



(51) International Patent Classification:

H04W 12/08 (2009.01) *H04L* 29/06 (2006.01)
H04W 12/06 (2009.01) *H04W* 4/00 (2009.01)
G06F 1/16 (2006.01) *H04L* 29/08 (2006.01)
G06F 21/34 (2013.01)

(21) International Application Number:

PCT/IB2016/000654

(22) International Filing Date:

2 May 2016 (02.05.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/156,030	1 May 2015 (01.05.2015)	US
62/156,035	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
62/197,945	28 July 2015 (28.07.2015)	US
62/197,985	28 July 2015 (28.07.2015)	US
62/198,240	29 July 2015 (29.07.2015)	US

(71) Applicant: ASSA ABLOY AB [SE/SE]; Klarabergsviadukten 90, SE-111 63 Stockholm (SE).

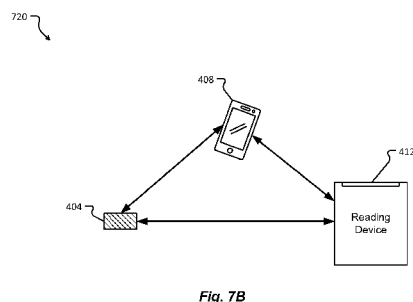
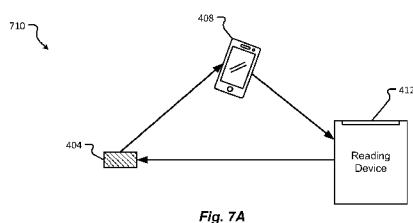
(72) Inventors: CATERINO, Mark, Anthony; 10 Meadow Lane, Prospect, CT 06712 (US). EINBERG, Fredrik, Carl Stefan; Klyftbagen 8, 14141 Huddinge (SE). HOYER, Philip; 43 Manor Road, Richmond TW9 1YA (GB). BERG, Daniel; Arrendevagen 48, SE-174 62 Sundbyberg (SE).

(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, 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,

[Continued on next page]

(54) Title: AUTHENTICATION CHANNEL FLOW THROUGH WEARABLE



(57) Abstract: An access control system comprising a reader configured to authenticate a primary mobile device only if the primary mobile device communicates with the reader via a required communication path that includes a secondary mobile device is described. Alternatively, the reader may be configured to evaluate credentials presented to the reader from a primary mobile device only if the primary mobile device communicates the credentials to the reader via a required communication path that includes a secondary mobile device.



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))*

AUTHENTICATION CHANNEL FLOW THROUGH WEARABLE

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 to 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.

[0006] As access control technology continually progresses, devices and communication protocols evolve to offer more security, portability, and interoperability. However, the benefits of this evolution may be thwarted by increasing instances of identity theft, stolen credentials, and/or other access control device theft.

SUMMARY

[0007] It is with respect to the above issues and other problems that the embodiments presented herein were contemplated.

[0008] Access control systems are well-suited for gathering useful information. For example, an access control system may be configured to count the number of times it grants access to the protected resource in a given period of time (hour, day, week, etc.), which information can then be used to identify needed access point maintenance intervals, or to schedule or allocate access-point resources (e.g. security guards, receptionists, and so forth). While some access control systems may be capable only of tracking generic information, others may be capable of tracking user-specific information, such as the time(s) at which each user presents credentials to the access control system reader. Such information can be used, for example, to verify an individual's claimed hours worked.

[0009] Wearable mobile devices may be used in place of or in conjunction with more traditional mobile devices to gather and send information to an access control system, thus

increasing the ability of the access control system to gather useful information and providing opportunities for enhancing security provided by access control systems.

[0010] Effective access control systems include safeguards to prevent or repel malicious attempts by unauthorized users to defeat the access control system and gain access to the protected resource. The communication of an authorized identification code is one such safeguard, as is use of an authentication process whereby a reader verifies that an RFID tag or mobile device is trusted. Ideal safeguards increase security without negatively affecting user convenience. For example, safeguards that do not require user intervention are preferable to safeguards that do require user intervention.

[0011] The proliferation of wearable mobile devices presents an opportunity to enhance access control system security without inconveniencing authorized users. An access control system is proposed herein that grants access only when authentication and/or authorization occur over a specific communication path that includes a reader, a primary mobile device (e.g. a smartphone or a tablet) and an auxiliary or secondary mobile device (such as, without limitation, a watch, a wristband, glasses, jewelry, clothes with an integrated IC, shoes, hair accessories, or another wearable device).

[0012] As used herein, an access control system is a system comprising a reader configured to control access to a protected resource at a given access point, such as a door or gate, and further comprising one or more credentials (e.g., an RFID tag, a mobile device, etc.) configured to communicate with the reader. A mobile device may be a smartphone, a tablet, or any other device comprising a processor, a data storage capability (e.g., computer memory), and a wireless communication capability. The terms identification code, electronic key, and mobile key are used interchangeably herein. A user is an individual in possession of a mobile device that has an authorized identification code and that is configured to wirelessly communicate with the reader of an access control system. A reader or reading device or interrogator is a device having a location (which may or may not be fixed) near an access point to a protected resource, and that is configured to grant access to the protected resource, for example, upon receipt of authorized credentials from a mobile device. A reader may comprise a contact-based or contactless communication interface (also referred to herein as a wireless communication interface, which may include one or both of a wireless communication receiver and a wireless communication transmitter, or a wireless communication transceiver), a memory for storing at least instructions, and a processor for carrying out instructions stored in memory. Alternatively or additionally, the instructions may be stored as firmware.

[0013] A wearable mobile device, also referred to simply as 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. A wearable mobile device is a type of mobile device, as the term mobile device is used herein. 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.

[0014] By way of example, visitors to a secure facility, or location, may be issued a wearable device for authentication while visiting. For example, the wearable device may be attached to a user's clothing, body, or other item that is in proximity to the user. This attachment may include clasping, pinning, connecting, or otherwise fastening the wearable device to be worn by the user.

[0015] Any number of communications protocols or channels may be employed by the wearable device and/or the mobile device. Examples of communications protocols or channels can include, but are in no way limited to, the protocol or protocols or channel or channels 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.

[0016] For instance, a user carrying a mobile device and wearing a wearable device while walking may impart a similar repetitive motion, force, or movement upon both the wearable device and the mobile device. Continuing this example, a user walking may provide a substantially similar force while stepping that is imparted to the wearable device and the mobile device. This force may occur with every step taken by the user (e.g., where a peak force occurs with every step that is taken at some point in time measured over a period of time, etc.). In other words, both the mobile device and the wearable device may experience a similar periodicity of maximum and minimum forces exerted on their

respective sensors (e.g., gyroscopic sensors, accelerometers, etc.). Additionally or alternatively, when a wearable device is separated from the mobile device, or vice versa, the motion results from the comparison may be determined to be different. For example, a user may leave a mobile device on a desk while walking with the wearable device in an access controlled environment.

[0017] Similarly, other information from one or more components of the wearable device and mobile device may be gathered and used by an access control system. This information may include, but is in no way limited to, temperature data, barometric pressure data, biometric data (e.g., heart rate, breathing rate, etc.), altimeter and/or altitude data, audible data (e.g., detecting similar sounds in an area around each device and comparing the detected sounds and/or sound profiles to one another determine whether continuous authentication is allowed, where matching audible data allows authentication and where nonmatching audible data disables authentication, etc.), light data (e.g., detecting similar light radiation in an area around each device and comparing the light detected at each device to determine whether continuous authentication is allowed, etc.), magnetic radiation data, other energy data, combinations thereof, and/or the like.

[0018] 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 and the two devices may utilize the same or different operating systems.

[0019] 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 by a mobile device and/or a reading device. One example of such electronics may be a wearable device having 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.

[0020] The terms “memory,” “computer memory,” and “computer-readable medium,” as used herein, refer 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.

[0021] As used herein, “credentials” or “credential information” refer to any data, set of data, encryption scheme, key, and/or transmission protocol used by a particular device (e.g., a “credential device,” a “mobile device,” or a “wearable device”) to authenticate and/or to verify its authenticity with a reader, mobile device, and/or interrogator.

[0022] 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_o).

[0023] 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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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

[0029] 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.

[0030] Fig. 1 is a diagram depicting an access control system in accordance with embodiments of the present disclosure;

[0031] Fig. 2 is a block diagram depicting a wearable device or components thereof in accordance with embodiments of the present disclosure;

[0032] Fig. 3 is a block diagram depicting a mobile device or components thereof in accordance with embodiments of the present disclosure;

[0033] Fig. 4 is a diagram depicting an access control system in accordance with other embodiments of the present disclosure;

[0034] Fig. 5A depicts a communication path according to an embodiment of the present disclosure;

[0035] Fig. 5B depicts another communication path according to another embodiment of the present disclosure;

[0036] Fig. 6A depicts yet another communication path according to yet another embodiment of the present disclosure;

[0037] Fig. 6B depicts still another communication path according to still another embodiment of the present disclosure;

[0038] Fig. 7A depicts an additional communication path according to an additional embodiment of the present disclosure;

[0039] Fig. 7B depicts another additional communication path according to another additional embodiment of the present disclosure;

[0040] Fig. 7C is a flowchart of a method in accordance with some embodiments of the present disclosure;

[0041] Fig. 8 is a diagram depicting an access control system in accordance with yet other embodiments of the present disclosure; and

[0042] Fig. 9 is a flowchart of another method in accordance with still other embodiments of the present disclosure.

DETAILED DESCRIPTION

[0043] 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.

[0044] An access control system in accordance with embodiments of the present disclosure includes a primary mobile device, a secondary mobile device, and a reader. The primary mobile device comprises a first processor, a first memory, and a first communication transceiver in communication with the processor and the memory. The first memory comprises a key vault in which a credential is stored. The first communication interface enables the primary mobile device to send and receive wireless communications. The secondary mobile device comprises a second processor, a second memory, and a second wireless communication transceiver in communication with the second processor and the second memory. The second wireless communication transceiver enables the secondary mobile device to exchange communications with the primary mobile device. The reader comprises a lock mechanism interface, a third processor, a third memory, and a third wireless communication transceiver in communication with the third processor and the third memory. The third memory comprises instructions for execution by the third processor that, when executed by the third processor, cause the third processor to: perform an initial authentication with the primary mobile device, thereby establishing a level of trust between the reader and the primary mobile device; following the initial authentication, require the primary mobile device to communicate with the secondary mobile device and obtain at least one piece of information from the secondary mobile device; receive the at least one piece of information at the reader; analyze the at least one piece of information at the reader; and based on the analysis of the at least one piece of information, make an access control decision at the reader with respect to a holder of the primary mobile device and a wearer of the secondary mobile device.

[0045] In the foregoing access control system, the primary mobile device may comprise at least one of a smartphone, a cellular phone, and a tablet. The secondary mobile device may comprise a wearable device. The wearable device may be at least one of a watch, a wristband, glasses, jewelry, clothes with an Integrated Circuit, shoes, and hair accessories.

[0046] Also in the foregoing access control system, the at least one piece of information may be communicated by both the second wireless communication transceiver and the first wireless communication transceiver. The at least one piece of information may also be communicated directly from the second wireless communication transceiver to the third wireless communication transceiver. The reader may communicate with one of the

primary mobile device and the secondary mobile device via the third wireless communication transceiver using a first communication protocol, and the primary mobile device may communicate with the secondary mobile device via the first wireless communication transceiver using a second communication protocol. Further, the first communication protocol or channel may be one of RFID and NFC, and the second communication protocol or channel may be one of Bluetooth, Bluetooth low energy (BLE), and WiFi. Alternatively, each of the first and second communication protocols or channels may be one of RFID, NFC, Bluetooth, BLE, and WiFi. Additionally, the third memory may comprise further instructions for execution by the third processor that, when executed by the third processor, cause the third processor to accept receipt of a credential from the primary mobile device only in response to determining that the at least one piece of information is a valid piece of information.

[0047] According to another embodiment of the present disclosure, a method of making an access control decision in a physical access control system includes performing an initial authentication between an access control reader and primary mobile device to establish a level of trust between the reader and primary mobile device; following the initial authentication, receiving, at a processor of the access control reader, a credential from the primary mobile device; determining, with the processor, whether the credential is valid; receiving, at the processor, a first password from the primary mobile device; receiving, at the processor, a second password from a secondary mobile device; comparing, with the processor, the first password with the second password; and based on the determination and the comparison, selectively operating a lock mechanism in communication with the reader to grant access to a protected resource.

[0048] In the foregoing method, the first password may be received via a first communication interface using a first communication protocol, and the second password may be received via a second communication interface using a second communication protocol different than the first communication protocol. Alternatively, the first communication protocol and the second communication protocol may be the same. One of the first communication protocol and the second communication protocol may be an NFC protocol or a Bluetooth protocol, and one of the primary mobile device and the secondary mobile device may be a wearable mobile device. Also, the password may be a one-time password. The credential may be received from the primary mobile device via an encrypted communication channel.

[0049] A mobile device according to another embodiment of the present disclosure includes a processor; a wireless radio and a different contactless communication interface, both in communication with the processor; and a memory having a key vault in which a credential is stored. The memory further stores instructions for execution by the processor. The instructions, when executed by the processor, cause the processor to: transmit a signal to an access control reader via one of the wireless radio and the contactless communication interface; transmit subsequent signals to the access control reader and a secondary mobile device in accordance with a predetermined communication path; and transmit the credential to the access control reader.

[0050] The instructions in the memory of the foregoing mobile device may cause the processor to transmit the subsequent signals to the access control reader via a first communication protocol, and may further cause the processor to transmit the subsequent signals to the secondary mobile device via a second communication protocol different than the first communication protocol. The instructions may also cause the processor to transmit the signal to the access control reader in response to receiving a first signal from the access control reader. The predetermined communication path may be provided to the mobile device via one of the wireless radio and the contactless communication interface, or the predetermined communication path (or information corresponding to the predetermined communication path) may be stored in the memory of the mobile device. The contactless communication interface may comprise at least one of a Bluetooth, a BLE, and an NFC interface. Also, the subsequent signals transmitted to the access control reader and the secondary mobile device may comprise a password.

[0051] Before any embodiments of the disclosure are explained in further 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.

[0052] One advantage of mobile devices as credentials, as opposed to, for example, RFID tags, is that mobile devices are generally capable of beyond-near-field communications using communication protocols such as Bluetooth, BLE, WiFi, ZigBee,

infrared, sound, light, etc. In access control systems comprising a reader configured to communicate with a mobile device using one or more such communication protocols, the mobile device can communicate information to the reader even when it is not in close proximity to (e.g., more than 1.0m away from) the reader. Mobile devices are also often equipped to communicate with other mobile devices via communication paths that do not use traditional mobile telecommunication networks. Additionally, storing credentials on mobile devices, which users typically carry (or wear) for other purposes, allows users to carry fewer objects. And mobile devices are typically equipped with various sensors not included in traditional RFID tags. Still further, mobile devices typically have greater processing power than traditional RFID tags. As described herein, these and other advantages may be exploited to enhance the security provided by an access control system by requiring that an authentication and/or authorization process include communications with or via a wearable device.

[0053] Fig. 1 is a diagram depicting an access control system 100 for authenticating a user 102 via multiple mobile devices (one or more of which may be a wearable device) in accordance with embodiments of the present disclosure. The user 102 is depicted as having multiple wearable devices 104. 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/mobile device 108. In other embodiments, the access control system 100 may comprise two wearable devices 104, or two portable devices 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 118 across a communication network 128. The access data memory 118 may be located remotely, locally, and/or locally and remotely, from the reading device 112.

[0054] One or both of the wearable device 104 and 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/or the portable device 108 on the one hand and the

reading device 112 on the other may be established automatically when the wearable device 104 and/or portable device 108 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/or the portable device 108 and the intensity of RF signals emitted by the wearable device 104 and/or the portable device 108 exceeds a threshold of sensitivity of the reading device 112.

[0055] 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 other communication networks and/or protocols as provided herein.

[0056] In one embodiment, authentication may be required between the wearable device 104 and one or both of the reading device 112 and the mobile device 108 before further communications are enabled. In another embodiment, authentication may be required between the mobile device 108 and one or both of the reading device 112 and the wearable device 104 before further communications are enabled. In accordance with embodiments of the present disclosure, any one or more of various authentication channel flows involving both a mobile device 108 and a wearable device 104 (or, in embodiments, two mobile devices 108, or in other embodiments, two wearable devices 104) may be required to successfully complete authentication and enable further communications. In any event, the further communications may include communications in which access control information (e.g., keys, codes, credentials, etc.) is 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.

[0057] 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 access control information may be used to validate the wearable device 104 or the mobile device 108 to the reading device 112. 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 physical or logical 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 or some other system backend component may generate such signals.

[0058] 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.

[0059] 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 118. Like the memory of the access server 120, the access data memory 118 may comprise a solid state memory or devices. The access data memory 118 may comprise a hard disk drive or other random access memory.

[0060] 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.

[0061] 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.

[0062] 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.

[0063] 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 and/or access control information. For instance, the credential information/access control 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.

[0064] 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 a mobile device 108. As can be appreciated, the antenna(s) 212A-N may be arranged to operate using one or more wireless communication protocols or channels 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.

[0065] 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.

[0066] 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.

[0067] 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 device 104 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 device 104 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.

[0068] 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.).

[0069] 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 mobile device 108 may be associated with the wearable device 104, and/or the wearable device may be associated with 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. Additionally, motion comparison results (or simply detected motion information) may be used by the wearable device 104, the mobile device 108, and/or the reader 112 to assist in making an ingress or egress determination for the mobile device 108 and/or the wearable device 104. 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.

[0070] 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. Although

location information may not always be available inside buildings or other structures, location information provided by the one or more location sensors 228 may be used, where available, to make an ingress or egress determination for the wearable device 104 and/or the mobile device 108.

[0071] 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. Although not depicted in Fig. 2, a wearable device 104 may also include a key vault for storing one or more keys, which may be utilized in the same manner as described herein with respect to mobile device 108. The key(s) in the key vault 312 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.

[0072] If NFC is being used for the communication channel (as one non-limiting example), 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.

[0073] If BLE or some other non-inductive protocol (e.g., Wi-Fi) is being used for the communication channel (or for a portion thereof, e.g. for communications between the mobile device 108 and a wearable device 104 or another wearable device 108), then the devices utilizing that communication channel (e.g. the reader 112 and mobile device 108, or the mobile device 108 and a wearable device 104) 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 connected devices may then exchange needed authentication or authorization information (which may include the key(s)), to enable an authentication or an access control decision to be made. If a positive authentication decision is made, then further communications (e.g. if communication of the key(s) or other access control information) may be permitted, and 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.

[0074] 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 device 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.

[0075] 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.

[0076] 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.

[0077] 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 implements 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.

[0078] 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, device 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 device interface 328 may be adapted to ensure that the device interface 328 follows the appropriate proximity-based protocols (e.g., BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, etc.) such that the device 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.).

[0079] 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.

[0080] The device interface 328 may correspond to the hardware that facilitates communications between the mobile device 108 and other devices, such as the wearable devices 104 and the reader device 112. The device interface 328 may include, by way of example and without limitation, 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 device interface 328 is specifically provided to facilitate proximity-based communications with other devices via communication channel or multiple communication channels for authentication or authorization purposes.

[0081] 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.

[0082] 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.

[0083] Turning now to Fig. 4, an access control system may be configured such that a reader 412 will accept credentials (e.g. a mobile key, an identification code, or other credentials) from a mobile device (which may be a wearable device) only after conducting an authentication process to determine that the mobile device is trusted. According to embodiments of the present disclosure, the authentication process may involve communication among the reader 112, a primary mobile device 408 (e.g. a smart phone),

and a secondary mobile device 404 (e.g. a wearable device in the form of a watch) along a specific path, referred to herein as the required or desired communication path. The primary mobile device 408 may have the same components as those described above with respect to the mobile device 108, and the secondary mobile device 404 may have the same components as those described above with respect to the wearable device 104. Once the authentication process is successfully completed, then the authorization process can begin, in which the primary mobile device 408 transmits credentials to the reader 412. If the reader 412 recognizes the credentials, then it grants access to the protected resource.

[0084] With reference to Figs. 5A and 5B, access control systems may utilize any one of many possible required or desired communication paths. In some embodiments, the required communication path is linear, such that communications between two components are always required to pass through a third component. For example, a linear required communication path 510 begins or ends at the primary mobile device 408 and the reader 412, with all communications between the primary mobile device 408 and the reader 412 passing through the secondary mobile device 404.

[0085] The required communication path 510 may correspond to physical or functional limitations of the components of the access control system. For example, the reader 412 may be configured to communicate via a near field communication protocol (NFC), and the primary mobile device 408 may be configured to communicate via Bluetooth. The secondary mobile device 404 may be capable of both NFC and Bluetooth communications. Thus, a user 402 seeking access to a protected resource may position his or her wrist (and thus the smart watch secondary mobile device 404) near the reader 412, thus allowing the reader 412 to communicate with the secondary mobile device 404 using NFC. The secondary mobile device 404 can then communicate with the smartphone primary mobile device 408 (which can be left in the user's pocket, purse, etc.) using the Bluetooth protocol. In other embodiments, described more fully below, the required communication path 510 may not correspond to physical or functional limitations of the components of the access control system, and the communicating devices (e.g. the reader 412, the primary mobile device 408, and the secondary mobile device 404) may all communicate using NFC, or Bluetooth, or BLE, or any other suitable communication protocol or channel.

[0086] In embodiments, a required communication path may vary as the authentication sequence progresses. For example, the authentication process 520 may require that a message be sent from the primary mobile device 408 to the secondary mobile device 404

(520a) to the reader 412 (520b), then from the reader 412 to the secondary mobile device 404 (520c) and back to the reader 412 (520d), then from the reader 412 to the secondary mobile device 404 (520e) to the primary mobile device 408 (520f), then from the primary mobile device 408 to the secondary mobile device 404 (520g) to the reader 412 (520h). As persons of ordinary skill in the art will recognize in light of the foregoing disclosure, many such variations are possible without departing from the scope of the present disclosure.

[0087] With reference to Fig. 6A, in another embodiment according to the present disclosure, a required communication path 610 may begin or end at the secondary mobile device 404 and the reader 412, with communications between those devices passing through the primary mobile device 408. This may be a desirable communication path when the primary mobile device 408 is equipped to communicate with the secondary mobile device 404 and the reader 412, but the reader 412 cannot communicate directly with the secondary mobile device 404.

[0088] While communications in the embodiment of Fig. 6A are between the secondary mobile device 404 and the primary mobile device 408, and between the primary mobile device 408 and the reading device 412, the communication path 610 may in some embodiments require that a message originated by the secondary mobile device 404 be communicated first to the primary mobile device 408 and then from the primary mobile device 408 to the reading device 412, while in other embodiments the communication path 610 may require that no messages (or may not require that any messages) originated by the secondary communication device 404 be communicated to the reading device 412 through the primary mobile device 408. In other embodiments, such as the communication path 620 depicted in Fig. 6B, the intermediary device (here, the primary mobile device 408) may generate or originate all of the messages that it sends to the secondary mobile device 404 (e.g. messages 620c, 620g) and/or to the reading device 412 (e.g. messages 620a, 620e, 620h). The primary mobile device 408 may, however, utilize information received from one or both of the secondary mobile device 404 or the reading device 412 (e.g. in messages 620b, 620d, 620f) to generate or originate its own messages.

[0089] In some embodiments, the required communication path is circular rather than linear, meaning that each device communicates with the other two devices in a prescribed sequence. For example, in Fig. 7A, the communication path 710 flows from the primary mobile device 408 to the reader 412, from the reader 412 to the secondary mobile device 404, and from the secondary mobile device 404 to the primary mobile device 408. A

communication path such as the communication path 710 allows the reader 412, for example, to send information to the secondary mobile device 404, perhaps utilizing a first communication protocol, and to determine whether the secondary mobile device 404 is in communication with the primary mobile device 408 by determining whether the primary mobile device 408 returns the same information (or information sufficient to verify that the primary mobile device received the sent information) to the reading device 412. Thus, for example, the reader 412 may generate a nonce (e.g. a message or signal for one-time use) and transmit the nonce to the secondary mobile device 404. The secondary mobile device 404 may transmit the nonce as is to the primary mobile device 408, or the secondary mobile device 404 may electronically sign the nonce, then transmit the nonce and signature to the primary mobile device 408. The primary mobile device 408 may then add its own electronic signature to the nonce (or to the nonce and the signature of the secondary mobile device 404, as the case may be), and transmits the nonce, the signature of the primary mobile device 408, and, if applicable, the signature of the secondary mobile device 404 to the reader 412. The reader 412 may then validate the received nonce and signature(s) and make an appropriate access control decision.

[0090] Although the circular communication path 710 has one particular component order (e.g. from reading device 412 to secondary mobile device 404 to primary mobile device 408), other component orderings also fall within the scope of the present disclosure. For example, the primary mobile device 408 may send messages to the secondary mobile device 404, the secondary mobile device 404 may send messages to the reader 412, and the reader 412 may send messages to the primary mobile device 408.

[0091] As with other embodiments, an access control system utilizing a circular required communication path may or may not require that messages travel sequentially along the entire path, and may require two-way communication between two or more components of the access control system, as shown in Fig. 7B. For example, a required communication path 720 may flow from the reader 412 to the secondary mobile device 404 to the primary mobile device 408, back to the secondary mobile device 404, then to the primary mobile device 408 and on to the reader 412, then back to the primary mobile device 408. Here again, many variations are possible without departing from the scope of the present disclosure.

[0092] Enforcement of an authentication communication path requirement may occur naturally due to authorization requirements. For example, a required authentication communication path may be based upon which device (between the primary mobile device

408 and the secondary mobile device 404) holds the credentials that must be presented to the reading device 412 to gain access to the protected resource. Thus, for example, the device holding the credentials (for example, the primary mobile device 408) may only be enabled (whether structurally or logically) to communicate with another device (e.g. the secondary mobile device 404), which may in turn be enabled (whether structurally or logically) to communicate both with the first device (e.g. the primary mobile device 408) and with the reading device 412. Also, in some embodiments, both the primary mobile device 408 and the secondary mobile device 404 may have a portion of the needed credentials, such that each device must provide its respective credentials to the reading device 412 to gain access to the protected resource. In still other embodiments, one device (e.g. the primary mobile device 408) may have stored in memory certain data that must be modified by one or more algorithms stored in the memory of a second device (e.g. the secondary mobile device 404) before being presented to the reading device 412 in order to obtain an access granted decision from the reading device 412.

[0093] In some embodiments, a reader 412 may generate a nonce and transmit the generated nonce separately, over two different communication protocols or channels, to each of the primary mobile device 408 and the secondary mobile device 404. For example, the reader 412 may transmit the nonce to the primary mobile device 408 using BLE, and to the secondary mobile device 404 using NFC. The primary mobile device 408 and the secondary mobile device 404 may then each sign the nonce and return the signed nonce to the reader 412. In some embodiments, the primary mobile device 408 and the secondary mobile device 404 may each return the signed nonce directly to the reader 412, while in other embodiments one or both of the primary mobile device 408 and the secondary mobile device 404 may transmit its respective signed nonce to the other of the primary mobile device 408 and the secondary mobile device 404, which may then transmit the received signed nonce to the reader 412. Once it has received the signed nonces from both of the primary mobile device 408 and the secondary mobile device 404, the reader 412 may validate the signed nonces and make an appropriate access control decision.

[0094] Required communication paths as described above may be implemented as described below.

[0095] With reference to Fig. 7C (and referring also to elements depicted in Fig. 4), a method 750 of utilizing a required communication path for authentication or authorization purposes according to some embodiments of the present disclosure begins at step 754. A

one-time step of registering a user 402's primary mobile device 408 and secondary mobile device 404 (step 758) allows the reader 412 (or an access control server 420, or any other suitable component of an access control system) to store identification information corresponding to the primary mobile device 408 and the secondary mobile device 412 in a memory 416 of the reader or in a memory 432 of the access control system.

[0096] When a device is presented to the reader 412 for authentication, the reader 412 can obtain identification information from the device and, using the registration information stored in the memory 416 or 432, evaluate whether the device has been registered (step 760). If the device has not been registered, then the reader 412 can utilize an authentication process that does not use a required communication path (but that, in embodiments, imposes other, alternative authentication requirements). If the device has been registered, then the reader 412 can apply the required communication path authentication requirement when authenticating the device, and, based on the registration information, can ensure that the proper primary mobile device and secondary mobile device (e.g. primary mobile device 408 and secondary mobile device 404) are used to comply with the required communication path requirement.

[0097] Having determined that a device presented for authentication (e.g. the primary mobile device 408 or the secondary mobile device 404) has been registered, the reader 412 can determine a required communication path to use for authenticating the device in question (step 762). The reader need not utilize the same required communication path every time the same device is presented for authentication, but may instead vary both the order of communication among the devices (e.g. among the primary mobile device 408, the secondary mobile device 404, and the reader 412) as well as the number of communications that must be sent between any two of the three devices. For example, the reader 412 may utilize a required communication path such as that described in Figs. 5A and 5B on one occasion, a required communication path such as that described in Figs. 6A and 6B on another occasion, and a required communication path such as that described in Fig. 7A or 7B on yet another occasion. The path selected by the reader 412 may depend on whether the primary mobile device 408 or the secondary mobile device 404 has been presented to the reader 412. Additionally, the reader 412 may select a predetermined required communication path, or the reader 412 may generate a required communication path, utilizing a random or pseudo-random number generator to achieve random or pseudo-random variation among required communication paths generated on successive occasions.

[0098] Having determined a required communication path to use in authenticating the primary mobile device 408 and/or the secondary mobile device 404, the reader 412 commences the authentication process (step 766). Unless the selected required communication path is already known to the primary mobile device 408 or to the secondary mobile device 404 (in embodiments, the required communication path may, for example, always be the same, or may, as another example, vary according to a predetermined pattern, such that the primary mobile device 408 and/or the secondary mobile device 404 may already know or be able to determine which required communication path will be used for a given authentication attempt), the reader 412 communicates the required communication path (or information corresponding thereto) to one or both of the primary mobile device 408 and the secondary mobile device 404. Whether the reader 412 sends the required communication path to the primary mobile device 408, the secondary mobile device 404, or both may depend at least in part on whether the reader 412 can establish a communication channel with the primary mobile device 408 and with the secondary mobile device 404, and may also depend at least in part on the required communication path that will be used. For example, if the required communication path requires that communications proceed from the reader 412 to the primary mobile device 408 to the secondary mobile device 404 (as depicted in Fig. 7A), then the reader 412 may send the required communication path to the primary mobile device 408, which send the required communication path to the secondary mobile device 404. Any other communications that must be sent or received as part of the authentication process are made according to the required communication path.

[0099] Once authentication communications are complete, the reader 412 determines whether the authentication communications followed the required communication path (step 770). This may be as simple as determining whether a required communication was received from the proper device (e.g., if the required communication path is as shown in Fig. 7A, then the reader 412 may simply determine whether it received a communication from the secondary mobile device 404), or it may involve determining whether information provided to one device was received from another device (thus indicating that the one device communicated the information to the other device). In embodiments, each device (the primary mobile device 408, the secondary mobile device 404, and the reader 412) appends a digital signature to a message every time it receives the message, such that after a message has been passed among the devices in question, the reader 412 can analyze the message to determine whether it has signatures from each device, in an order

corresponding to the order of the required communication path. These are just some examples of ways that the reader 412 can determine whether the authentication process for the primary mobile device 408 and the secondary mobile device 404 complied with the required communication path.

[00100] If the reader 412 determines that the primary mobile device 408 and the secondary mobile device 404 complied with the required communication path, then the reader 412 may request and receive credentials from one or both of the primary mobile device 408 and the secondary mobile device 404, evaluate those credentials, and make an access determination based on the evaluation (step 774). If the reader 412 determines that the required communications path was not complied with, then the reader may deny access without evaluating any credentials, or may impose additional or alternative authentication and/or authorization requirements beyond the required communication path requirement and beyond the presentation of credentials. Once an access determination has been made, the method 750 ends (step 778).

[00101] In some embodiments, a required communication path is enforced by virtue of the physical or functional limitations of the primary and secondary mobile devices. In other words, in some embodiments the required communication path is the only communication path that allows communications between one of the primary and secondary mobile devices 408 and 404 and the reader 412. For example, if the authentication process of an access control system utilizes digital signatures requiring a minimum threshold of processing power to verify, then a secondary mobile device 404 with less than the minimum threshold of processing power will be unable to complete the verification. However, the secondary mobile device 404 may be the only mobile device capable of communicating with the reader 412. Additionally or alternatively, the secondary mobile device 404 may be the most convenient device to use for communications with the reader 412. For example, if the reader 412 can only communicate via NFC, such that a mobile device must be placed in close proximity to the reader 412 for communications to occur, then a secondary mobile device 404 such as a smart watch or other wearable device may be more conveniently placed within communication range of the reader 412 than a primary mobile device 408 such as a phone or tablet (which a user 402 may typically store, for example, in a pocket or purse). In either case, the reader 412 may send information to the secondary mobile device 404 that the secondary mobile device 404 is unable to process. The secondary mobile device 404 may then send the information to the primary mobile device 408 (perhaps using a different

communications protocol), which processes the information and sends a response to the secondary mobile device 404 (or, in embodiments, to the reader 412). The secondary mobile device 404 may then forward the response to the reader 412 (with or without further processing) to complete the authentication process.

[00102] In other embodiments, the required communication path may not be influenced by the capabilities of the primary and secondary mobile devices 408 and 404, such that the primary and secondary mobile devices 408 and 404 are essentially interchangeable (at least until the authentication process begins). In these embodiments, the primary mobile device 408, the secondary mobile device 404, and the reader 412 may all communicate with each other using NFC, Bluetooth, BLE, WiFi, or any other suitable communication protocol or channel. In such embodiments, one or more of the components of the access control system may be configured to modify messages in a way that allows one or both of the other components to verify that the message followed the required communication path. For example, if a required communication path flows from the primary mobile device 408 to the reader 412 through the secondary mobile device 404, the secondary mobile device 404 may be configured to modify every message that it passes from the primary mobile device 408 to the reader 412 and from the reader 412 to the primary mobile device 408. When the primary mobile device 408 or the reader 412 receives each message, it can verify that the message came through the secondary mobile device 404 by checking for the modification.

[00103] In embodiments, the modification may be different depending on whether the secondary mobile device 404 received the message from the reader 412 or from the primary mobile device 408. The modification may be a necessary part of the authentication process, such as verifying a digital signature with a public key. Alternatively, the modification may comprise information that is added to the message. For example, the modifying component may add its own digital signature to the message. The modification may also comprise a function to which the message is input and from which the modified message is output. For example, the secondary mobile device 404 may convert a message from a first format (i.e. a format in which the message was generated by the primary mobile device 408) into a different second format. The format change may be necessary in order for the recipient device (e.g. reader 412) to understand the message, or it may be necessary simply as an indication to the recipient device that the message followed the required communication path.

[0100] Sometimes, the secondary mobile device 404 may not be configured to communicate with the reader 412 (and may not even be capable of communication with the reader 412), yet may still be part of a required communication path. In such situations, the primary mobile device 408 may send messages that it generates to the secondary mobile device 404 for modification, and the secondary mobile device 404 may then send the message to the primary mobile device 408 for retransmission (with or without further modification) to the reader 412. Similarly, after receiving a message from the reader 412, the primary mobile device 408 may send the message (with or without modification) to the secondary mobile device 404 for modification, and the secondary mobile device 404 may then send the modified message to the primary mobile device 408.

[0101] Regardless of the particular communication path required by a given access control system, one or more components of the system are configured to determine whether the required communication path has been followed. Such a determination may be implicit or explicit. For example, in embodiments where all messages between two components of the access control system must be sent through a third component of the access control system, and where the third component of the access control system reformats each message into a format that can be read by the intended recipient of the message, the fact that the intended recipient is able to understand the message constitutes an implicit determination that the required communication path has been followed. Likewise, when only the secondary mobile device 404 is capable of communications with a reader 412 but only the primary mobile device 408 has the processing capability needed to complete the authentication process, receipt by the reader 412 of a processed authentication message implicitly indicates that the message originated with the primary mobile device 408 and was communicated through the secondary mobile device 404.

[0102] Alternatively, in embodiments where one or more components along a required communication path add information to a message, the recipient device may search the message for the added information to verify that the message followed the required communication path. Such a determination is an example of an explicit determination that the required communication path has been followed.

[0103] Although the above description focuses on access control systems having a single reader 412, a primary mobile device 408, and a secondary mobile device 404, embodiments of the present disclosure may utilize additional components, which may include one or more additional readers and/or one or more additional mobile devices. In such embodiments, the required communication path may include communications to

and/or from the additional components. Similarly, although the above description depicts the primary mobile device 408 as a smart phone and the secondary mobile device 404 as a smart watch, the primary and secondary mobile devices may be any mobile devices. Thus, for example, the primary and secondary mobile devices may both be smart phones or tablets, or they may both be wearable mobile devices.

[0104] Also, the primary and secondary mobile devices need not belong to or be in possession of a single user. With reference now to Fig. 8, a primary mobile device 808 may belong to a user 802, and a secondary mobile device 804 may belong to a user 801. The reading device 812 may grant access to the resource it protects only upon authentication of the primary mobile device 808 and/or the secondary mobile device 804 by way of a predetermined communication path involving both the primary mobile device 808 and the secondary mobile device 804. Regardless of which communication path is required for authentication and/or authorization (whether one of the communication paths described above or another communication path), requiring a communication path that flows through devices belonging to separate users enhances security by limiting access to the protected resource to instances where two individuals are present (provided that one individual does not obtain possession, whether licitly or illicitly, of both the primary and the secondary mobile devices 808 and 804). Moreover, if two individuals must be present to gain access to a protected resource, then each individual can also use his or her own perception to determine whether the other individual is known, recognized, etc. Embodiments such as that depicted in Fig. 8 may be particularly useful to ensure that a guest to a protected facility stays with his or her host, or to ensure that two persons are present (and can thus monitor each other) in highly secure areas (e.g. bank vaults, military facilities, and the like). In some embodiments, identification information may be stored in a memory of the reader 812 that allows the reader 812 to confirm that the mobile devices 808 and 804 belong to different individuals.

[0105] While some access control systems may be configured to allow successful authentication only when a required communication path flowing through both a primary and a secondary mobile device is used, other access control systems may be configured with alternative requirements for authentication, such that authentication can be achieved either when the required communication path has been followed or when some other criterion is met. Such embodiments may be particularly useful in situations where not all persons authorized to enter a protected resource have both a primary and a secondary mobile device, or to allow persons who do not have both a primary and a secondary

mobile device in a specific instance to still obtain access. Some access control systems may be configured to use a required communication path that includes mobile devices belonging to different individuals as an alternative for some other authentication requirement (e.g. one that is less convenient) that must be satisfied when only one user seeks authentication.

[0106] When an access control system is used to protect multiple access points to a protected resource, each of which is associated with a reader, an administrator of the access control system can create a customized required communication path for one or more of the readers. The same required communication path may be used for a group of readers or for every reader, or each reader may have a different required communication path. Use of required communication paths for authentication provides an additional layer of security for the protected resource, because a given user must first successfully authenticate using the required communication path and then communicate the correct key to the reader in order to gain access to the protected resource.

[0107] Although the above examples describe the use of a required communication path during the authentication process, a required communication path may be utilized during authorization instead of or in addition to during authentication. When used for authorization, the required communication path can be implemented in essentially the same way as when used for authentication, and may be used for communication of an identification code or other electronic key from one of the mobile devices to the reader.

[0108] Turning now to Fig. 9 (and referring to elements depicted in Fig. 4), a method 900 for implementing a required communication path for authentication and/or authorization utilizing two mobile devices according to embodiments of the present disclosure begins at step 904. A user 402 having a primary mobile device 408 and a secondary mobile device 404 approaches a reader 412 from a distance. As the primary mobile device 408 of the user 402 comes within communication range of the reader 412, the primary mobile device 408 authenticates with the reader 412 (step 908) using a communication protocol (e.g., BLE) that allows for communications at distances greater than NFC range (e.g. greater than 1 meter). The determination that the primary mobile device 408 is within communication range of the reader 412 may be made implicitly, e.g. by the receipt at the primary mobile device 408 of a signal broadcast by the reader 412, or by the receipt at the reader 412 of a signal broadcast by the primary mobile device 408, or explicitly, e.g. through the use of one or more location sensors on the primary mobile device 408, or by analyzing RSSI or time-of-flight information, or using any other means.

In some embodiments, the authentication of the primary mobile device 408 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.

[0109] After the primary mobile device 408 has authenticated with the reader 412, the primary mobile device 408 sends credentials stored in a memory thereof (e.g. a memory 304, and perhaps even a key vault 312 of a memory 304) to the reader 412 (step 912). The primary mobile device 408 may establish a secure communication path with the reader 412, using known encryption or other security techniques, prior to sending the credentials. Additionally, the primary mobile device 408 may, in some embodiments, send the credentials in response to a message from the reader 412 indicating that the primary mobile device 408 has been successfully authenticated, or in response to a request from the reader 412 for the credentials. Alternatively, the primary mobile device 408 may send the credentials to the reader 412 without being prompted to do so by any message from the reader 412.

[0110] Upon receipt of the credentials from the primary mobile device 408, the reader 412 analyzes the credentials, using, in embodiments, information stored in a memory of the reader 412, or accessible to the reader 412 via a wired or wireless connection, to determine whether the credentials are valid (step 916). The reader 412 may utilize one or more algorithms, using information from or corresponding to the received credentials, in analyzing the credentials, and may evaluate whether the result of running the algorithms corresponds to a predetermined result. The reader 412 may simply compare the received credentials with credentials stored in a memory of the reader 412, or in a memory accessible to the reader 412. The reader 412 may also initiate communications with one or more other components of an access control system as part of performing the credential analysis. The reader 412 may or may not provide an indication to the primary mobile device 408 of whether the credentials provided by the primary mobile device 408 are valid.

[0111] Whether together with the credentials or separately, and whether during the authentication or authorization process or not, the primary mobile device 408 sends a password or other data to both the reader 412 and to the secondary mobile device 404 (step 920). (The primary mobile device 408 may use BLE to communicate with the secondary mobile device 408 as well as with the reader 412, or may use any other available communication protocol.) Alternatively, the reader 412 may communicate a

password or other data to the primary mobile device 408, which may then communicate the same password or other data to the secondary mobile device 404.

[0112] As the user 402 reaches the access point, the user 402 presents the secondary mobile device 404 to the reader 412 (step 924). If the secondary mobile device 404 is configured to communicate with the reader 412 using a short-range communication protocol (e.g. NFC, RFID, capacitive coupling (where information is transmitted from the wearable via the human body to a recipient device)), the user 402 may tap the secondary mobile device 404 on the reader 412, or bring the secondary mobile device 404 within close proximity (e.g. within 1 meter, or within 10 inches, or within 5 inches or within 3 inches, or within 1 inch) of the reader 412. Once a communication channel has been established between the secondary mobile device 404 and the access control reader 412, the secondary mobile device 404 communicates the password or other data to the reader 412. While short-range communication protocols are well-suited for communications between the secondary mobile device 404 and the reader 412, any communication protocol, including, for example, BLE, may be used.

[0113] Upon receipt of the password or other data from the secondary mobile device 404, the reader 412 evaluates the password or other data to determine whether it matches the password or other data received by the reader 412 directly from the primary mobile device 408. Alternatively, the reader 412 may evaluate the password or other data received from the secondary mobile device 404 to determine whether it satisfies some other predetermined requirement ((e.g. by comparing the received password or data to a stored password or data, or by inputting the received password or data into an algorithm and determining whether the result matches or otherwise corresponds with a predetermined result).

[0114] If the reader 412 determines that the password or other data received from the secondary mobile device 404 is valid, then the reader 412 grants access to the user 402 (step 932). Granting access may comprise unlocking a locked door, opening a door, suspending an alarm that would otherwise be triggered as the user passes through the access point associated with the reader 412, and/or any other act of granting access. Once access has been granted to the user 402, the method 400 ends (step 936).

[0115] The password or other data provided by the primary mobile device 408 to the secondary mobile device 404 and the reader 412, and by the secondary mobile device 404 to the reader 412, may be a One-Time Password (OTP) that the primary mobile device 408 communicates to the reader 412 and to the secondary mobile device 404. Alternatively,

the reader 412 may communicate the OTP to the primary mobile device 408, and the primary mobile device 408 may communicate the OTP to the secondary mobile device 404. Because the OTP can be used only once, the communication channel between the secondary mobile device 404 and the reader 412 need not (but may) be encrypted. When less security is required, the password or other data provided by the secondary mobile device 404 to the reader 412 may be an identification number (e.g. a serial number) associated with the secondary mobile device 404, which the primary mobile device 408 communicates to the reader 412 during or after the authentication/authorization process between the primary mobile device 408 and the reader 412. For added security, the reader 412 may be configured to grant access only if it receives the password or other data from the secondary mobile device 404 (e.g. an OTP, an identification number, etc.) within a certain time period after the authentication/authorization process between the primary mobile device 408 and the reader 412 is complete.

[0116] Embodiments of the present disclosure may be implemented using any known authentication protocol, including the FIDO authentication protocol and the authentication protocol implemented by the SEOS platform. (SEOS, which is proprietary to ASSA ABLOY, provides an ecosystem for issuing, delivering, and revoking digital keys on mobile devices.)

[0117] 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.

[0118] 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.

[0119] 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.

[0120] 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.

[0121] 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.

[0122] 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.

[0123] 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.

[0124] In other embodiments, 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.

[0125] 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.

[0126] 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.

[0127] 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.

[0128] 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.

[0129] Any of the steps, functions, and operations discussed herein can be performed continuously and automatically.

[0130] 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. An access control system, comprising:
a primary mobile device comprising:
a first processor;
a first memory comprising a key vault in which a credential is stored; and
a first communication transceiver in communication with the processor and the memory, the first communication transceiver enabling the primary mobile device to send and receive wireless communications;
a secondary mobile device comprising:
a second processor;
a second memory; and
a second wireless communication transceiver in communication with the second processor and the second memory, the second wireless communication transceiver enabling the secondary mobile device to exchange communications with the primary mobile device; and
a reader comprising:
a lock mechanism interface;
a third processor;
a third memory; and
a third wireless communication transceiver in communication with the third processor and the third memory,
wherein the third memory comprises instructions for execution by the third processor that, when executed by the third processor, cause the third processor to:
perform an initial authentication with the primary mobile device, thereby establishing a level of trust between the reader and the primary mobile device;
following the initial authentication, require the primary mobile device to communicate with the secondary mobile device and obtain at least one piece of information from the secondary mobile device;
receive the at least one piece of information at the reader;
analyze the at least one piece of information at the reader; and
based on the analysis of the at least one piece of information, make an access control decision at the reader with respect to a holder of the primary mobile device and a wearer of the secondary mobile device.

2. The access control system of claim 1, wherein the primary mobile device comprises at least one of a smartphone, a cellular phone, and a tablet, and wherein the secondary mobile device comprises a wearable device.

3. The access control system of claim 1, wherein the at least one piece of information is communicated by both the second wireless communication transceiver and the first wireless communication transceiver.

4. The access control system of claim 1, wherein the at least one piece of information is communicated directly from the second wireless communication transceiver to the third wireless communication transceiver.

5. The access control system of claim 1, wherein the reader communicates with one of the primary mobile device and the secondary mobile device via the third wireless communication transceiver using a first communication protocol, and wherein the primary mobile device communicates with the secondary mobile device via the first wireless communication transceiver using a second communication protocol.

6. The access control system of claim 5, wherein the first communication protocol is one of RFID and NFC, and the second communication protocol is one of Bluetooth, Bluetooth low energy (BLE), and WiFi.

7. The access control system of claim 1, wherein the third memory comprises further instructions for execution by the third processor that, when executed by the third processor, cause the third processor to:

accept receipt of a credential from the primary mobile device only in response to determining that the at least one piece of information is a valid piece of information.

8. A method of making an access control decision in a physical access control system, the method comprising:

performing an initial authentication between an access control reader and primary mobile device to establish a level of trust between the reader and primary mobile device;

following the initial authentication, receiving, at a processor of the access control reader, a credential from the primary mobile device;

determining, with the processor, whether the credential is valid;

receiving, at the processor, a first password from the primary mobile device;

receiving, at the processor, a second password from a secondary mobile device;

comparing, with the processor, the first password with the second password; and

based on the determination and the comparison, selectively operating a lock mechanism in communication with the reader to grant access to a protected resource.

9. The method of claim 8, wherein the first password is received via a first communication interface using a first communication protocol and the second password is received via a second communication interface using a second communication protocol different than the first communication protocol.

10. The method of claim 9, wherein one of the first communication protocol and the second communication protocol is an NFC protocol.

11. The method of claim 8, wherein one of the primary mobile device and the secondary mobile device is a wearable mobile device.

12. The method of claim 8, wherein the password is a one-time password.

13. The method of claim 8, wherein the credential is received from the primary mobile device via an encrypted communication channel.

14. A mobile device, comprising:

a processor;

a wireless radio in communication with the processor;

a contactless communication interface, different than the wireless radio, in communication with the processor; and

a memory having a key vault in which a credential is stored, the memory further storing instructions for execution by the processor, the instructions, when executed by the processor, causing the processor to:

transmit a signal to an access control reader via one of the wireless radio and the contactless communication interface;

transmit subsequent signals to the access control reader and a secondary mobile device in accordance with a predetermined communication path; and

transmit the credential to the access control reader.

15. The mobile device of claim 14, wherein the instructions cause the processor to transmit the subsequent signals to the access control reader via a first communication protocol and further cause the processor to transmit the subsequent signals to the secondary mobile device via a second communication protocol different than the first communication protocol.

16. The mobile device of claim 14, wherein the predetermined communication path is provided to the mobile device via one of the wireless radio and the contactless communication interface.

17. The mobile device of claim 14, wherein the predetermined communication path, or information corresponding to the predetermined communication path, is stored in the memory.

18. The mobile device of claim 14, wherein the contactless communication interface comprises at least one of a Bluetooth and an NFC interface.

19. The mobile device of claim 14, wherein the subsequent signals transmitted to the access control reader and the secondary mobile device comprise a password.

20. The mobile device of claim 14, wherein the instructions, when executed by the processor, cause the processor to transmit the signal to the access control reader in response to receiving a first signal from the access control reader.

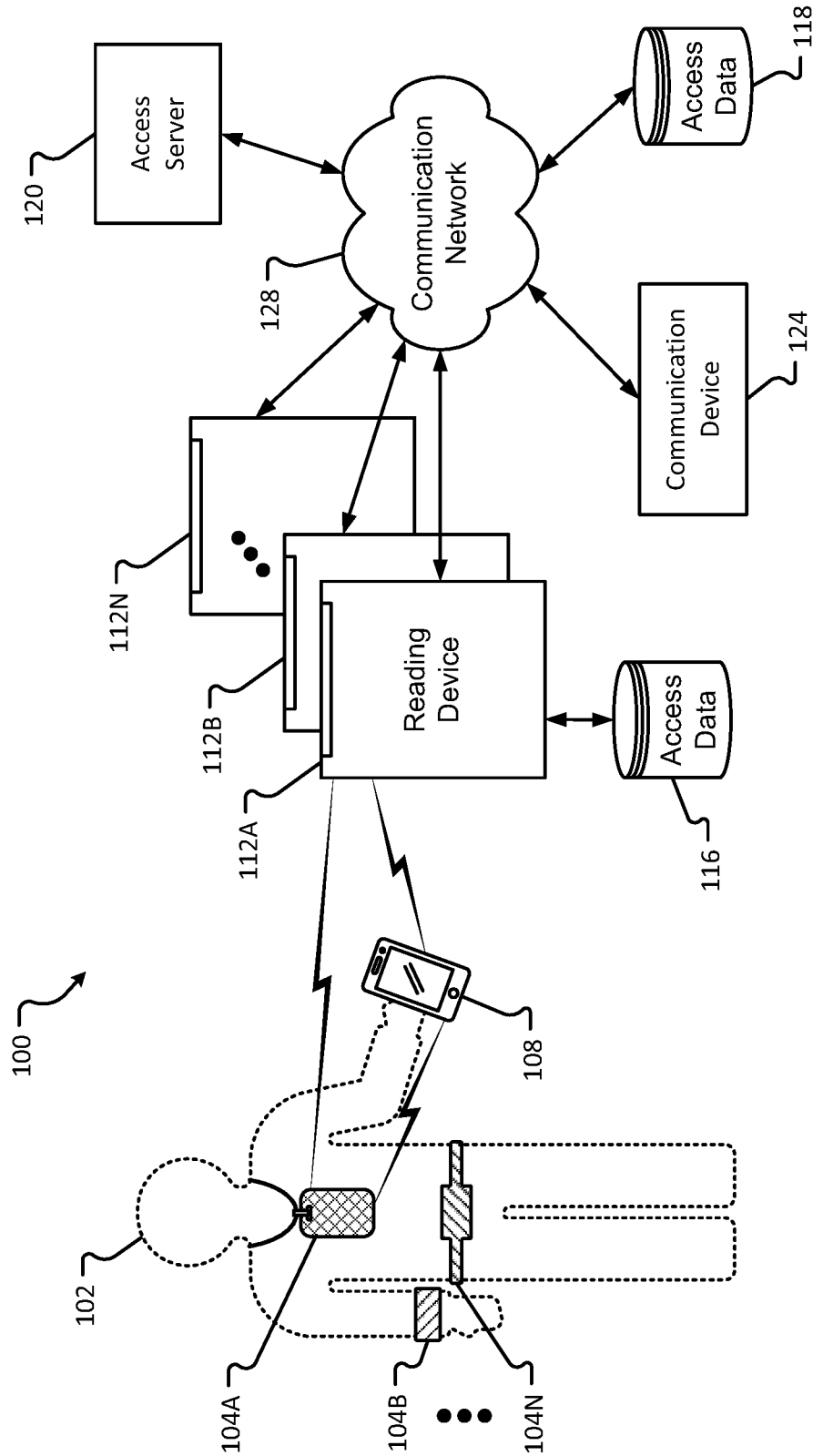
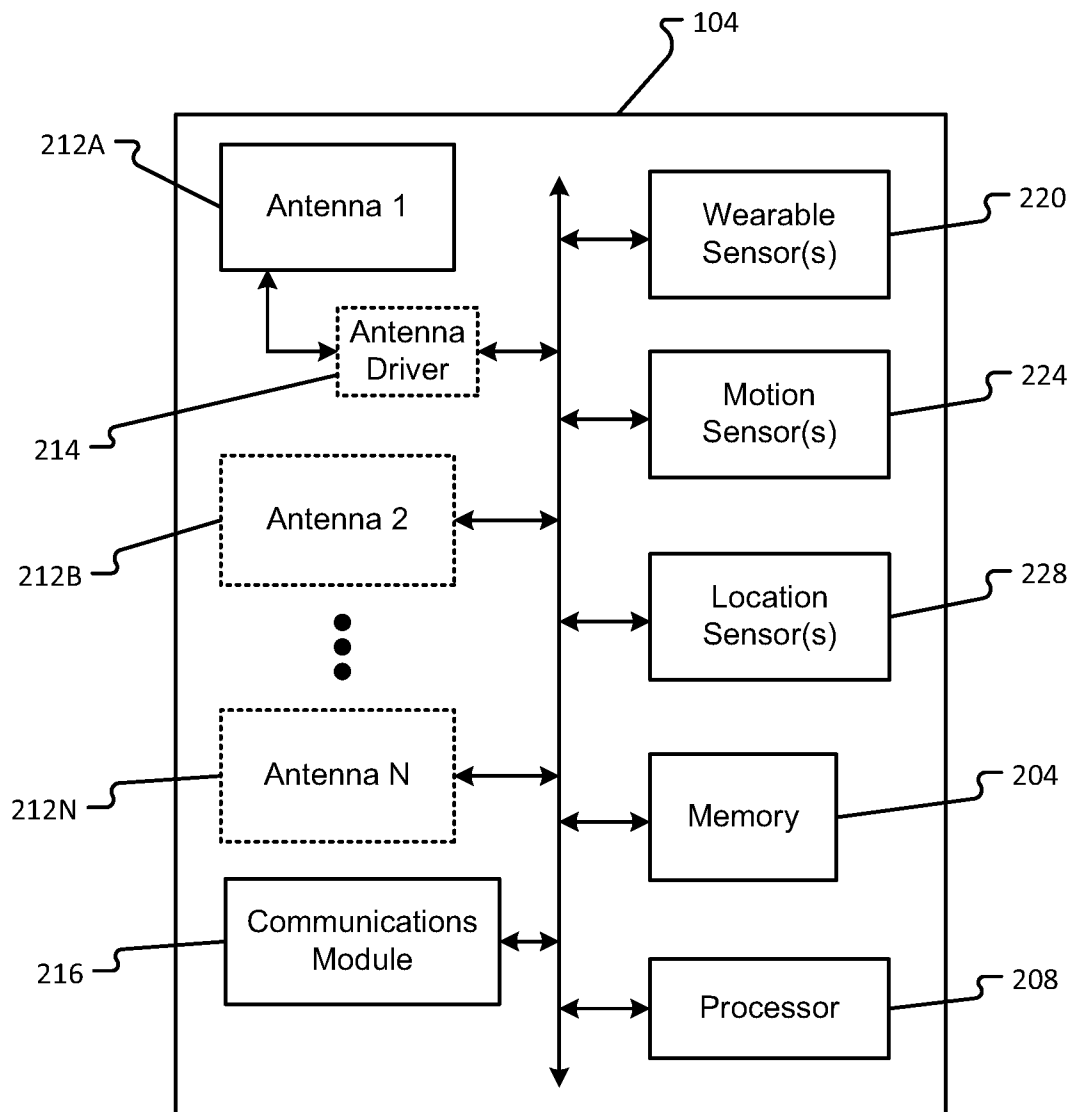
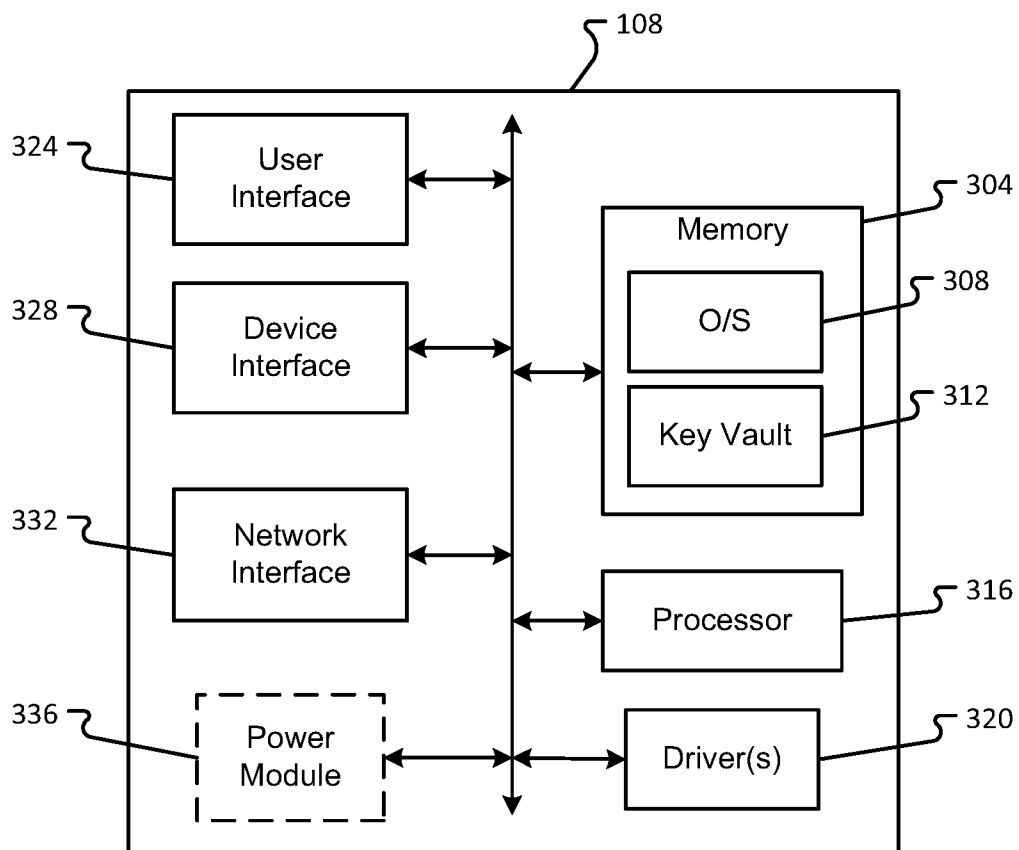


Fig. 1

**Fig. 2**

**Fig. 3**

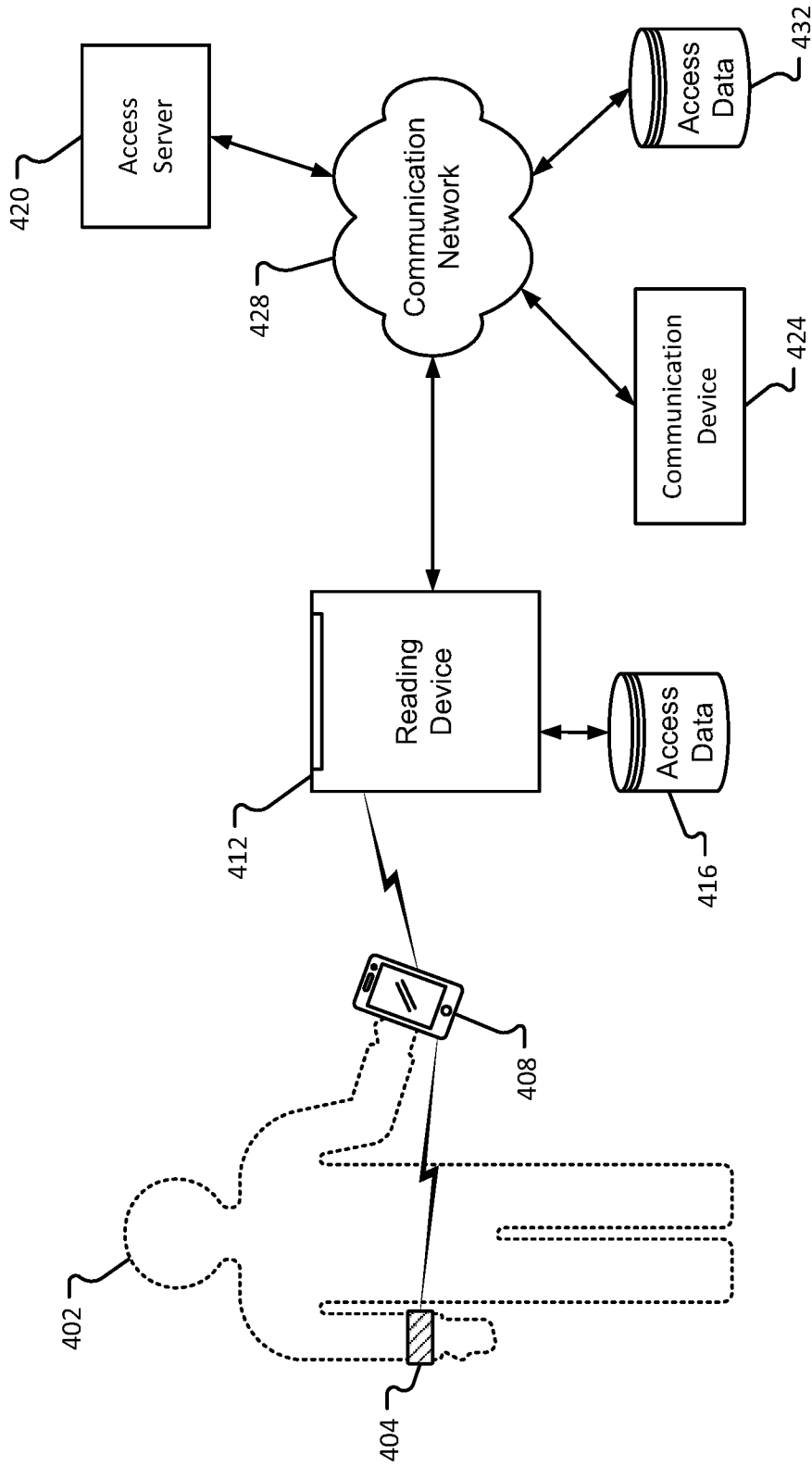


Fig. 4

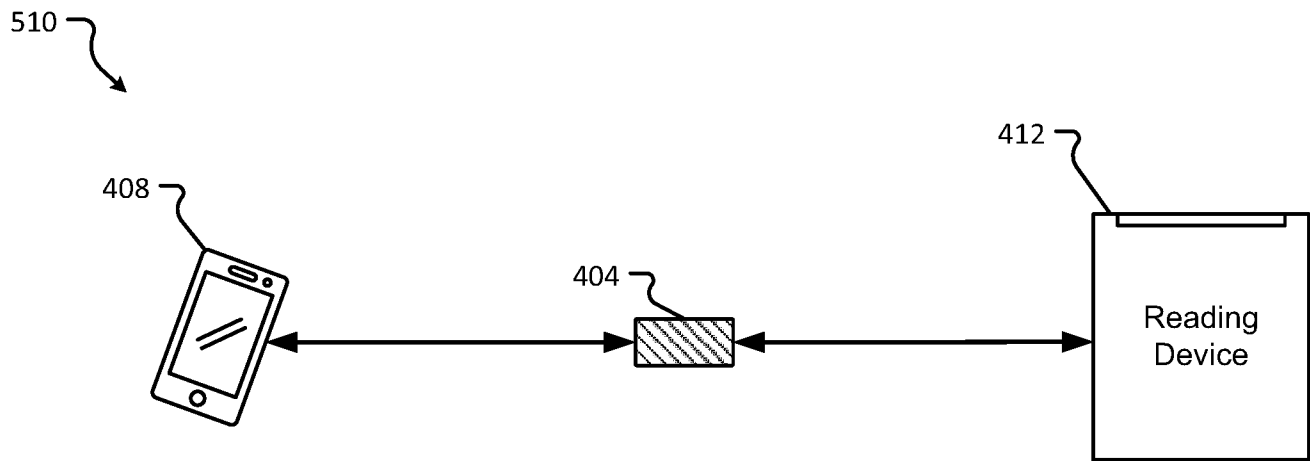


Fig. 5A

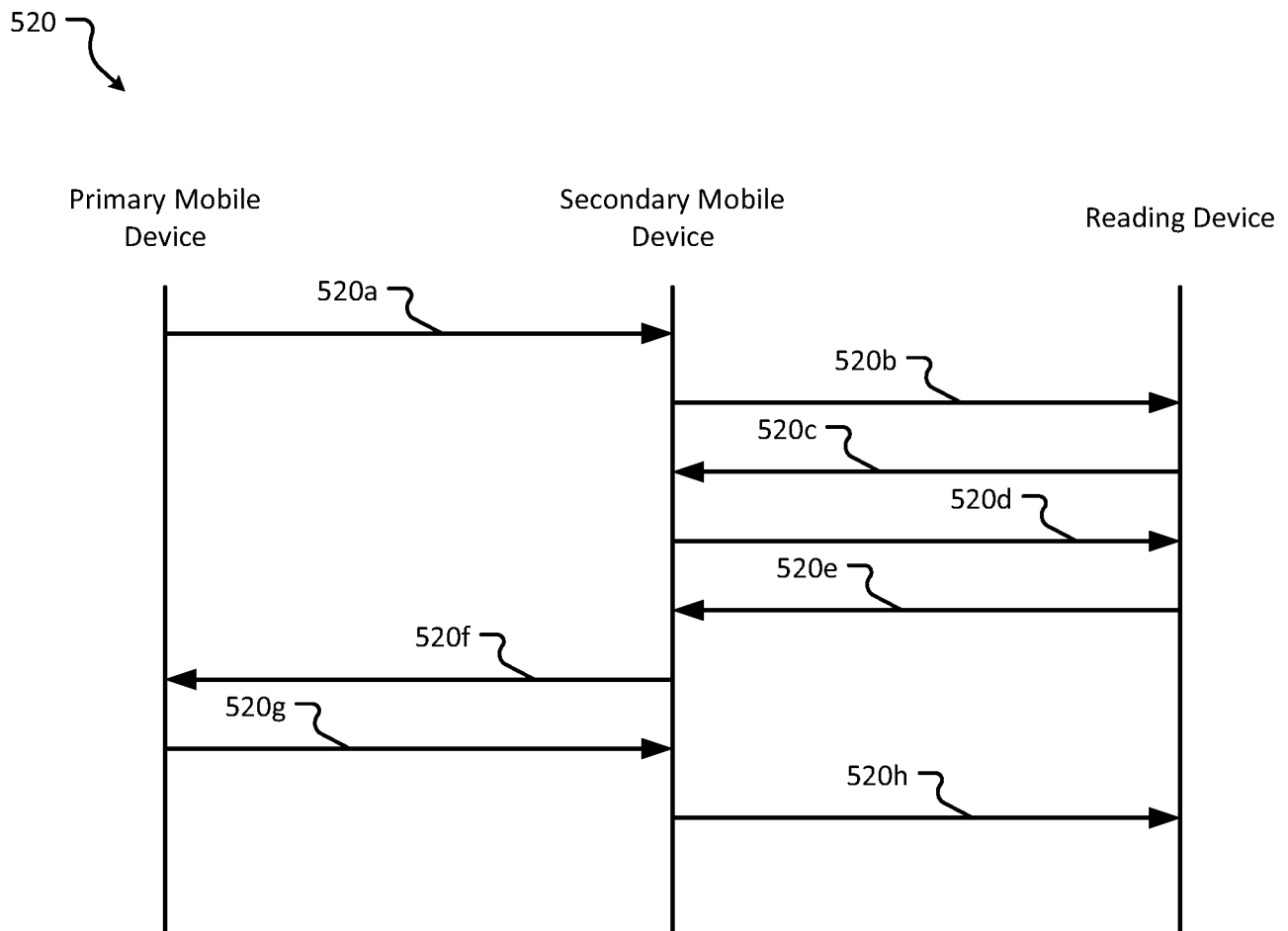
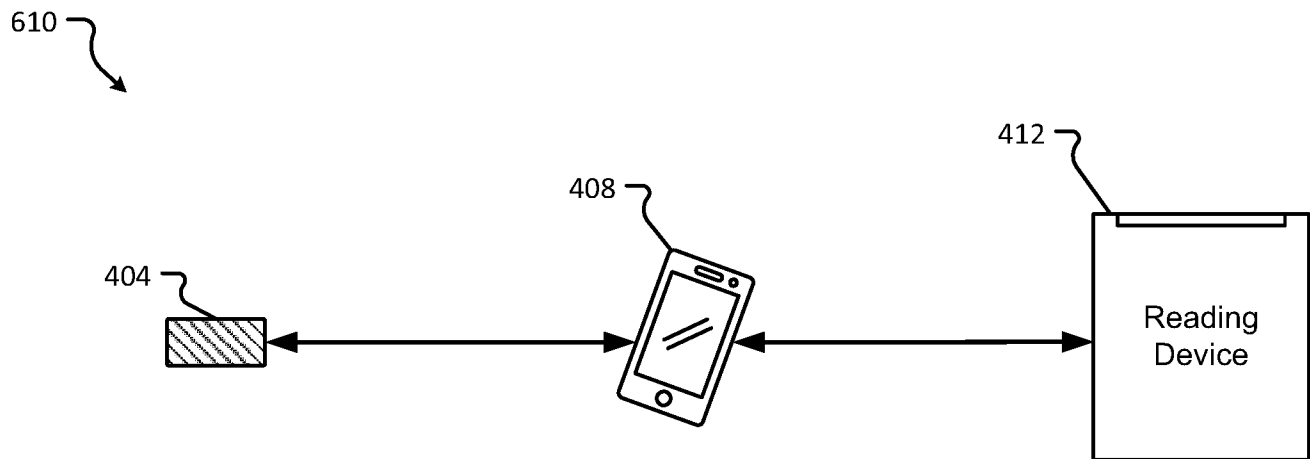
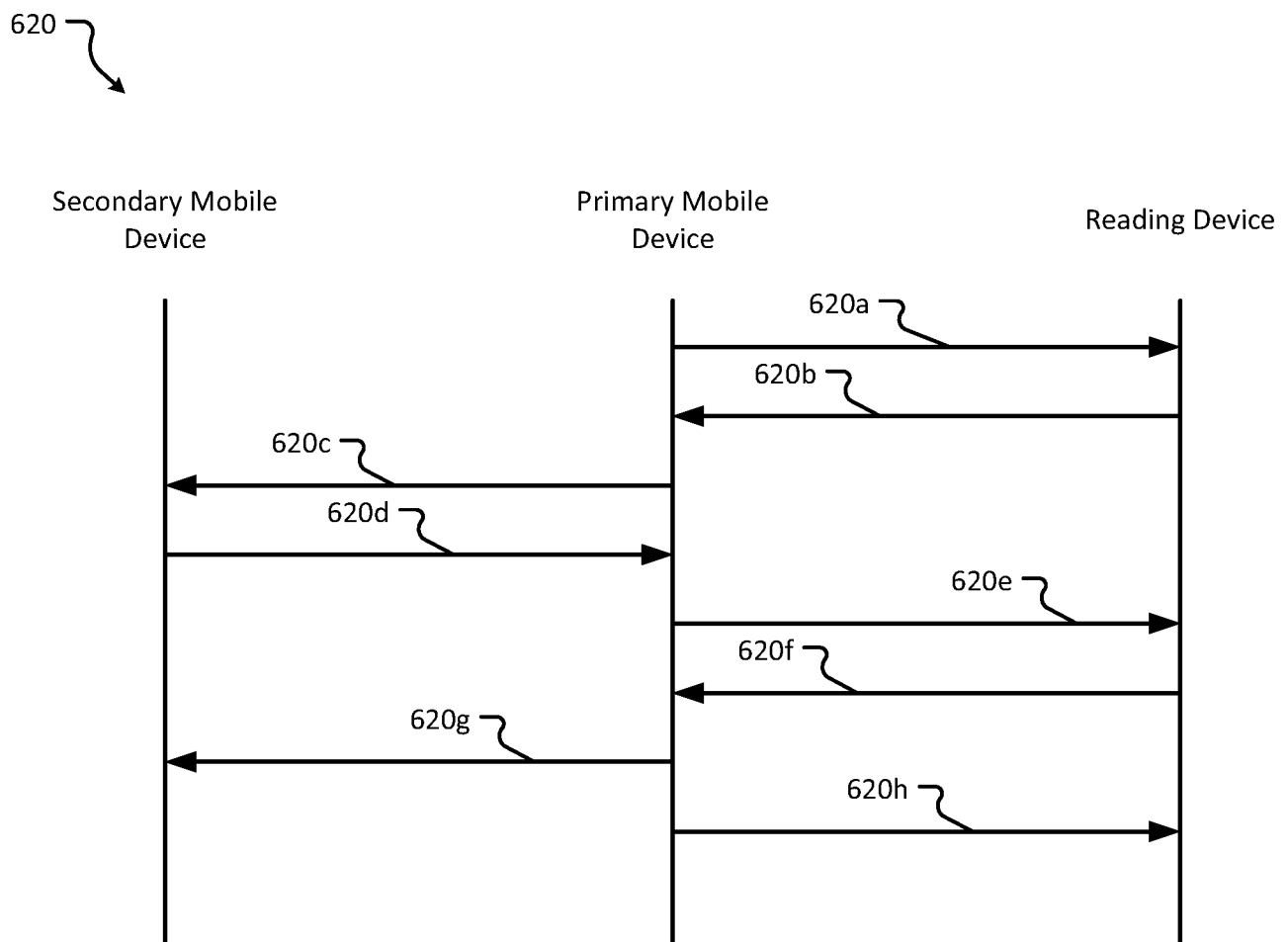


Fig. 5B

**Fig. 6A****Fig. 6B**

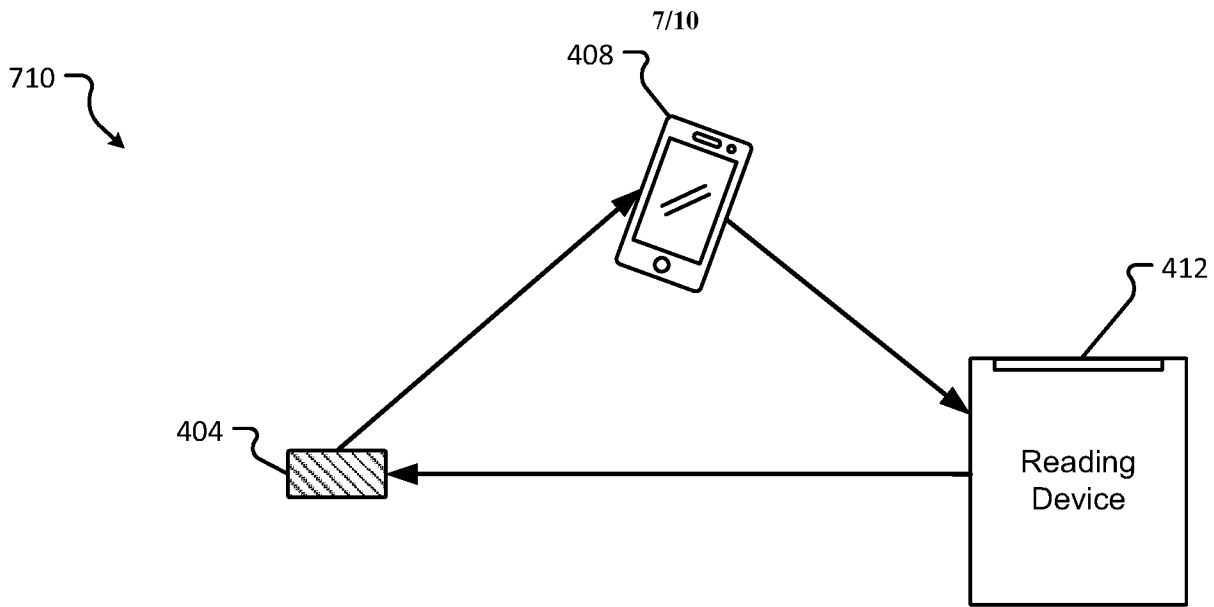


Fig. 7A

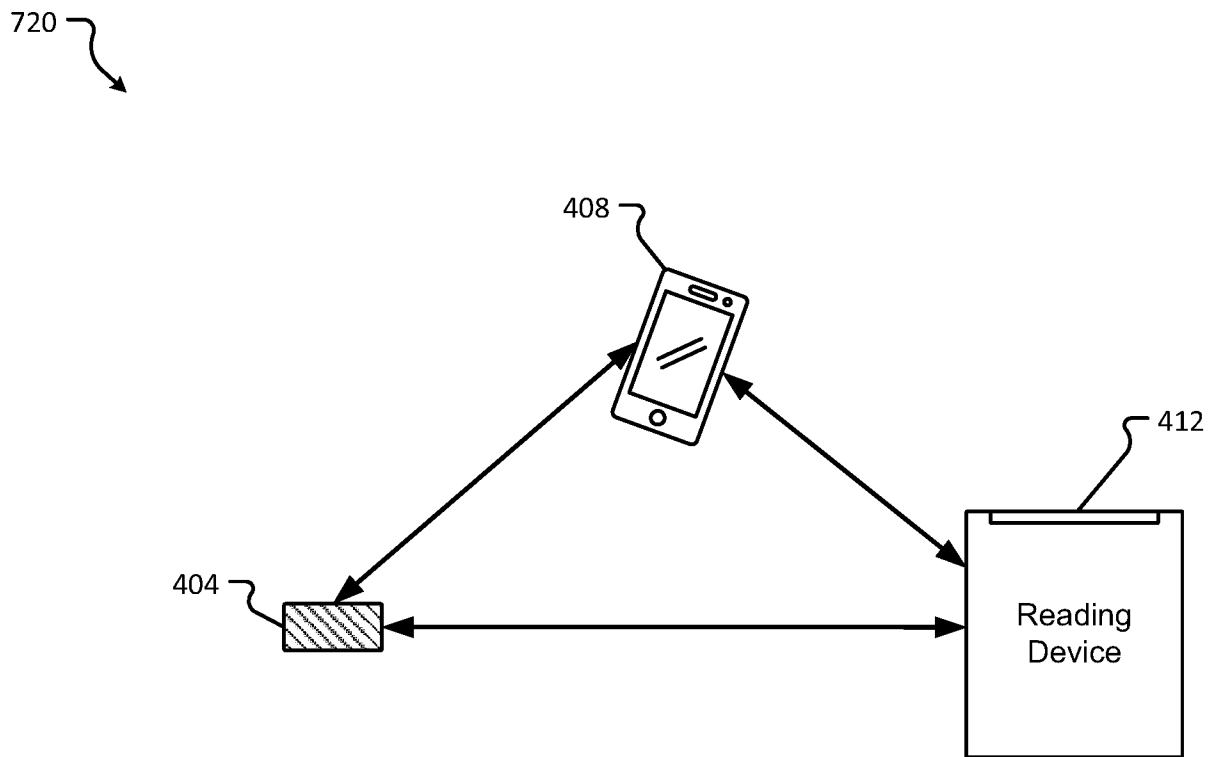
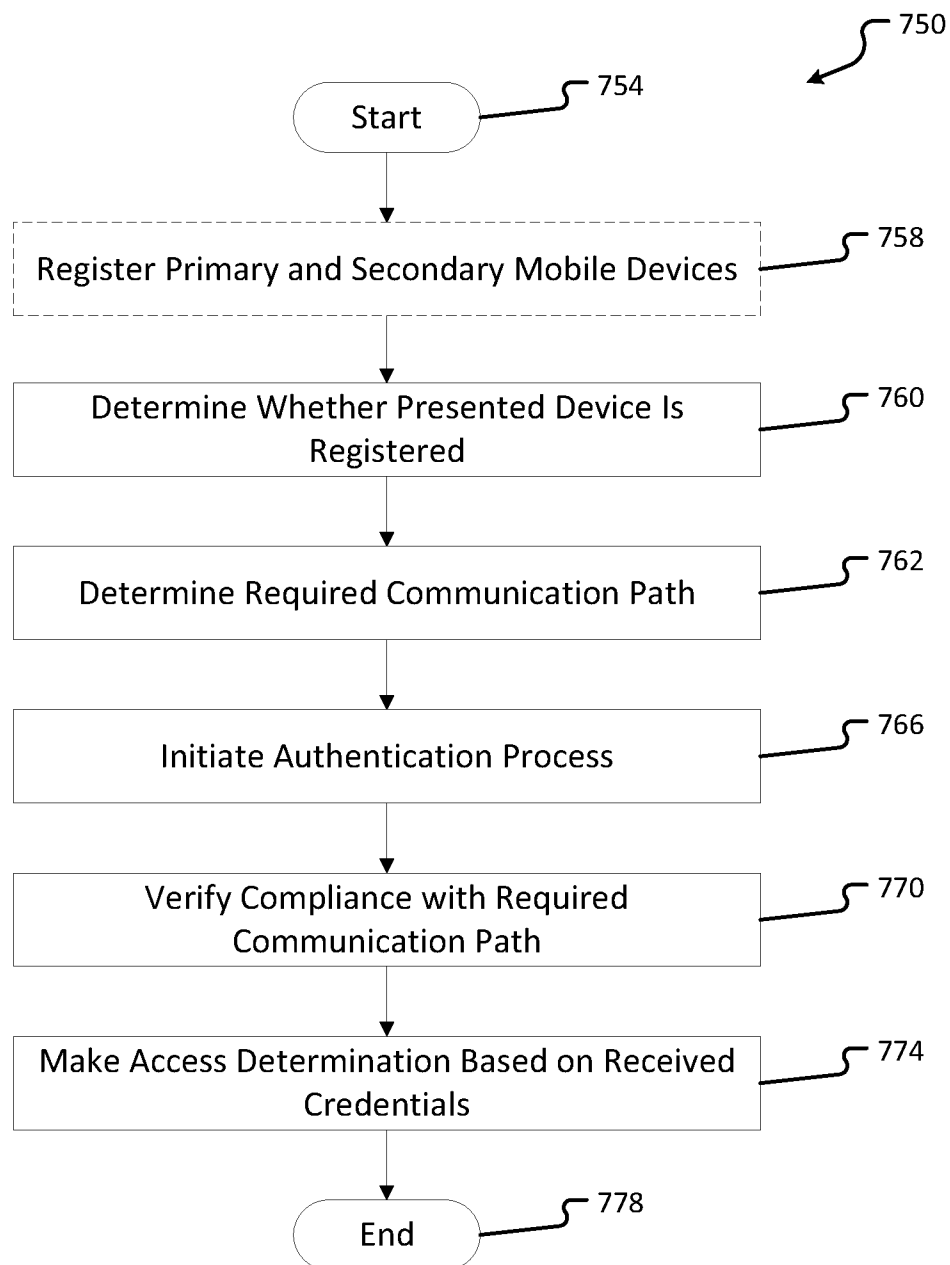


Fig. 7B

**Fig. 7C**

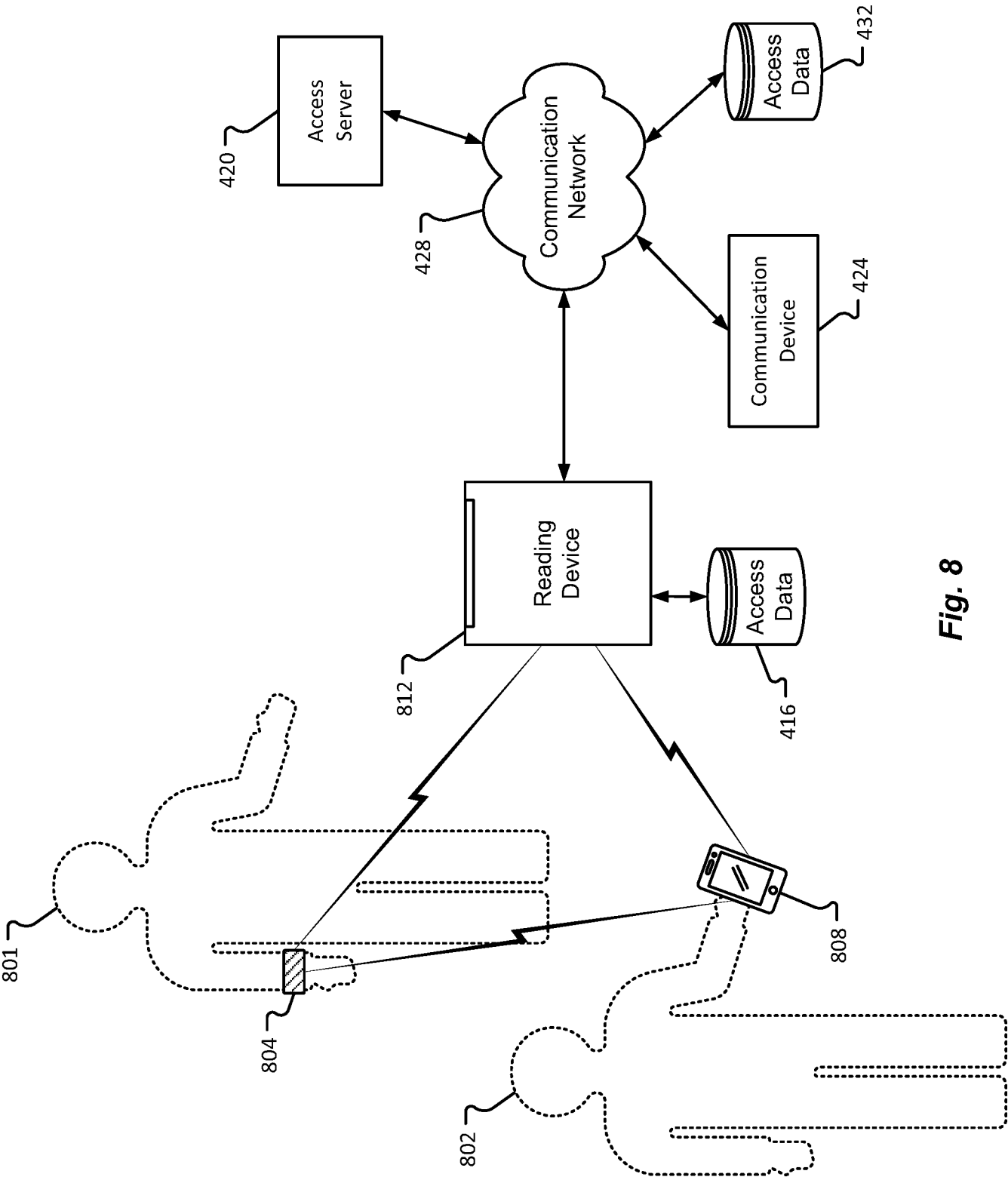
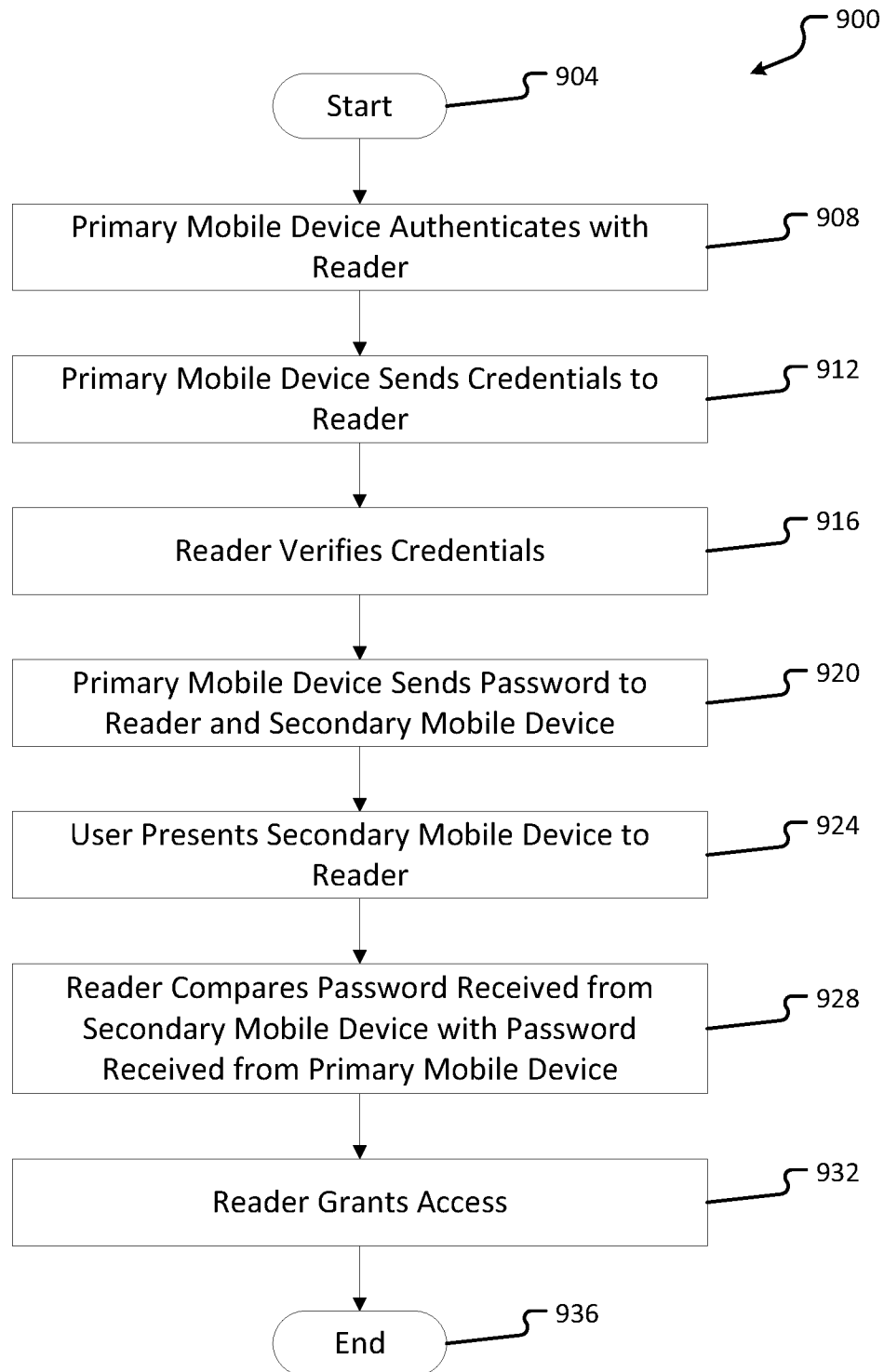


Fig. 8

**Fig. 9**

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2016/000654

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/08 H04W12/06

ADD. G06F1/16 G06F21/34 H04L29/06 H04W4/00 H04L29/08

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

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 710 974 A1 (TOSHIBA KK [JP]) 11 October 2006 (2006-10-11) abstract; figures 1-7 paragraphs [0005], [0009] - [0028], [0031] - [0034], [0037] - [0041], [0044] - [0087] paragraph [0104] -----	1-20
X A	EP 1 926 038 A1 (MATSUSHITA ELECTRIC IND CO LTD [JP]) 28 May 2008 (2008-05-28) abstract; figures 1, 5, 7, 13, 18, 19, 37-39, 41-43, 53-55, 56 paragraphs [0231] - [0239], [0245] - [0248] ----- -/--	1-4, 14 5-13, 15-20



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

29 July 2016

Date of mailing of the international search report

08/08/2016

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/IB2016/000654

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/124855 A1 (VARADARAJAN RAMMOHAN [US] ET AL) 16 May 2013 (2013-05-16) abstract; figures 2A, 2B, 4 paragraphs [0034], [0038], [0039], [0043], [0046], [0047], [0057] - [0064] -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2016/000654

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1710974	A1	11-10-2006	CN 1848140 A	18-10-2006
			EP 1710974 A1	11-10-2006
			JP 2006295234 A	26-10-2006
			KR 20060107315 A	13-10-2006
			SG 126101 A1	30-10-2006
			US 2006219778 A1	05-10-2006

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

US 2013124855	A1	16-05-2013	US 2013124855 A1	16-05-2013
			US 2015088758 A1	26-03-2015
