment such as a work or enterprise environment. The control, management, and/or maintenance of the keys associated with each operational environment can be split or even performed by different provisioning authorities.



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))*

SPLIT-PROVISIONING OF PERSONAL WEARABLE AND ENTERPRISE PHONE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims the benefits of and priority, under 35 U.S.C. § 119(e), to U.S. Provisional Application Serial Nos. 62/156,035, filed on May 1, 2015, entitled “Authentication Channel Flow through Wearable”; 62/156,030, filed on May 1, 2015, entitled “Using Multiple Mobile Devices to Determine Position, Location, or Inside/Outside Door”; 62/161,640, filed on May 14, 2015, entitled “Using Wearable to Determine Ingress or Egress”; 62/162,273, filed on May 15, 2015, entitled “Continuous Authentication”; 62/164,099, filed on May 20, 2015, entitled “Using a Secondary Mobile Device to Identify a Trusted Environment”; 62/167,172, filed on May 27, 2015, entitled “Method and Apparatus for Making a Decision on a Card”; 62/167,136, filed on May 27, 2015, entitled “Split Provisioning of Personal Wearable and Enterprise Phone”; 62/197,945, filed on July 28, 2015, entitled “Wearable Discovery for Authentication”; 62/197,985, filed on July 28, 2015, entitled “Wearable Misplacement”; and 62/198,240, filed on July 29, 2015, entitled “Invisible Indication of Duress via Wearable.” The entire disclosures of the applications listed above are hereby incorporated by reference, in their entirety, for all that they teach and for all purposes.

FIELD

[0002] The present disclosure is generally directed to access control systems and more specifically to devices that are configured to provide access information for access control systems.

BACKGROUND

[0003] In general, access control systems rely upon lock and key principles to grant or deny access to a secure asset. Whether the keys are configured as physical keys presented to a mechanical lock or virtual keys presented to an access control unit, most keys include specific features or characteristics that are either recognized by or match lock features before access is granted to the asset. Some access control systems employ the use of various portable devices to maintain credential information for presentation to a reading device. The portable devices are generally configured to communicate with the reading device via wireless communication protocols.

[0004] One example of a portable device includes the radio frequency identification (RFID) device, such as a contactless smart card, key fob, or the like, to store credential information

that can be used to gain access to an asset. When presented to a reader/interrogator, the smart card transmits the stored credential information for verification by the reader/interrogator. The reader/interrogator processes the credential information and determines if the smart card being presented is a valid smart card. If the reader/interrogator determines that credential information associated with the smart card is valid, then the reader/interrogator initiates any number of actions including allowing the holder of the smart card access to an asset protected thereby.

[0005] Another example of a portable device can include a wireless mobile device, such as a communication device, mobile phone, smartphone, etc. In this case, credential information may be stored in a memory associated with the mobile device and communicated to a reading device using at least one wireless communication protocol available to the mobile phone.

SUMMARY

[0006] It is with respect to the above issues and other problems that the embodiments presented herein were contemplated. In general, embodiments of the present disclosure provide methods, devices, and systems for splitting the provisioning of keys between various devices. For example, keys may be split between a wearable device having a personal context and a mobile device having an enterprise context. In one embodiment, personal keys may be stored on a wearable device associated with a user, while enterprise, or business, keys may be stored on a mobile device associated with the user, or vice versa. In some embodiments, the personal keys, stored on the wearable device, as well as the enterprise keys, stored on the mobile device, may be accessed, or read, through an access control application running on the mobile device.

[0007] As can be appreciated, a wearable device is more personal to a user than a mobile device (e.g., a phone, etc.). Additionally or alternatively, the wearable device may have a longer operational life than the mobile device. Splitting the provisioning of keys as described herein allows a mobile device, or phone, to be changed without requiring any change to the wearable device, or vice versa. By way of example, a mobile device may be replaced, exchanged, and/or upgraded with a new mobile device and at least some of the user's keys that are stored on the separate wearable device may be maintained by the user. In this example, the new mobile device can receive the personal keys stored on the wearable device for presentation to a reading device.

[0008] In some embodiments, the provisioning authority for one type of key (e.g., personal or enterprise) may be different from the provisioning authority for the other type of key. For instance, a user may receive enterprise access control keys (e.g., keys that are associated with a work context, a business, a company, etc.) from an enterprise provisioning authority (e.g., the business, company, third party, and/or administrative unit associated with the business or company, etc.) that are stored on a mobile device associated with the user. Continuing this example, the user may have personal access control keys (e.g., keys that are associated with a personal context, such as a home asset, recreational asset, etc.) stored on a wearable device and issued via a personal provisioning authority. Where the enterprise provisioning authority is different from the personal provisioning authority, only the keys associated with the particular provisioning authority may be controlled (e.g., updated, maintained, and/or revoked, etc.) by that particular provisioning authority. For example, the enterprise provisioning authority may be restricted from controlling the personal access control keys stored on the wearable. Additionally or alternatively, the personal provisioning authority may be restricted from controlling the enterprise access control keys stored on the mobile device.

[0009] It is an aspect of the present disclosure that keys may be stored on different devices (e.g., a wearable device, a mobile device, etc.). By way of example, residential keys may be stored on the wearable device and enterprise keys may be stored on the mobile device, or vice versa.

[0010] In one embodiment, an application may be configured to present, or graphically render, a particular menu to a display (e.g., a graphical user interface, touchscreen, screen, etc.) based on a context associated with a reading device. The display may be associated with a mobile device, a wearable device, a reading device, a communication device, and/or some other device associated with the access control system. In one embodiment, the application may be running on the mobile device, the reading device, the communication device, an access server, and/or other device associated with the access control system. In any event, an enterprise reading device associated with an enterprise, or work, context may cause a first menu having a first configuration and informational content to be presented to the display. A non-enterprise reading device associated with a non-enterprise or personal context may cause a second menu having a second configuration and informational content to be presented to the display. This second menu may be different (e.g., in appearance, content, behavior, etc.) from the first menu.

[0011] By way of example, if a user walks up to a work reader (e.g., an enterprise reading device) the menu may be presented in a particular manner (e.g., to have a particular appearance, look, or feel, or via the mobile device). Continuing this example, if the user walks up to a home reader (e.g., a non-enterprise reading device) the menu may be presented in a different manner (e.g., having a different appearance, look, and/or feel when compared to the work menu or via the wearable device).

[0012] A wearable device can include any physical electronic device having a processor, a memory, and a communications module that is configured to be worn by, or otherwise attached to, a user. In some cases, the wearable device may be worn as an implant introduced intradermally (e.g., within the skin, etc.) and/or subdermally (e.g., under the skin, etc.) in a user. Additionally or alternatively, a wearable device may be adhered or otherwise placed into contact with the dermis of a user (e.g., supradermally or outside of the skin of a user, etc.). In some embodiments, a wearable device may be worn as an article of clothing or other accessory. Examples of wearable devices can include, but are in no way limited to, activity monitors, heart rate monitors, watches, rings, belts, bracelets, jewelry, clothing, buttons, necklaces, shoes, hats, pins, accessories, scarves, combinations and/or parts thereof, and/or any other wearable item.

[0013] In some embodiments, the authentication of a user may be based on whether the wearable device is within a communication range of the mobile device. The communication range may be based on any number of communications protocols associated with the wearable and/or the mobile device. Examples of communications protocols can include, but are in no way limited to, the protocol or protocols associated with near field communication (NFC), radio frequency identification (RFID)(e.g., operating at 125kHz, 13.56kHz, etc.), Bluetooth® wireless communication, Bluetooth® Low Energy (BLE), Personal Area Network (PAN), Body Area Network (BAN), cellular communications, WiFi communications, and/or other wireless communications.

[0014] As provided herein, the wearable device may be configured to operate in conjunction with one or more mobile devices. In some embodiments, the mobile devices may be provided by a manufacturer different from the wearable device.

[0015] The wearable device may include its own power source or use power provided from another source. In some embodiments, the wearable device may include electronics that can be powered (e.g., inductively, capacitively, wirelessly, via a wired connection, or some other mechanism) by a mobile device and/or a reading device. One example of such electronics

that may be incorporated into a wearable device includes RFID components, (e.g., a capacitor, antenna, etc.). In this example, when the wearable device is presented within an RFID field provided by the mobile device and/or the reading device, the mobile device and/or the reading device provides energy via the RFID field that can be stored in the capacitor of the wearable device.

[0016] The term “computer-readable medium,” as used herein, refers to any tangible data storage medium that participates in providing instructions to a processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, NVRAM, or magnetic or optical disks. Volatile media includes dynamic memory, such as main memory. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, magneto-optical medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, a solid state medium like a memory card, any other memory chip or cartridge, or any other medium from which a computer can read instructions. When the computer-readable medium is configured as part of a database, it is to be understood that the database may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Accordingly, the disclosure is considered to include a tangible storage medium or distribution medium and prior art-recognized equivalents and successor media, in which the software implementations of the present disclosure are stored.

[0017] As used herein, “credential information” is any data, set of data, encryption scheme, key, and/or transmission protocol used by a particular device (e.g., a “credential device”) to authenticate and/or verify its authenticity with a reader, mobile device, and/or interrogator.

[0018] The phrases “at least one”, “one or more”, and “and/or” are open-ended expressions that are both conjunctive and disjunctive in operation. For example, each of the expressions “at least one of A, B and C”, “at least one of A, B, or C”, “one or more of A, B, and C”, “one or more of A, B, or C” and “A, B, and/or C” means A alone, B alone, C alone, A and B together, A and C together, B and C together, or A, B and C together. When each one of A, B, and C in the above expressions refers to an element, such as X, Y, and Z, or class of elements, such as X_1 - X_n , Y_1 - Y_m , and Z_1 - Z_o , the phrase is intended to refer to a single element selected from X, Y, and Z, a combination of elements selected from the same class (e.g., X_1

and X_2) as well as a combination of elements selected from two or more classes (e.g., Y_1 and Z_0).

[0019] The term “a” or “an” entity refers to one or more of that entity. As such, the terms “a” (or “an”), “one or more” and “at least one” can be used interchangeably herein. It is also to be noted that the terms “comprising”, “including”, and “having” can be used interchangeably.

[0020] The terms “determine,” “calculate,” and “compute,” and variations thereof, as used herein, are used interchangeably and include any type of methodology, process, mathematical operation, or technique.

[0021] The term “means” as used herein shall be given its broadest possible interpretation in accordance with 35 U.S.C., Section 112, Paragraph 6. Accordingly, a claim incorporating the term “means” shall cover all structures, materials, or acts set forth herein, and all of the equivalents thereof. Further, the structures, materials or acts and the equivalents thereof shall include all those described in the summary of the invention, brief description of the drawings, detailed description, abstract, and claims themselves.

[0022] The term “module” as used herein refers to any known or later developed hardware, software, firmware, artificial intelligence, fuzzy logic, or combination of hardware and software that is capable of performing the functionality associated with that element.

[0023] It should be understood that every maximum numerical limitation given throughout this disclosure is deemed to include each and every lower numerical limitation as an alternative, as if such lower numerical limitations were expressly written herein. Every minimum numerical limitation given throughout this disclosure is deemed to include each and every higher numerical limitation as an alternative, as if such higher numerical limitations were expressly written herein. Every numerical range given throughout this disclosure is deemed to include each and every narrower numerical range that falls within such broader numerical range, as if such narrower numerical ranges were all expressly written herein.

[0024] The preceding is a simplified summary of the disclosure to provide an understanding of some aspects of the disclosure. This summary is neither an extensive nor exhaustive overview of the disclosure and its various aspects, embodiments, and configurations. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure but to present selected concepts of the disclosure in a simplified form as an introduction to the more detailed description presented below. As will

be appreciated, other aspects, embodiments, and configurations of the disclosure are possible utilizing, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The accompanying drawings are incorporated into and form a part of the specification to illustrate several examples of the present disclosure. These drawings, together with the description, explain the principles of the disclosure. The drawings simply illustrate preferred and alternative examples of how the disclosure can be made and used and are not to be construed as limiting the disclosure to only the illustrated and described examples. Further features and advantages will become apparent from the following, more detailed, description of the various aspects, embodiments, and configurations of the disclosure, as illustrated by the drawings referenced below.

[0026] Fig. 1 is a diagram depicting an access control system in accordance with embodiments of the present disclosure;

[0027] Fig. 2 is a block diagram depicting a wearable device or components thereof in accordance with embodiments of the present disclosure;

[0028] Fig. 3 is a block diagram depicting a mobile device or components thereof in accordance with embodiments of the present disclosure

[0029] Fig. 4A is a block diagram depicting a first operational environment of a wearable device and a mobile device in accordance with embodiments of the present disclosure;

[0030] Fig. 4B is a block diagram depicting a second operational environment of a wearable device and a mobile device in accordance with embodiments of the present disclosure; and

[0031] Fig. 5 is a flow chart depicting a method of selectively authenticating a user based on a context associated with an access control system in accordance with embodiments of the present disclosure.

DETAILED DESCRIPTION

[0032] COPYRIGHT AND LEGAL NOTICES

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyrights whatsoever.

[0033] Before any embodiments of the disclosure are explained in detail, it is to be understood that the disclosure is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the following drawings. The disclosure is capable of other embodiments and of being practiced or of being carried out in various ways. Also, it is to be understood that the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of “including,” “comprising,” or “having” and variations thereof herein is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

[0034] Fig. 1 is a diagram depicting an access control system 100 for authenticating a user 102 via wearable devices 104 in accordance with embodiments of the present disclosure. In one embodiment, the access control system 100 comprises at least one reading device 112, at least one wearable device 104, and at least one portable device 108. The reading device 112 may include an access data memory 116. The access data memory 116 may be configured to store access information, identification data, rules, program instructions, and/or other data associated with performing access operations of an access control system 100. In some embodiments, the reading device 112 may be configured to communicate with an access data memory 116 across a communication network 128. The access data memory 116 may be located remotely, locally, and/or locally and remotely, from the reading device 112.

[0035] The wearable device 104 and/or the mobile device 108 may be configured to communicate with a reading device 112 across one or more wireless communication connections. These one or more wireless communication connections can include communications via at least one of conventional radio protocols, proximity-based wireless communication protocols, Bluetooth™, BLE, infrared, audible, NFC, RF, and other wireless communication networks and/or protocols. In some cases, communications between the wearable device 104 and the reading device 112 may be established automatically when the wearable device 104 enters an active zone of an interrogating reading device 112. In one embodiment, the active zone of the reading device 112 may be defined as a three-dimensional space where the intensity of RF signals emitted by the reading device 112 exceeds a threshold of sensitivity of the wearable device 104 and the intensity of RF signals emitted by the wearable device 108 exceeds a threshold of sensitivity of the reading device 112.

[0036] In some embodiments, the wearable device 104 and/or the mobile device 108 may be configured to communicate with a reading device 112 across a communication network

128. The communication network 128 can include communication via at least one of conventional radio networks, wireless communication networks, Zig-Bee, GSM, CDMA, WiFi, and/or using other communication networks and/or protocols as provided herein.

[0037] In one embodiment, authentication may be required between the wearable device 104 and the reading device 112 before further communications are enabled. Additionally or alternatively, authentication may be required between the wearable device 104 and the mobile device 108 before further communications are enabled. In any event, the further communications may provide communications in which access control information (e.g., keys, codes, credentials, etc.) are shared. In some embodiments, the authentication may be provided via one-way or mutual authentication. Examples of authentication may include, but are not limited to, simple authentication based on site codes, trusted data formats, shared secrets, and/or the like. As can be appreciated, access control information is more sensitive and may require more involved validation via, for example, an encrypted exchange of access control information.

[0038] In some embodiments, the reading device 112 may be configured to request access control information from the wearable device 104 and/or the mobile device 108. This information may be used to validate the wearable device 104. Validation may include referring to information stored in access data memory 120 or some other memory associated with the wearable device 104 and/or the mobile device 108. Typically, a reading device 112 is associated with a particular asset (e.g., a door protecting access to a secure room, a computer lock protecting sensitive information or computer files, a lock on a safe, and the like). In one embodiment, the wearable device 104 and/or the mobile device 108 may be validated via one or more components of the access control system 100. Once the wearable device 104 and/or the mobile device 108 is authenticated, credential information associated with the wearable device 104 may be validated. During this process, the reading device 112 may generate signals facilitating execution of the results of interrogating the wearable device 104 (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, provides access to a computer system, provides access to a particular document, and the like). Alternatively, the access server 120 may generate such signals.

[0039] In accordance with embodiments of the present disclosure, the reading device 112 may collect access control information associated with the wearable device 104 before an access control decision can be made. For example, the reading device 112 may require

credential information stored on the wearable device 104 to validate the wearable device 104. The validity of the wearable device 104 may be based on the validity of an associated mobile device 108, or vice versa. In one embodiment, upon validating credential information stored on the wearable device 104, the reading device 112 generates signals facilitating execution of the results of interrogating the wearable device 104 and/or the mobile device 108 (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, provides access to a computer system, provides access to a particular document, and the like). As provided above, the access server 120 may generate such signals.

[0040] The access server 120 may include a processor, a memory, and one or more inputs/outputs. The memory of the access server 120 may be used in connection with the execution of application programming or instructions by the processor, and for the temporary or long term storage of program instructions and/or data. As examples, the memory may comprise RAM, DRAM, SDRAM, or other solid state memory. Additionally or alternatively, the access server 120 may communicate with an access data memory 116. Like the memory of the access server 120, the access data memory 116 may comprise a solid state memory or devices. The access data memory 116 may comprise a hard disk drive or other random access memory.

[0041] In some embodiments, the reading device 112 may be configured to communicate with one or more devices across a communication network 128. For example, the reading device 112 may communicate with a wearable device 104 and/or a mobile device 108 across the communication network 128. Among other things, this communication can allow for back-end authentication and/or provide notifications from the reading device 112 to the mobile device 108. The communication network 128 may comprise any type of known communication medium or collection of communication media and may use any type of protocols to transport messages between endpoints. The communication network 128 may include wired and/or wireless communication technologies. The Internet is an example of the communication network 128 that constitutes an Internet Protocol (IP) network consisting of many computers, computing networks, and other communication devices located all over the world, which are connected through many telephone systems and other means. Other examples of the communication network 128 include, without limitation, a standard Plain Old Telephone System (POTS), an Integrated Services Digital Network (ISDN), the Public Switched Telephone Network (PSTN), a Local Area Network (LAN), a Wide Area Network

(WAN), a Session Initiation Protocol (SIP) network, a Voice over Internet Protocol (VoIP) network, a cellular network, RS-232, similar networks used in access control systems between readers and control panels, and any other type of packet-switched or circuit-switched network known in the art. In addition, it can be appreciated that the communication network 128 need not be limited to any one network type, and instead may be comprised of a number of different networks and/or network types. Moreover, the communication network 128 may comprise a number of different communication media such as coaxial cable, copper cable/wire, fiber-optic cable, antennas for transmitting/receiving wireless messages, and combinations thereof.

[0042] In some embodiments, the access control system 100 may include at least one communication device 124. A communication device 124 may include, but is not limited to, a mobile phone, smartphone, smart watch, soft phone, telephone, intercom device, computer, tablet, mobile computer, alarm, bell, notification device, pager, and/or other device configured to convert received electrical and/or communication signals. In one embodiment, the communication device 124 may be used to receive communications sent from the wearable device 104 via the reading device 112.

[0043] Referring now to Fig. 2, a block diagram depicting a wearable device 104 is shown in accordance with embodiments of the present disclosure. The wearable device 104 may include one or more components, such as, a memory 204, a processor 208, an antenna 212A-N, a communications module 216, a wearable sensor 220, a motion sensor 224, and a location sensor 228. In some embodiments, the wearable device 104 may further include a power module. The processor 208 may be an application specific integrated circuit (ASIC), microprocessor, programmable controller, or the like.

[0044] The memory 204 of the wearable device 104 may be used in connection with the execution of application programming or instructions by the processor 208, and for the temporary or long term storage of program instructions and/or data. The memory 204 may contain executable functions that are used by the processor 208 to run other components of the wearable device 104. In one embodiment, the memory 204 may be configured to store credential information. For instance, the credential information may include, but is not limited to, unique identifications, manufacturer identification, passwords, keys, encryption schemes, transmission protocols, and the like. As examples, the memory 204 may comprise RAM, DRAM, SDRAM, or other solid state memory.

[0045] The one or more antennas 212A-N may be configured to enable wireless communications between the wearable device 104 and a reading device 112 and/or mobile device 108. As can be appreciated, the antenna(s) 212A-N may be arranged to operate using one or more wireless communication protocols and operating frequencies including, but not limited to, Bluetooth®, NFC, Zig-Bee, GSM, CDMA, WiFi, RF, and the like. By way of example, the antenna(s) 212A-N may be RF antenna(s), and as such, may transmit RF signals through free-space to be received by a reading device 112 having an RF transceiver.

[0046] In some embodiments, the wearable device 104 may include a power module. The power module may be configured to provide power to the parts of the wearable device 104 in order to operate. The power module may store power in a capacitor of the power module. In one embodiment, electronics in the power module may store energy in the capacitor and turn off when an RF field is present. This arrangement can ensure that energy is presented to the wearable device 104 minimizing any effect on read distance. Although the wearable device 104 may be configured to receive power passively from an electrical field of a reading device 112, it should be appreciated that the wearable device 104 may provide its own power. For example, the power module may include a battery or other power source to supply power to parts of the wearable device 104.

[0047] The wearable device 104 may include a communications module 216 that is configured to communicate with one or more different systems or devices either remotely or locally to the wearable device 104. Thus, the communications module 216 can send or receive messages from other wearable devices 104, from mobile devices 108, from reading devices 112, from communication devices 124, from access servers 120, from access control systems, or from other systems. In some embodiments, the communicated information may be provided to, or exchanged with, other components within the wearable device 104.

[0048] Embodiments of the wearable device 104 may include at least one wearable sensor 220. Among other things, the wearable sensor 220 may be configured to detect an attachment and/or detachment of the wearable to a user 102. For instance, a wearable device 104 may include a clasp that is required to be opened in attaching and/or removing the wearable from a user 102 (e.g., similar to a clasp of a watch band, bracelet, earring, necklace, etc.). The actuation of the clasp may be detected by a wearable sensor 220 of the wearable device 104. Examples of other wearable sensors 220 may include, but are in no way limited to, contact sensors, switches, proximity sensors, etc., and/or combinations thereof.

[0049] In some embodiments, the wearable device 104 may employ one or more sensors 220, 224, 228 that are configured to detect information corresponding to a state of the wearable device 104. The wearable sensors 220 may include, but are not limited to, one or more biometric sensors (e.g., heart rate, body temperature and/or heat signature, blood pressure, etc.), capacitive sensors, light sensors, temperature sensors, pressure sensors, contact sensors, combinations thereof, and the like. It is an aspect of the present disclosure that the processor 208 of the wearable device 104 may receive the sensor information and determine whether the wearable device 104 is being worn by a user 102, whether the wearable device 104 has been removed from a user 102, whether any interruption to the wearing of the wearable device 104 is detected (e.g., whether the wearable device 104 has been continuously worn by, and/or removed from, a user 102, timing associated therewith, etc.). By way of example, the biometric sensor of the wearable sensors 220 may detect biometric characteristics associated with a user 102 wearing the wearable device 104 (e.g., a heart rate, a blood pressure, a body temperature, skin contact data, etc.). The biometric characteristics may be used to determine a state of the wearable device 104 (e.g., being worn or not, etc.) and/or determine an identity of a user 102 wearing the wearable device 104 (e.g., via comparing collected biometric characteristics to baseline characteristics stored in a memory and associated with the user 102, etc.).

[0050] The motion sensors 224 may include one or more of a gyroscope, accelerometer, transducer, and/or other mechanical detection component that are each configured to detect a force and/or motion associated with the wearable device 104. This detected motion of the wearable device 104 may be compared, via the processor 208 of the wearable device 104, to known motion profiles stored in the memory 204 or other associated memory in determining a state of the wearable device 104. For instance, a particular motion of the wearable device 104 may indicate that the wearable device 104 is being worn by a user 102. In one embodiment, the detected motion of a wearable device 104 may be compared to the detected motion of an associated mobile device 108, or vice versa, to generate comparison results. The association of the mobile device 108 may be between the wearable device 104 and/or between a user 102 having the wearable device 104. In any event, the comparison results may indicate similarities between the motion of the wearable device 104 and a motion of the mobile device 108 over time. Similar motion comparison results between the wearable device 104 and the mobile device 108 may allow a continuous authentication for the user 102. Dissimilar motion comparison results between the wearable device 104 and the mobile device

108 may be used to disable or discontinue the continuous authentication for the user 102. In one embodiment, an extreme motion detected at one device (e.g., the wearable device 104 or the mobile device 108) but not the other device may cause continuous authentication to be broken, discontinued, and/or disallowed.

[0051] The wearable device 104 may include one or more location sensors 228. The location sensors may be configured to determine a geographical location and/or position of the wearable device 104. In one embodiment, this location may be based on Global Positioning System (GPS) data provided by a GPS module of the wearable device 104. In some embodiments, the location of the wearable device 104 may be provided based on cell tower data, WiFi information, iBeacon information, and/or some other location information provided by a location module and/or a communications module 216 of the wearable device 104. The location of a mobile device 108 may be determined in a similar, if not identical, manner as determining the location of the wearable device 104. In some embodiments, the continuous authentication of a user 102 may be based on determining a difference, or distance, between the location of the wearable device 104 and the location of the mobile device 108. For example, once the distance passes a specific threshold value, the continuous authentication may be disabled, discontinued, and/or keys (e.g., credential and/or access control keys, etc.) may be revoked.

[0052] Fig. 3 shows a block diagram depicting a mobile device 108 in accordance with embodiments of the present disclosure. The mobile device 108 may correspond to any type of electronic device and, as the name suggests, the electronic device may be portable in nature. As some examples, the mobile device 108 may correspond to a cellular phone or smartphone carried by a user. Other examples of a mobile device 108 include, without limitation, wearable devices (e.g., glasses, watches, shoes, clothes, jewelry, wristbands, stickers, etc.). The mobile device 108, as shown in Figs. 1 and 3, may be provided with a key vault 312 that stores one or a plurality of keys. The key(s) may be communicated to a reader 112 in connection with a holder of the mobile device 108 attempting to gain access to an asset protected by the reader 112. As an example, the mobile device 108 may be presented to the reader 112 by a user 102 or holder of the mobile device 108.

[0053] If NFC is being used for the communication channel, then the reader 112 and mobile device 108 may have their interfaces/antennas inductively coupled to one another at which point the reader and/or mobile device 108 will authenticate or mutually authenticate with one another. Following authentication, the reader 112 may request a key or multiple

keys from the mobile device 108, or the mobile device 108 may offer a key or multiple keys to the reader 112. Upon receiving the key(s) from the mobile device 108, the reader 112 may analyze the key(s) and determine if the key(s) are valid and, if so, allow the holder/user of the mobile device 108 access to the asset protected by the reader 112. It should be appreciated that the mobile device 108 may alternatively or additionally be configured to analyze information received from the reader 112 in connection with making an access control decision and/or in connection with making a decision whether or not to provide key(s) to the reader 112. Examples of technologies that can be used by the mobile device 108 to make an access control decision for itself are further described in U.S. Patent No. 8,074,271 to Davis et al. and U.S. Patent No. 7,706,778 to Lowe, both of which are hereby incorporated herein by reference in their entirety.

[0054] If BLE or some other non-inductive protocol (e.g., Wi-Fi) is being used for the communication channel, then the reader 112 and mobile device 108 may perform a discovery routine prior to pairing with one another or otherwise connecting to establish the communication channel. After the channel is established, however, the reader 112 and mobile device 108 may then authenticate one another and exchange relevant information, such as the key(s), to enable an access control decision to be made. If a positive access control decision is made (e.g., it is determined that the key(s) are valid and the mobile device 108 is allowed to access the asset protected by the reader 112), then the reader 112 may initiate one or more actions to enable the holder/user 102 of the mobile device 108 to access the asset protected by the reader 112.

[0055] The mobile device 108 is shown to include computer memory 304 that stores one or more Operating Systems (O/S) 308 and a key vault 312, among other items. The mobile device 108 is also shown to include a processor 316, one or more drivers 320, a user interface 324, a reader interface 328, a network interface 332, and a power module 336. Suitable examples of a mobile device 108 include, without limitation, smart phones, PDAs, laptops, PCs, tablets, netbooks, wearable devices, and the like.

[0056] The memory 304 may correspond to any type of non-transitory computer-readable medium. In some embodiments, the memory 304 may comprise volatile or non-volatile memory and a controller for the same. Non-limiting examples of memory 304 that may be utilized in the mobile device 108 include RAM, ROM, buffer memory, flash memory, solid-state memory, or variants thereof.

[0057] The O/S 308 may correspond to one or multiple operating systems. The nature of the O/S 308 may depend upon the hardware of the mobile device 108 and the form factor of the mobile device 108. The O/S 308 may be viewed as an application stored in memory 304 that is processor-executable. The O/S 308 is a particular type of general-purpose application that enables other applications stored in memory 304 (e.g., a browser, an email application, an SMS application, etc.) to leverage the various hardware components and driver(s) 320 of the mobile device 108. In some embodiments, the O/S 308 may comprise one or more APIs that facilitate an application's interaction with certain hardware components of the mobile device 108. Furthermore, the O/S 308 may provide a mechanism for viewing and accessing the various applications stored in memory 304 and other data stored in memory 304.

[0058] The processor 316 may correspond to one or many microprocessors that are contained within the housing of the mobile device 108 with the memory 304. In some embodiments, the processor 316 incorporates the functions of the user device's Central Processing Unit (CPU) on a single Integrated Circuit (IC) or a few IC chips. The processor 316 may be a multipurpose, programmable device that accepts digital data as input, processes the digital data according to instructions stored in its internal memory, and provides results as output. The processor 316 implement sequential digital logic as it has internal memory. As with most known microprocessors, the processor 316 may operate on numbers and symbols represented in the binary numeral system.

[0059] The driver(s) 320 may correspond to hardware, software, and/or controllers that provide specific instructions to hardware components of the mobile device 108, thereby facilitating their operation. For instance, the user interface 324, reader interface 328, and network interface 332, may each have a dedicated driver 320 that provides appropriate control signals to effect their operation. The driver(s) 320 may also comprise the software or logic circuits that ensure the various hardware components are controlled appropriately and in accordance with desired protocols. For instance, the driver 320 of the reader interface 328 may be adapted to ensure that the reader interface 328 follows the appropriate proximity-based protocols (e.g., BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, etc.) such that the reader interface 328 can exchange communications with the credential. Likewise, the driver 320 of the network interface 332 may be adapted to ensure that the network interface 332 follows the appropriate network communication protocols (e.g., TCP/IP (at one or more layers in the OSI model), UDP, RTP, GSM, LTE, Wi-Fi, etc.) such that the network interface 332 can exchange communications via the communication network 128. As can be

appreciated, the driver(s) 320 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0060] As mentioned above, the user interface 324 may comprise one or more user input devices and/or one or more user output devices. Examples of suitable user input devices that may be included in the user interface 324 include, without limitation, buttons, keyboards, mouse, touch-sensitive surfaces, pen, camera, microphone, etc. Examples of suitable user output devices that may be included in the user interface 324 include, without limitation, display screens, touchscreens, lights, speakers, etc. It should be appreciated that the user interface 324 may also include a combined user input and user output device, such as a touch-sensitive display or the like.

[0061] The reader interface 328 may correspond to the hardware that facilitates communications with the credential for the mobile device 108. The reader interface 328 may include a Bluetooth interface (e.g., antenna and associated circuitry), a Wi-Fi/802.11N interface (e.g., an antenna and associated circuitry), an NFC interface (e.g., an antenna and associated circuitry), an Infrared interface (e.g., LED, photodiode, and associated circuitry), and/or an Ultrasonic interface (e.g., speaker, microphone, and associated circuitry). In some embodiments, the reader interface 328 is specifically provided to facilitate proximity-based communications with a credential via communication channel or multiple communication channels.

[0062] The network interface 332 may comprise hardware that facilitates communications with other communication devices over the communication network 128. As mentioned above, the network interface 332 may include an Ethernet port, a Wi-Fi card, a Network Interface Card (NIC), a cellular interface (e.g., antenna, filters, and associated circuitry), or the like. The network interface 332 may be configured to facilitate a connection between the mobile device 108 and the communication network 128 and may further be configured to encode and decode communications (e.g., packets) according to a protocol utilized by the communication network 128.

[0063] The power module 336 may include a built-in power supply (e.g., battery) and/or a power converter that facilitates the conversion of externally-supplied AC power into DC power that is used to power the various components of the mobile device 108. In some embodiments, the power module 336 may also include some implementation of surge protection circuitry to protect the components of the mobile device 108 from power surges.

[0064] Referring now to Fig. 4A, a block diagram depicting a first operational environment 400A of a wearable device 104 and a mobile device 108 is shown in accordance with embodiments of the present disclosure. In particular, Fig. 4A shows a user 102 having multiple devices 104, 108 in a communication range of a reading device 112A associated with a non-enterprise location 404A (e.g., a personal property, residential building, home, recreational location, and/or other non-enterprise context, etc.). In one embodiment, the reading device 112A may provide an interrogation signal requesting a personal key to access an asset associated with the non-enterprise location 404A. This signal may be received by at least one of the wearable device 104 and the mobile device 108.

[0065] In some embodiments, the non-enterprise keys associated with a user 102 may be stored on one device but not on the other device. For example, the non-enterprise keys may be stored on the wearable device 104 and the enterprise keys may be stored on the mobile device 108, or vice versa. The non-enterprise keys may be provided to the reading device 112A directly via the wearable device 104 or via the mobile device 108 (e.g., via an application running on the mobile device 108, etc.). For instance, the mobile device 108 may receive one or more access control signals from the reading device 112A. Upon determining (e.g., via the application instructions executed by a processor of the mobile device 108) that the access control signal received corresponds to a request for keys that are stored on the wearable device 104, the mobile device 108 may request the non-enterprise keys from the wearable device 104. In response to the request, the keys may be presented to the reading device 112A via the mobile device 108 or the wearable device 104.

[0066] In one embodiment, the reading device 112A may provide a signal to one or more devices 104, 108 within a communication range of the device 112A, where the signal is configured to illicit a particular response from the one or more devices 104, 108. For example, the signal may only be capable of being decoded by one of the devices while remaining encoded to the other of the devices. In Fig. 4A, a non-enterprise key request signal may be provided to each device 104, 108 via the reading device 112A. The mobile device 108 may be configured as an enterprise device with enterprise credentials and/or keys, and as such, may not be able to decode the non-enterprise key request from the reading device 112A. However, the wearable device 104 may receive this signal and decode the signal as a request for the non-enterprise key request. In this case, the wearable device 104 may send the non-enterprise keys stored thereon via a signal transmitted by the wearable device 104 to the reading device 112A.

[0067] As shown in Fig. 4A, a menu 408A may be presented to the user 102 via one or more displays associated with the first operational environment 400A. Although shown as rendered to the mobile device 108 display, it should be appreciated that the menu 408A may be rendered to a display or graphical user interface of the reading device 112A, mobile device 108, wearable device 104, communication device 124, access server 120, and/or some other device associated with the access control system 100. The menu may include an identification of the context (e.g., non-enterprise, enterprise, home, recreational, etc.) of the access control, a user identification, a location of the key required to gain access, and/or other information associated with the access control and/or operational environment 400A.

[0068] Fig. 4B shows a block diagram depicting a second operational environment 400B of a wearable device 104 and a mobile device 108 in accordance with embodiments of the present disclosure. Specifically, Fig. 4B shows a user 102 having multiple devices 104, 108 in a communication range of a reading device 112B associated with an enterprise location 404B (e.g., a business property, corporate building, work, company location, and/or other enterprise context, etc.). In one embodiment, the reading device 112B may provide an interrogation signal requesting an enterprise key to access an asset associated with the enterprise location 404B. This signal may be received by at least one of the wearable device 104 and the mobile device 108.

[0069] In some embodiments, the enterprise keys associated with a user 102 may be stored on one device but not on the other device. By way of example, the enterprise keys may be stored on the mobile device 108 and the non-enterprise keys may be stored on the wearable device 104, or vice versa. The enterprise keys may be provided to the reading device 112B via the mobile device 108 (e.g., via an application running on the mobile device 108, etc.). For instance, the mobile device 108 may receive one or more access control signals from the reading device 112A. Upon determining (e.g., via the application instructions executed by a processor of the mobile device 108) that the access control signal received corresponds to a request for keys that are stored on the mobile device 108, the mobile device 108 may retrieve the enterprise keys from a memory associated with the mobile device 108. In response to the request, the keys may be presented to the reading device 112B via the mobile device 108.

[0070] In one embodiment, the reading device 112B may provide a signal to one or more devices 104, 108 within a communication range of the device 112B, where the signal is configured to illicit a particular response from the one or more devices 104, 108. For example, the signal may only be capable of being decoded by one of the devices while

remaining encoded to the other of the devices. In Fig. 4B, an enterprise key request signal may be provided to each device 104, 108 via the reading device 112B. The wearable device 104 may be configured as a non-enterprise device with personal credentials and/or keys, and as such, may not be able to decode the enterprise key request from the reading device 112B. However, the mobile device 108 may receive this signal and decode the signal as a request for the enterprise key request. In this case, the mobile device 108 may send the enterprise keys stored thereon via a signal transmitted by the mobile device 108 to the reading device 112B.

[0071] As shown in Fig. 4B, a menu 408B may be presented to the user 102 via one or more displays associated with the second operational environment 400B. Although shown as rendered to the mobile device 108 display, it should be appreciated that the menu 408A may be rendered to a display or graphical user interface of the reading device 112B, mobile device 108, wearable device 104, communication device 124, access server 120, and/or some other device associated with the access control system 100. The menu may include an identification of the context (e.g., non-enterprise, enterprise, home, recreational, etc.) of the access control, access control level, a user identification, a location of the key required to gain access, and/or other information associated with the access control and/or operational environment 400B. The menu 400B associated with the second operational environment 400B may be different in appearance, behavior, and/or content when compared to the menu 408A associated with the first operational environment 400A.

[0072] Fig. 5 is a flow chart depicting a method 500 of selectively authenticating a user based on a context associated with an access control system 100 in accordance with embodiments of the present disclosure. While a general order for the steps of the method 500 is shown in Fig. 5, the method 500 can include more or fewer steps or can arrange the order of the steps differently than those shown in Fig. 5. Generally, the method 500 starts with a start operation 504 and ends with an end operation 528. The method 500 can be executed as a set of computer-executable instructions executed by a computer system and encoded or stored on a computer readable medium. Hereinafter, the method 500 shall be explained with reference to the systems, components, modules, environments, software, etc. described in conjunction with Figs. 1-4.

[0073] The method 500 begins at step 504 and proceeds by receiving an access control signal from a reading device 112 (step 508). The signal may be received by the wearable device 104, the mobile device 108, and/or a combination thereof. In some embodiments, the

signal may be configured to be interpreted by a particular device while remaining uninterpretable to another device.

[0074] Next, the method 500 proceeds by determining whether the signal received is an enterprise or non-enterprise signal (step 512). In some embodiments, this determination may be made by an application running on the mobile device 108. In one embodiment, this determination may be made by a device 104, 108 receiving and automatically interpreting the signal. In the event that the signal cannot be interpreted by a particular device the other device may be configured to interpret the signal. If the signal is neither an enterprise nor non-enterprise signal, the method 500 ends at step 528. In other embodiments, the transmitter of the signal (e.g., the reader 112) may include an identifier of the reader or a site code indicating whether the reader 112 is associated with a home asset or an enterprise asset. The identifier may be used to enable the device(s) 104, 108 to determine whether the signal is an enterprise signal or a non-enterprise signal.

[0075] In the event that the signal is an enterprise signal, the mobile device 108 may provide the enterprise key stored thereon based on rules stored in a memory associated with the mobile device 108 (step 516). The key may be provided via at least one signal that is transmitted from the mobile device 108.

[0076] In the event that the signal is determined to be a non-enterprise, or personal, signal, the method 500 may retrieve the personal key from a memory 204 of the wearable device 104. Retrieving the personal key may include exchanging messages between the mobile device 108 and the wearable device 104. In one embodiment, retrieving the personal key may include establishing a communication path between the wearable device 104 and the reading device 112. In yet another embodiment, retrieving the personal key may include sending, via the mobile device 108, a signal to the reading device 112 requesting that the reading device 112 interrogate the wearable device 104 for the personal key directly.

[0077] The method 500 continues by providing the personal key to the reading device 112 based on rules stored in memory. The personal key may be provided via at least one signal that is transmitted from the wearable device 104 and/or the mobile device 108. The method 500 ends at step 528.

[0078] The exemplary systems and methods of this disclosure have been described in relation to wearable devices, systems, and methods in an access control system. However, to avoid unnecessarily obscuring the present disclosure, the preceding description omits a number of known structures and devices. This omission is not to be construed as a limitation

of the scopes of the claims. Specific details are set forth to provide an understanding of the present disclosure. It should, however, be appreciated that the present disclosure may be practiced in a variety of ways beyond the specific detail set forth herein. Moreover, it should be appreciated that the methods disclosed herein may be executed via a wearable device, a mobile device, a reading device, a communication device, and/or an access server of an access control system, etc.

[0079] Furthermore, while the exemplary aspects, embodiments, options, and/or configurations illustrated herein show the various components of the system collocated, certain components of the system can be located remotely, at distant portions of a distributed network, such as a LAN and/or the Internet, or within a dedicated system. Thus, it should be appreciated, that the components of the system can be combined in to one or more devices, such as a Personal Computer (PC), laptop, netbook, smart phone, Personal Digital Assistant (PDA), tablet, etc., or collocated on a particular node of a distributed network, such as an analog and/or digital telecommunications network, a packet-switch network, or a circuit-switched network. It will be appreciated from the preceding description, and for reasons of computational efficiency, that the components of the system can be arranged at any location within a distributed network of components without affecting the operation of the system. For example, the various components can be located in a switch such as a PBX and media server, gateway, in one or more communications devices, at one or more users' premises, or some combination thereof. Similarly, one or more functional portions of the system could be distributed between a telecommunications device(s) and an associated computing device.

[0080] Furthermore, it should be appreciated that the various links connecting the elements can be wired or wireless links, or any combination thereof, or any other known or later developed element(s) that is capable of supplying and/or communicating data to and from the connected elements. These wired or wireless links can also be secure links and may be capable of communicating encrypted information. Transmission media used as links, for example, can be any suitable carrier for electrical signals, including coaxial cables, copper wire and fiber optics, and may take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

[0081] Also, while the flowcharts have been discussed and illustrated in relation to a particular sequence of events, it should be appreciated that changes, additions, and omissions to this sequence can occur without materially affecting the operation of the disclosed embodiments, configuration, and aspects.

[0082] A number of variations and modifications of the disclosure can be used. It would be possible to provide for some features of the disclosure without providing others.

[0083] Optionally, the systems and methods of this disclosure can be implemented in conjunction with a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit element(s), an ASIC or other integrated circuit, a digital signal processor, a hard-wired electronic or logic circuit such as discrete element circuit, a programmable logic device or gate array such as PLD, PLA, FPGA, PAL, special purpose computer, any comparable means, or the like. In general, any device(s) or means capable of implementing the methodology illustrated herein can be used to implement the various aspects of this disclosure. Exemplary hardware that can be used for the disclosed embodiments, configurations and aspects includes computers, handheld devices, telephones (e.g., cellular, Internet enabled, digital, analog, hybrids, and others), and other hardware known in the art. Some of these devices include processors (e.g., a single or multiple microprocessors), memory, nonvolatile storage, input devices, and output devices. Furthermore, alternative software implementations including, but not limited to, distributed processing or component/object distributed processing, parallel processing, or virtual machine processing can also be constructed to implement the methods described herein.

[0084] In yet another embodiment, the disclosed methods may be readily implemented in conjunction with software using object or object-oriented software development environments that provide portable source code that can be used on a variety of computer or workstation platforms. Alternatively, the disclosed system may be implemented partially or fully in hardware using standard logic circuits or VLSI design. Whether software or hardware is used to implement the systems in accordance with this disclosure is dependent on the speed and/or efficiency requirements of the system, the particular function, and the particular software or hardware systems or microprocessor or microcomputer systems being utilized.

[0085] In yet another embodiment, the disclosed methods may be partially implemented in software that can be stored on a storage medium, executed on programmed general-purpose computer with the cooperation of a controller and memory, a special purpose computer, a microprocessor, or the like. In these instances, the systems and methods of this disclosure can be implemented as program embedded on personal computer such as an applet, JAVA® or CGI script, as a resource residing on a server or computer workstation, as a routine embedded in a dedicated measurement system, system component, or the like. The system can also be

implemented by physically incorporating the system and/or method into a software and/or hardware system.

[0086] Although the present disclosure describes components and functions implemented in the aspects, embodiments, and/or configurations with reference to particular standards and protocols, the aspects, embodiments, and/or configurations are not limited to such standards and protocols. Other similar standards and protocols not mentioned herein are in existence and are considered to be included in the present disclosure. Moreover, the standards and protocols mentioned herein and other similar standards and protocols not mentioned herein are periodically superseded by faster or more effective equivalents having essentially the same functions. Such replacement standards and protocols having the same functions are considered equivalents included in the present disclosure.

[0087] The present disclosure, in various aspects, embodiments, and/or configurations, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various aspects, embodiments, configurations embodiments, subcombinations, and/or subsets thereof. Those of skill in the art will understand how to make and use the disclosed aspects, embodiments, and/or configurations after understanding the present disclosure. The present disclosure, in various aspects, embodiments, and/or configurations, includes providing devices and processes in the absence of items not depicted and/or described herein or in various aspects, embodiments, and/or configurations hereof, including in the absence of such items as may have been used in previous devices or processes, e.g., for improving performance, achieving ease and/or reducing cost of implementation.

[0088] The foregoing discussion has been presented for purposes of illustration and description. The foregoing is not intended to limit the disclosure to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the disclosure are grouped together in one or more aspects, embodiments, and/or configurations for the purpose of streamlining the disclosure. The features of the aspects, embodiments, and/or configurations of the disclosure may be combined in alternate aspects, embodiments, and/or configurations other than those discussed above. This method of disclosure is not to be interpreted as reflecting an intention that the claims require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed aspect, embodiment, and/or configuration. Thus,

the following claims are hereby incorporated into this Detailed Description, with each claim standing on its own as a separate preferred embodiment of the disclosure.

[0089] Moreover, though the description has included description of one or more aspects, embodiments, and/or configurations and certain variations and modifications, other variations, combinations, and modifications are within the scope of the disclosure, e.g., as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative aspects, embodiments, and/or configurations to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

[0090] Embodiments include a method, comprising: receiving, from a reading device of an access control system, an interrogation signal requesting an access key for the access control system; determining an operational environment of the access control system; determining, from two or more devices and based on the determined operational environment, a particular device having the access key, wherein a first device of the two or more devices is associated with a first operational environment and a second device of the two or more devices is associated with a second operational environment; and retrieving the access key from the particular device for presentation to the reading device.

[0091] Aspects of the above method include wherein only one device of the two or more devices has the access key stored thereon. Aspects of the above method include wherein the operational environment identifies whether the access control system is associated with an enterprise or non-enterprise asset. Aspects of the above method include wherein prior to retrieving the access key, the method further comprises: rendering, via a display, a menu associated with the operational environment. Aspects of the above method include wherein the menu is rendered to at least one of the reading device, a mobile device, a wearable device, a communication device, and an access server. Aspects of the above method include wherein an identification of the operational environment is rendered via the display. Aspects of the above method include wherein the first device or the second device is a wearable device, and wherein the other of the first device or the second device is a mobile device. Aspects of the above method include wherein the first operational environment is a non-enterprise environment, and wherein the second operational environment is an enterprise environment. Aspects of the above method include wherein the first device includes a non-enterprise access

key and the second device includes an enterprise access key, wherein the first device does not include the enterprise access key and the second device does not include the non-enterprise access key, and wherein the access key is one of the non-enterprise access key or the enterprise access key. Aspects of the above method include wherein the interrogation signal is received by the mobile device for a non-enterprise access key stored in a memory of the wearable device, and wherein the mobile device sends the non-enterprise access key across a wireless communication network to the reading device. Aspects of the above method include wherein the interrogation signal is received by the mobile device for a non-enterprise access key stored in a memory of the wearable device, and wherein the wearable device is caused to send the non-enterprise access key across a wireless communication network to the reading device.

[0092] Embodiments include a non-transitory computer readable medium having stored thereon instructions that, when executed by a processor, performs the above method or methods.

[0093] Embodiments include an access control system, comprising: a reading device configured to receive access information transmitted via at least one device in the access control system; a wearable device, comprising: a memory having a first access key stored thereon; and a controller configured to receive access control signals and determine to provide the first access key to a requesting device; and a mobile device, comprising: a memory having a second access key stored thereon; a communications module configured to enable communications between at least one of the reading device and the wearable device; and a processor configured to receive, from the reading device, an interrogation signal requesting an access key for the access control system, determine an operational environment of the access control system, determine, based on the determined operational environment, a particular device from the wearable device and mobile device having the access key, wherein a first device of the wearable device and mobile device is associated with a first operational environment and a second device of the wearable device and mobile device is associated with a second operational environment, and retrieve the access key from the particular device for presentation to the reading device.

[0094] Aspects of the above access control system include wherein the communications module of the mobile device is further configured to retrieve the access key from the wearable device in response to receiving an input releasing the key from the wearable device to the mobile device. Aspects of the above access control system further comprise: an access

processing module, configured to interpret the information received from the particular device and perform an access function based at least partially on whether the access key is valid. Aspects of the above access control system include wherein the mobile device further comprises a display configured to render a menu associated with the operational environment. Aspects of the above access control system include wherein the wearable device further comprises a display configured to render a menu associated with the operational environment. Aspects of the above access control system include wherein the reading device further comprises a display configured to render a menu associated with the operational environment.

[0095] Embodiments include a device, comprising: a memory including at least one access key stored thereon; a communications module configured to enable communications between at least one of a reading device and an associated device; and a processor configured to receive, from the reading device, an interrogation signal requesting an access key for the access control system, determine an operational environment of the access control system, determine, from the device and the associated device, a particular device having the access key, wherein a first device of the device and the associated device is associated with a first operational environment and a second device of the device and the associated device is associated with a second operational environment, and retrieve the access key from the particular device for transmission to the reading device.

[0096] Aspects of the above device include wherein the access key is stored on the associated device and not on the device, and wherein the device causes the associated device to transmit the access key to the reading device.

[0097] Any of the steps, functions, and operations discussed herein can be performed continuously and automatically.

[0098] Examples of the processors as described herein may include, but are not limited to, at least one of Qualcomm® Snapdragon® 800 and 801, Qualcomm® Snapdragon® 610 and 615 with 4G LTE Integration and 64-bit computing, Apple® A7 processor with 64-bit architecture, Apple® M7 motion coprocessors, Samsung® Exynos® series, the Intel® Core™ family of processors, the Intel® Xeon® family of processors, the Intel® Atom™ family of processors, the Intel Itanium® family of processors, Intel® Core® i5-4670K and i7-4770K 22nm Haswell, Intel® Core® i5-3570K 22nm Ivy Bridge, the AMD® FX™ family of processors, AMD® FX-4300, FX-6300, and FX-8350 32nm Vishera, AMD® Kaveri processors, Texas Instruments® Jacinto C6000™ automotive infotainment processors, Texas

Instruments® OMAP™ automotive-grade mobile processors, ARM® Cortex™-M processors, ARM® Cortex-A and ARM926EJ-S™ processors, other industry-equivalent processors, and may perform computational functions using any known or future-developed standard, instruction set, libraries, and/or architecture.

What Is Claimed Is:

1. A method, comprising:
receiving, from a reading device of an access control system, an interrogation signal requesting an access key for the access control system;
determining an operational environment of the access control system;
determining, from two or more devices and based on the determined operational environment, a particular device having the access key, wherein a first device of the two or more devices is associated with a first operational environment and a second device of the two or more devices is associated with a second operational environment; and
retrieving the access key from the particular device for presentation to the reading device.
2. The method of claim 1, wherein only one device of the two or more devices has the access key stored thereon.
3. The method of claim 1, wherein the operational environment identifies whether the access control system is associated with an enterprise or non-enterprise asset.
4. The method of claim 3, wherein prior to retrieving the access key, the method further comprises:
rendering, via a display, a menu associated with the operational environment.
5. The method of claim 4, wherein the menu is rendered to at least one of the reading device, a mobile device, a wearable device, a communication device, and an access server.
6. The method of claim 5, wherein an identification of the operational environment is rendered via the display.
7. The method of claim 1, wherein the first device or the second device is a wearable device, and wherein the other of the first device or the second device is a mobile device.

8. The method of claim 7, wherein the first operational environment is a non-enterprise environment, and wherein the second operational environment is an enterprise environment.

9. The method of claim 8, wherein the first device includes a non-enterprise access key and the second device includes an enterprise access key, wherein the first device does not include the enterprise access key and the second device does not include the non-enterprise access key, and wherein the access key is one of the non-enterprise access key or the enterprise access key.

10. The method of claim 8, wherein the interrogation signal is received by the mobile device for a non-enterprise access key stored in a memory of the wearable device, and wherein the mobile device sends the non-enterprise access key across a wireless communication network to the reading device.

11. The method of claim 8, wherein the interrogation signal is received by the mobile device for a non-enterprise access key stored in a memory of the wearable device, and wherein the wearable device is caused to send the non-enterprise access key across a wireless communication network to the reading device.

12. A non-transitory computer readable medium having stored thereon instructions that, when executed by a processor, performs the method of claim 1.

13. An access control system, comprising:
a reading device configured to receive access information transmitted via at least one device in the access control system;
a wearable device, comprising:
a memory having a first access key stored thereon; and
a controller configured to receive access control signals and determine to provide the first access key to a requesting device; and
a mobile device, comprising:
a memory having a second access key stored thereon;

a communications module configured to enable communications between at least one of the reading device and the wearable device; and

a processor configured to receive, from the reading device, an interrogation signal requesting an access key for the access control system, determine an operational environment of the access control system, determine, based on the determined operational environment, a particular device from the wearable device and mobile device having the access key, wherein a first device of the wearable device and mobile device is associated with a first operational environment and a second device of the wearable device and mobile device is associated with a second operational environment, and retrieve the access key from the particular device for presentation to the reading device.

14. The access control system of claim 13, wherein the communications module of the mobile device is further configured to retrieve the access key from the wearable device in response to receiving an input releasing the key from the wearable device to the mobile device.

15. The access control system of claim 13, further comprising:
an access processing module, configured to interpret the information received from the particular device and perform an access function based at least partially on whether the access key is valid.

16. The access control system of claim 13, wherein the mobile device further comprises a display configured to render a menu associated with the operational environment.

17. The access control system of claim 13, wherein the wearable device further comprises a display configured to render a menu associated with the operational environment.

18. The access control system of claim 13, wherein the reading device further comprises a display configured to render a menu associated with the operational environment.

19. A device, comprising:
- a memory including at least one access key stored thereon;
 - a communications module configured to enable communications between at least one of a reading device and an associated device; and
 - a processor configured to receive, from the reading device, an interrogation signal requesting an access key for the access control system, determine an operational environment of the access control system, determine, from the device and the associated device, a particular device having the access key, wherein a first device of the device and the associated device is associated with a first operational environment and a second device of the device and the associated device is associated with a second operational environment, and retrieve the access key from the particular device for transmission to the reading device.
20. The device of claim 19, wherein the access key is stored on the associated device and not on the device, and wherein the device causes the associated device to transmit the access key to the reading device.

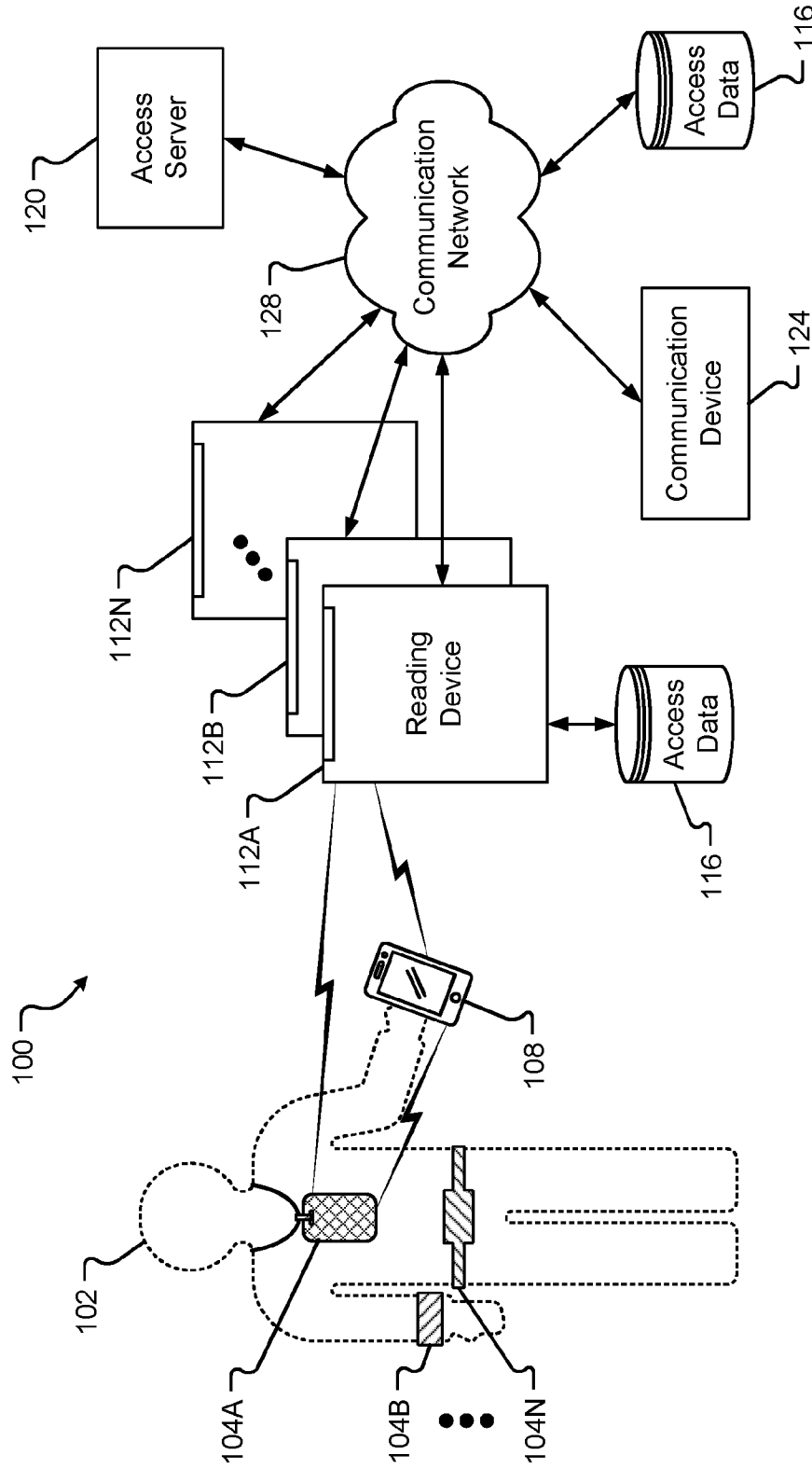
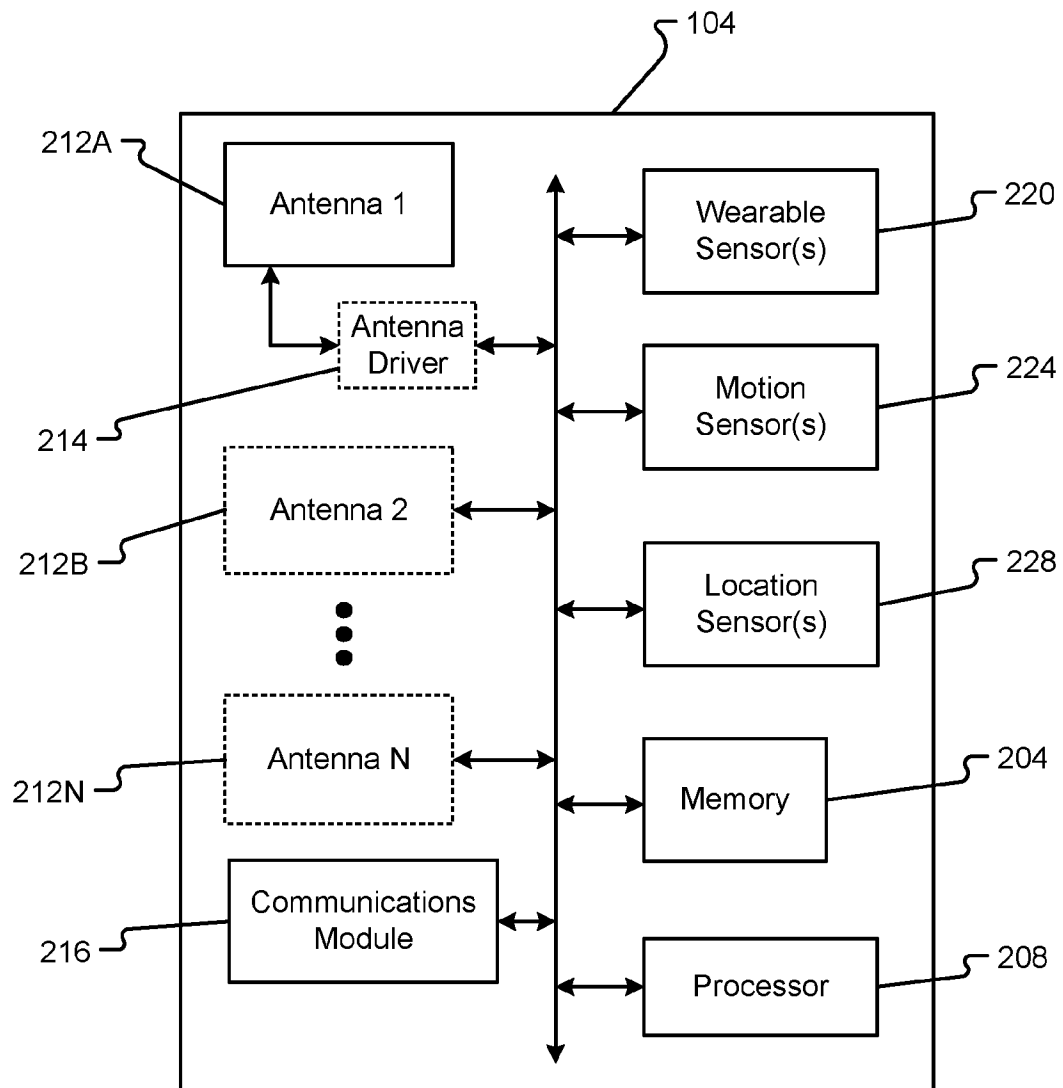
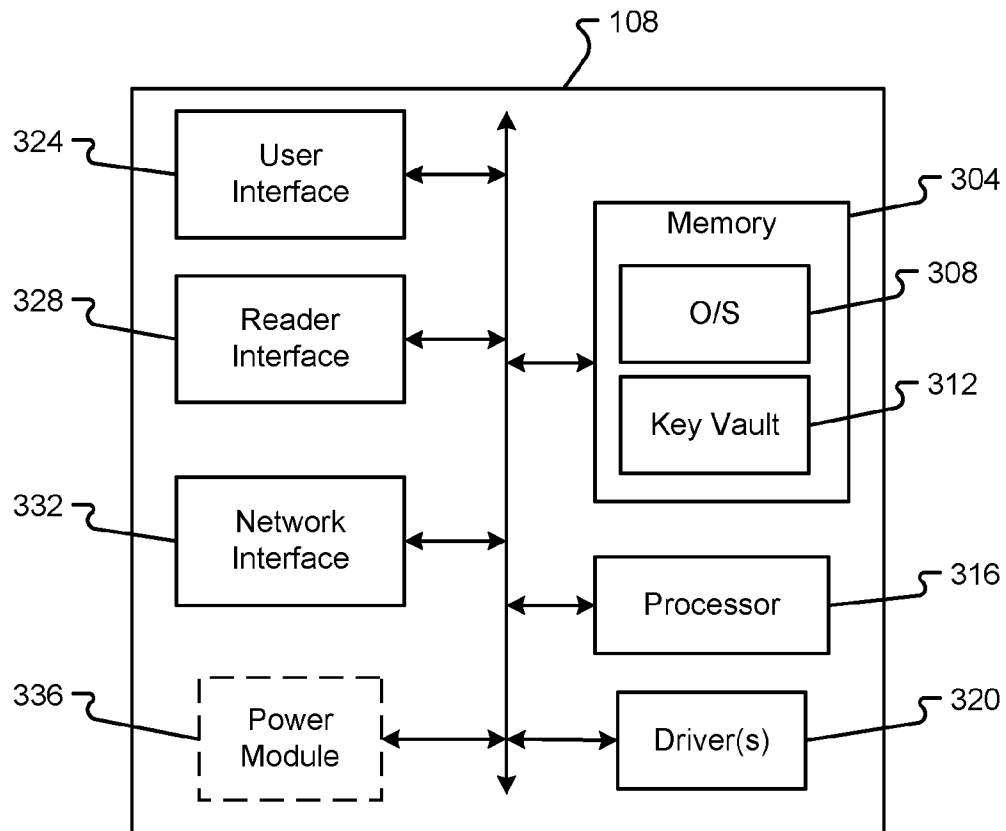


Fig. 1

**Fig. 2**

**Fig. 3**

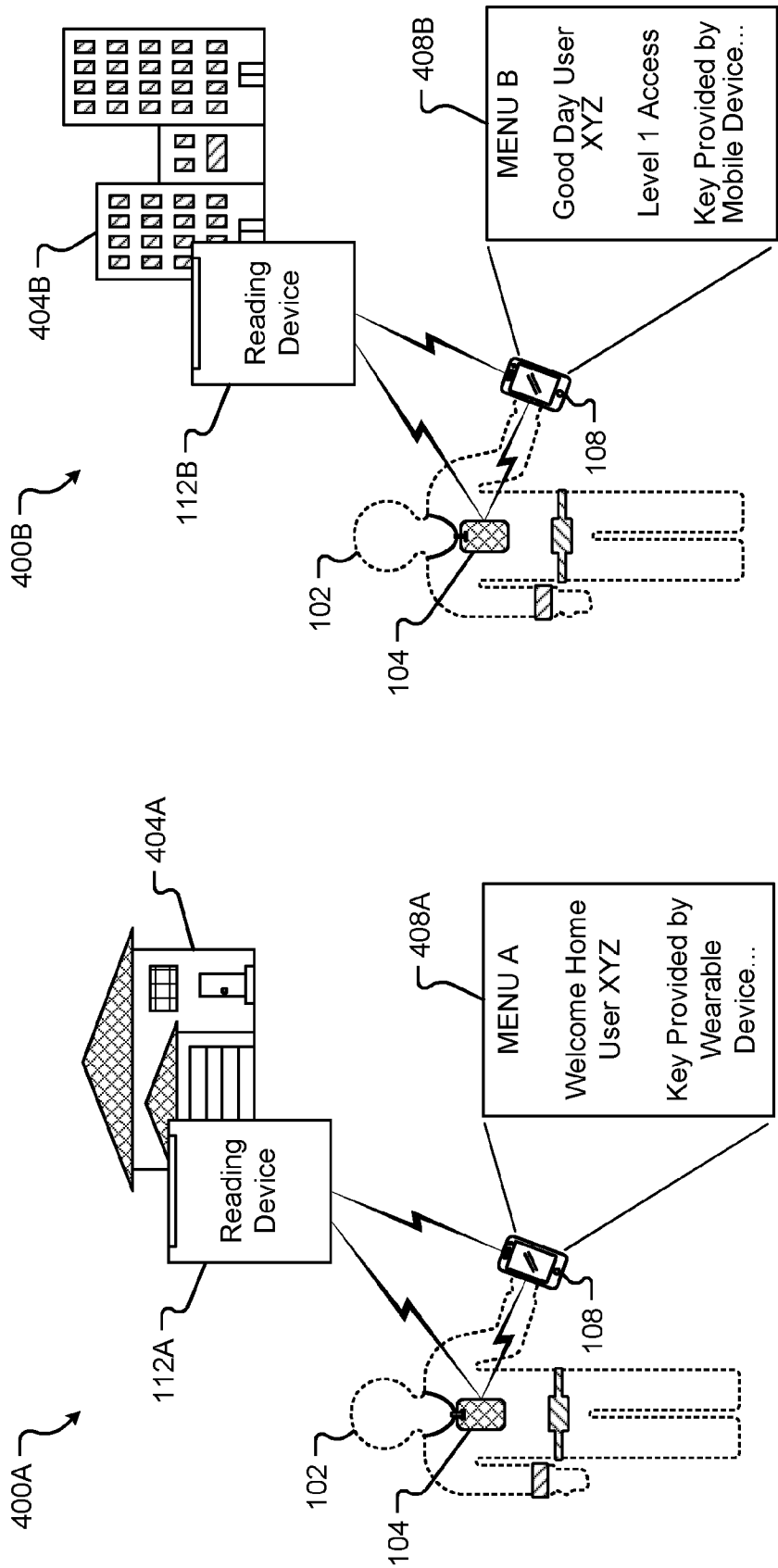
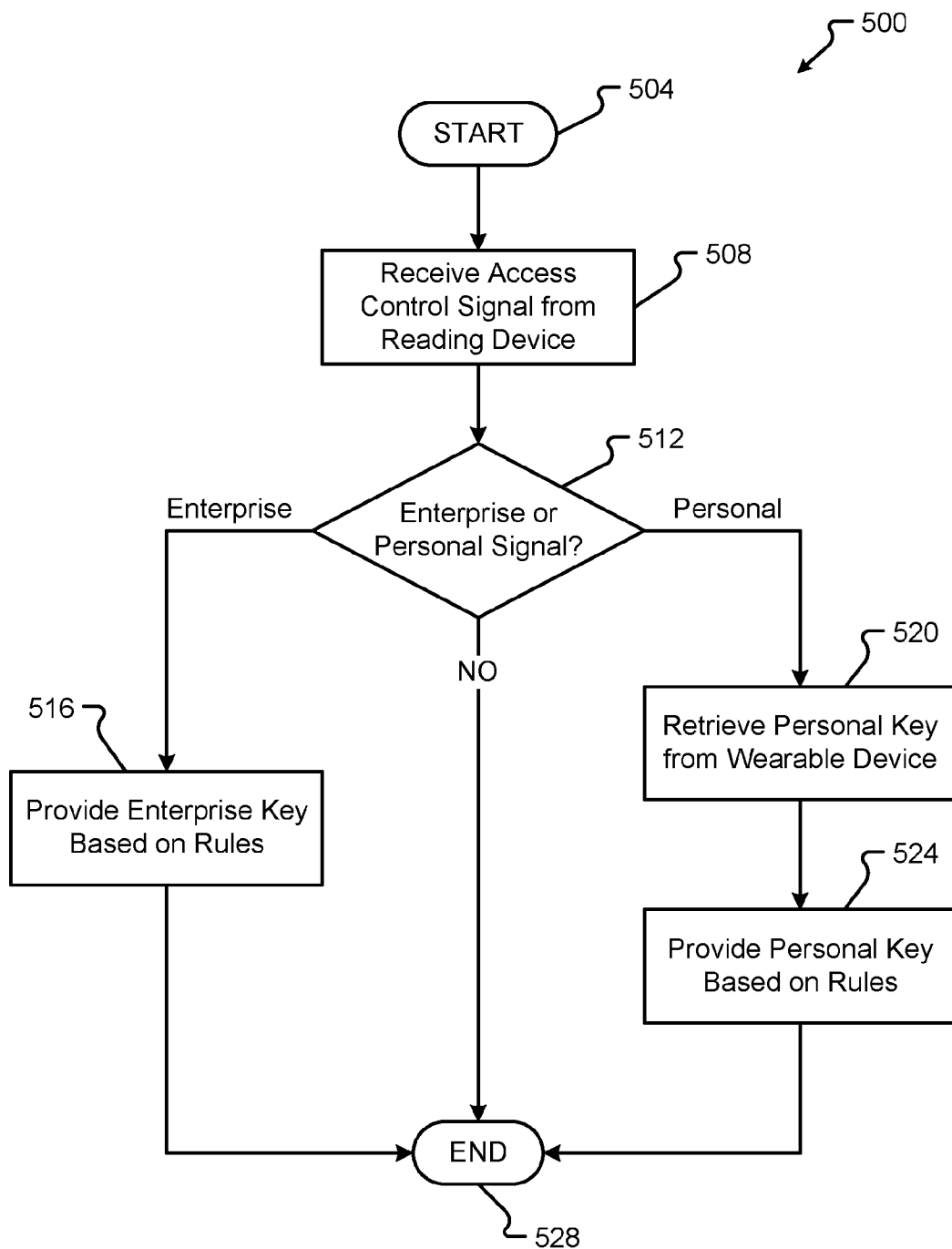


Fig. 4B

Fig. 4A

**Fig. 5**

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/059753

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/06 H04M1/725 H04W4/04 H04W12/08
ADD. G06F21/34 H04L29/06 H04W4/00 H04W12/04

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)

H04L H04W G06F H04M

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

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

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 926 038 A1 (MATSUSHITA ELECTRIC IND CO LTD [JP]) 28 May 2008 (2008-05-28) abstract; figures 5, 6, 7a-7d, 13, 19, 45 paragraphs [0042] - [0044], [0062] - [0073], [0124] - [0130] -----	1-20
A	EP 2 809 046 A1 (BLACKBERRY LTD [CA]) 3 December 2014 (2014-12-03) abstract; figures 1, 2, 3 paragraphs [0001], [0004] - [0007], [0010] - [0015], [0020], [0021], [0023], [0027] paragraphs [0028], [0031] - [0033], [0038], [0040], [0047], [0048], [0055] paragraphs [0056], [0063] - [0065] ----- -/-	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

27 May 2016

Date of mailing of the international search report

03/06/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Hristova, Ana

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/059753

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 2 469 816 A1 (LG ELECTRONICS INC [KR]) 27 June 2012 (2012-06-27) abstract; figure 4B paragraphs [0007] - [0020], [0181] -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/059753

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1926038	A1	28-05-2008	CN 101243455 A 13-08-2008
			EP 1926038 A1 28-05-2008
			US 2009043681 A1 12-02-2009
			WO 2007020782 A1 22-02-2007
EP 2809046	A1	03-12-2014	EP 2809046 A1 03-12-2014
			US 2014359750 A1 04-12-2014
EP 2469816	A1	27-06-2012	AU 2011202832 A1 05-07-2012
			CN 102572093 A 11-07-2012
			EP 2469816 A1 27-06-2012
			US 2012157165 A1 21-06-2012