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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2016 (10.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/177671 A1

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

(21) International Application Number:
PCT/EP2016/059752

(22) International Filing Date:
2 May 2016 (02.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/156,035	1 May 2015 (01.05.2015)	US
62/156,030	1 May 2015 (01.05.2015)	US
62/161,640	14 May 2015 (14.05.2015)	US
62/162,273	15 May 2015 (15.05.2015)	US
62/164,099	20 May 2015 (20.05.2015)	US
62/167,172	27 May 2015 (27.05.2015)	US
62/167,136	27 May 2015 (27.05.2015)	US
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]; P.O. Box 70340, 107 23 Stockholm (SE).

(72) Inventors: **EINBERG, Fredrik**; Klyftvägen 8, 141 41 Huddinge (SE). **HOYER, Philip**; 43 Manor Road, Richmond TW9 1YA (GB). **BERG, Daniel**; Grönlingens väg 25, 174 62 Sundbyberg (SE).

(74) Agent: **KRANSELL & WENNBORG KB**; P.O Box 27834, 115 93 Stockholm (SE).

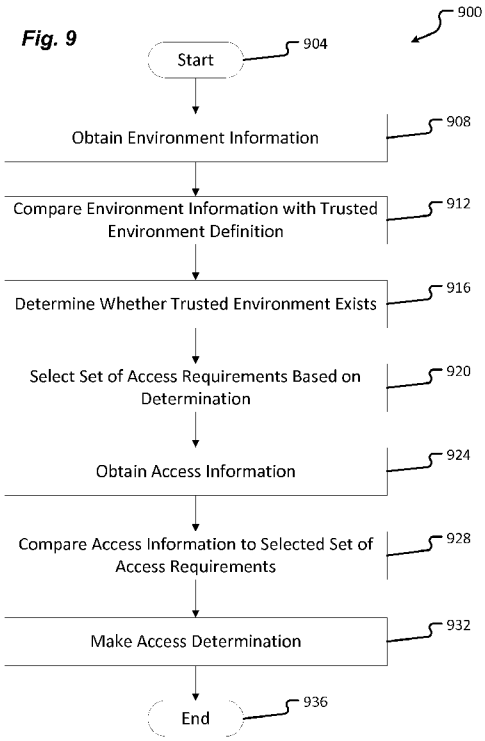
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, 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,

[Continued on next page]

(54) Title: USING A SECONDARY MOBILE DEVICE TO IDENTIFY A TRUSTED ENVIRONMENT

Fig. 9



(57) Abstract: An access control system is described in which the access control requirements enforced by one or more components of the access control system correspond to the environment of the one or more components of the access control system. A trusted environment may be defined that corresponds to a less restrictive or less burdensome set of access control requirements. A mobile device may be used to provide information about the environment to one or more other components of the access control system.

WO 2016/177671 A1

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

USING A SECONDARY MOBILE DEVICE TO IDENTIFY A TRUSTED ENVIRONMENT

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] The proliferation of wearable mobile devices presents an opportunity to enhance access control system functionality. Such 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.

[0010] Some access control systems are configured to grant or deny access based not only on the presentation of electronic credentials (e.g. a mobile key stored on a mobile device), but also upon information received from biometric sensors in communication with the access control reader (e.g. fingerprint readers, retina scanners, etc.), information received from sensors integrated into the same mobile device(s) in which the mobile key is stored, or other sources. Greater security can often be provided by increasing the number of requirements that must be satisfied before access is granted. Increasing the number of requirements that must be satisfied to gain access, however, often causes greater inconvenience to users of the protected resource, by increasing the amount of time or effort it takes to complete the authorization process.

[0011] In accordance with embodiments of the present disclosure, user inconvenience can be reduced while security is maintained by defining one or more trusted environments and reducing or changing authorization requirements when a trusted environment is recognized. Alternatively, authorization requirements may be added or enhanced when a trusted environment is not recognized or when a distrusted environment is recognized. A user's mobile device(s) may be used to identify a trusted environment (or lack thereof).

[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 may be employed by the wearable device and/or the mobile device. Examples of communications protocols can include, but are in no way limited to, the protocol or protocols associated with near field communication (NFC), radio frequency identification (RFID) (e.g., operating at 125kHz, 13.56kHz, etc.), Bluetooth® wireless communication, Bluetooth® Low Energy (BLE), Personal Area Network (PAN), Body Area Network (BAN), cellular communications, WiFi communications, and/or other wireless communications.

[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 block diagram depicting a reading device or components thereof in accordance with embodiments of the present disclosure;

[0034] Fig. 5A is a diagram depicting an access control system in accordance with other embodiments of the present disclosure;

[0035] Fig. 5B is a block diagram depicting a mobile device or components thereof in accordance with other embodiments of the present disclosure;

[0036] Fig. 6A is a diagram depicting an access control system in accordance with still other embodiments of the present disclosure;

[0037] Fig. 6B is a diagram depicting an access control system in accordance with yet another embodiment of the present disclosure;

[0038] Fig. 7 is a diagram depicting still another embodiment of the present disclosure in an office setting;

[0039] Fig. 8 is a block diagram depicting an access server or components thereof in accordance with embodiments of the present disclosure;

[0040] Fig. 9 is a flowchart depicting a method according to some embodiments of the present disclosure; and

[0041] Fig. 10 is a flowchart depicting a method according to other embodiments of the present disclosure.

DETAILED DESCRIPTION

[0042] 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.

[0043] According to one embodiment of the present disclosure, an access control reader includes a processor, a communication interface, and a memory. The memory stores instructions that, when executed by the processor, cause the processor to obtain information about the environment surrounding the reader, compare the information with a trusted environment definition, and select, based on the comparison, one of a first and a second set of access control requirements for use in making an access determination.

[0044] The information about the environment surrounding the reader may include information about a physical environment of the reader, information about the an electromagnetic environment of the reader, and/or information about a location of the reader. The information about the physical environment of the reader may include temperature information, lighting information, audio information, and/or humidity information. The information about the electromagnetic environment of the reader may include information about a wireless network from which the reader receives a wireless signal, information about a cellular network tower from which the reader receives a wireless signal, and/or information about a mobile device from which the reader receives a wireless signal.

[0045] Additionally, the information about the environment surrounding the reader may include information about a detected mobile device's physical environment; information about the detected mobile device's electromagnetic environment; information about the detected mobile device's location; and/or identifying characteristics of the detected mobile device. The information about the environment surrounding the reader may be obtained from one or more sensors on the reader.

[0046] Further, the first set of access control requirements may correspond to a trusted environment. The first set of access control requirements may be a subset of the second set of access control requirements.

[0047] In some embodiments, the information about the environment surrounding the reader may correspond to: the reader's inability to connect to a known wireless network; the reader's inability to detect a specific wireless network; the reader's inability to detect any wireless networks; the reader's inability to communicate with another device; the reader's inability to detect a specific device; the reader's detection of an unknown device; the reader's detection of a known mobile device having one or more settings that do not match one or

more predetermined settings; and/or the reader's detection of a mobile device in a locked condition.

[0048] At least one of the first and second sets of access control requirements may be stored on a device other than the reader. That device may be an external memory, a host computer, or a control panel.

[0049] According to another embodiment of the present disclosure, an access control system includes a processor, a communication interface, and a computer readable memory. The computer readable memory stores a trusted environment definition that comprises information about one or more characteristics of a trusted environment, a primary set of access control requirements and a secondary set of access control requirements, and access control instructions. The access control instructions cause the processor to obtain at least one current environmental characteristic, selectively apply the primary set of access control requirements or the secondary set of access control requirements based on whether the at least one current environmental characteristic corresponds to the trusted environment definition, receive a credential from a mobile device via the communication interface, and make an access determination based on the credential and the selectively applied primary set of access control requirements or secondary set of access control requirements.

[0050] A reader may receive the current environmental characteristic from the mobile device. Also, the primary set of access control requirements may comprise fewer requirements than the secondary set of access control requirements.

[0051] In yet another embodiment according to the present disclosure, a method comprises enabling an access control reader to communicate with a first and second mobile device; based on environmental information received at the reader from the first and second mobile device, selecting whether to apply a first set of access control requirements or a second set of access control requirements; and applying the selected first or second set of access control requirements at the reader with respect to making an access control decision for a holder of either the first or second mobile device.

[0052] The method may further comprise determining, based on the environmental information, that a trusted environment exists; and in response to determining that a trusted environment exists, selecting the first set of access control requirements. The trusted environment may be determined to exist in response to receiving substantially similar environmental information from both the first mobile device and the second mobile device.

The environmental information may describe at least one of a temperature, sound profile, or light profile in proximity to the first mobile device and the second mobile device.

[0053] Also, the environmental information may describe network information available to the first mobile device and the second mobile device. The environmental information may further relate to at least one of a temperature, a noise level, a noise profile, a lighting level, an electromagnetic signal, and a wireless connection.

[0054] 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.

[0055] 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. 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 well as a greater array of sensors and interfaces through which to gather information. As described herein, these advantages may be exploited to allow an access control system to identify a trusted environment (or lack thereof) and adjust authorization requirements accordingly.

[0056] Fig. 1 is a diagram depicting an access control system 100 for authenticating a user 102 via wearable devices 104 in accordance with embodiments of the present disclosure. In one embodiment, the access control system 100 comprises at least one reading device 112, at

least one wearable device 104, and at least one portable/mobile device 108. The reading device 112 may include an access data memory 116. The access data memory 116 may be configured to store access information, identification data, rules, program instructions, and/or other data associated with performing access operations of an access control system 100. In some embodiments, the reading device 112 may be configured to communicate with an access data memory 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.

[0057] The wearable device 104 and/or the mobile device 108 may be configured to communicate with a reading device 112 across one or more wireless communication connections. These one or more wireless communication connections can include communications via at least one of conventional radio protocols, proximity-based wireless communication protocols, Bluetooth™, BLE, infrared, audible, NFC, RF, and other wireless communication networks and/or protocols. In some cases, communications between the wearable device 104 and the reading device 112 may be established automatically when the wearable device 104 enters an active zone of an interrogating reading device 112. In one embodiment, the active zone of the reading device 112 may be defined as a three-dimensional space where the intensity of RF signals emitted by the reading device 112 exceeds a threshold of sensitivity of the wearable device 104 and the intensity of RF signals emitted by the wearable device 108 exceeds a threshold of sensitivity of the reading device 112.

[0058] In some embodiments, the wearable device 104 and/or the mobile device 108 may be configured to communicate with a reading device 112 across a communication network 128. The communication network 128 can include communication via at least one of conventional radio networks, wireless communication networks, Zig-Bee, GSM, CDMA, WiFi, and/or using other communication networks and/or protocols as provided herein.

[0059] In one embodiment, authentication may be required between the wearable device 104 and the reading device 112 before further communications are enabled. Additionally or alternatively, authentication may be required between the wearable device 104 and the mobile device 108 before further communications are enabled. In any event, the further communications may provide communications in which access control information (e.g., keys, codes, credentials, etc.) are shared. In some embodiments, the authentication may be provided via one-way or mutual authentication. Examples of authentication may include, but are not limited to, simple authentication based on site codes, trusted data formats, shared secrets, and/or the like. As can be appreciated, access control information is more sensitive

and may require more involved validation via, for example, an encrypted exchange of access control information.

[0060] 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 and/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.

[0061] 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.

[0062] 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.

[0063] 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.

[0064] 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.

[0065] 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.

[0066] 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.

[0067] 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 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.

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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.).

[0072] 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, or the mobile device 108 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.

[0073] 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.

[0074] Fig. 3 shows a block diagram depicting a mobile device 108 in accordance with embodiments of the present disclosure. The mobile device 108 may correspond to any type of electronic device and, as the name suggests, the electronic device may be portable in nature. As some examples, the mobile device 108 may correspond to a cellular phone or smartphone carried by a user. Other examples of a mobile device 108 include, without limitation, wearable devices (e.g., glasses, watches, shoes, clothes, jewelry, wristbands, stickers, etc.). The mobile device 108, as shown in Figs. 1 and 3, may be provided with a key vault 312 that stores one or a plurality of keys. The key(s) may be communicated to a reader 112 in connection with a holder of the mobile device 108 attempting to gain access to an asset protected by the reader 112. As an example, the mobile device 108 may be presented to the reader 112 by a user 102 or holder of the mobile device 108.

[0075] If NFC is being used for the communication channel, then the reader 112 and mobile device 108 may have their interfaces/antennas inductively coupled to one another at which point the reader and/or mobile device 108 will authenticate or mutually authenticate with one another. Following authentication, the reader 112 may request a key or multiple keys from the mobile device 108, or the mobile device 108 may offer a key or multiple keys to the reader 112. Upon receiving the key(s) from the mobile device 108, the reader 112 may analyze the key(s) and determine if the key(s) are valid and, if so, allow the holder/user of the mobile device 108 access to the asset protected by the reader 112. It should be appreciated that the mobile device 108 may alternatively or additionally be configured to analyze information received from the reader 112 in connection with making an access control decision and/or in connection with making a decision whether or not to provide key(s) to the reader 112. Examples of technologies that can be used by the mobile device 108 to make an access control decision for itself are further described in U.S. Patent No. 8,074,271 to Davis

et al. and U.S. Patent No. 7,706,778 to Lowe, both of which are hereby incorporated herein by reference in their entirety.

[0076] If BLE or some other non-inductive protocol (e.g., Wi-Fi) is being used for the communication channel, then the reader 112 and mobile device 108 may perform a discovery routine prior to pairing with one another or otherwise connecting to establish the communication channel. After the channel is established, however, the reader 112 and mobile device 108 may then authenticate one another and exchange relevant information, such as the key(s), to enable an access control decision to be made. If a positive access control decision is made (e.g., it is determined that the key(s) are valid and the mobile device 108 is allowed to access the asset protected by the reader 112), then the reader 112 may initiate one or more actions to enable the holder/user 102 of the mobile device 108 to access the asset protected by the reader 112.

[0077] The mobile device 108 is shown to include computer memory 304 that stores one or more Operating Systems (O/S) 308 and a key vault 312, among other items. The mobile device 108 is also shown to include a processor 316, one or more drivers 320, a user interface 324, a reader interface 328, a network interface 332, and a power module 336. Suitable examples of a mobile device 108 include, without limitation, smart phones, PDAs, laptops, PCs, tablets, netbooks, wearable devices, and the like.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] The driver(s) 320 may correspond to hardware, software, and/or controllers that provide specific instructions to hardware components of the mobile device 108, thereby facilitating their operation. For instance, the user interface 324, reader interface 328, and network interface 332, may each have a dedicated driver 320 that provides appropriate control signals to effect their operation. The driver(s) 320 may also comprise the software or logic circuits that ensure the various hardware components are controlled appropriately and in accordance with desired protocols. For instance, the driver 320 of the reader interface 328 may be adapted to ensure that the reader interface 328 follows the appropriate proximity-based protocols (e.g., BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, etc.) such that the reader interface 328 can exchange communications with the credential. Likewise, the driver 320 of the network interface 332 may be adapted to ensure that the network interface 332 follows the appropriate network communication protocols (e.g., TCP/IP (at one or more layers in the OSI model), UDP, RTP, GSM, LTE, Wi-Fi, etc.) such that the network interface 332 can exchange communications via the communication network 128. As can be appreciated, the driver(s) 320 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0082] 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.

[0083] The reader interface 328 may correspond to the hardware that facilitates communications with the credential for the mobile device 108. The reader interface 328 may include a Bluetooth interface (e.g., antenna and associated circuitry), a Wi-Fi/802.11N interface (e.g., an antenna and associated circuitry), an NFC interface (e.g., an antenna and associated circuitry), an Infrared interface (e.g., LED, photodiode, and associated circuitry), and/or an Ultrasonic interface (e.g., speaker, microphone, and associated circuitry). In some embodiments, the reader interface 328 is specifically provided to facilitate proximity-based communications with a credential via communication channel or multiple communication channels.

[0084] 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.

[0085] 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.

[0086] Although not depicted in Fig. 3, a mobile device 108 according to embodiments of the present disclosure may also include one or more sensors similar to those described previously with respect to the wearable device 104, including, without limitation, one or more motion sensors, location sensors, light sensors, audio sensors (e.g. microphones), biometric sensors, air quality sensors, and the like.

[0087] Turning now to Fig. 4, according to embodiments of the present disclosure, a reader 412 includes a memory 404, a processor 416, one or more drivers 420, one or more sensors 424, a device interface 428, a network interface 432, and a power module 436.

[0088] Like the memory 304, the memory 404 may correspond to any type of non-transitory computer-readable medium. The memory 404 may be located locally or remotely to the other components of the reader 412. In some embodiments, the memory 404 may

comprise volatile or non-volatile memory and a controller for the same. Non-limiting examples of memory 404 that may be utilized in the reader 412 include RAM, ROM, buffer memory, flash memory, solid-state memory, or variants thereof.

[0089] The memory 404 stores a first set of access requirements 408, a second set of access requirements 410, and one or more trusted environment definitions 414. The first set of access requirements 408 applies in a non-trusted environment (e.g. an environment that does not satisfy the trusted environment definition 414) and the second set of access control requirements 410 applies in a trusted environment (e.g. an environment that does satisfy the trusted environment definition 414). The second set of access control requirements 410 may be less restrictive or less burdensome than the first set of access control requirements 408. For example, the second set of access control requirements 410 may be less restrictive because it will accept a given mobile key for a longer period of time than the first set of access control requirements 408. As another example, the second set of access control requirements 410 may comprise a subset of the requirements in the first set of access control requirements 408, and therefore may be less burdensome than the first set of access control requirements 408. The reader 412, through the processor 416 (described below), may determine whether the environment at a given point in time (e.g. during an access attempt) meets the trusted environment definition 414 based on information obtained solely from its own components (e.g. sensors, communication interfaces, etc.). Or, the reader 412 may receive information from one or more external sources (via one or more communication interfaces, including the device interface 428 and the network interface 432) that it uses, alone or in combination with information from its own components, to determine whether a trusted environment exists. Based on that determination, the reader 412 applies the appropriate set of access control requirements 408 or 410.

[0090] The processor 416 may correspond to one or many microprocessors that are contained within the housing of the reader 412. In some embodiments, the processor 416 incorporates the functions of the a Central Processing Unit (CPU) on a single Integrated Circuit (IC) or a few IC chips. The processor 416 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 416 implements sequential digital logic as it has internal memory. As with most known microprocessors, the processor 416 may operate on numbers and symbols represented in the binary numeral system.

[0091] The driver(s) 420 may correspond to hardware, software, and/or controllers that provide specific instructions to hardware components of the reader 412, thereby facilitating their operation. For instance, the sensor(s) 424, device interface 428, and network interface 432 may each have a dedicated driver 420 that provides appropriate control signals to effect their operation. The driver(s) 420 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 420 of the device interface 428 may be adapted to ensure that the device interface 428 follows the appropriate proximity-based protocols (e.g., BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, etc.) such that the device interface 428 can exchange communications with mobile devices such as mobile device 108 or wearable mobile devices 104. Likewise, the driver 420 of the network interface 432 may be adapted to ensure that the network interface 432 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 432 can exchange communications via a communication network such as the communication network 128. As can be appreciated, the driver(s) 420 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0092] The reader 412 may employ one or more sensors 424 that are configured to detect information about the environment surrounding the reader 412. The sensors 424 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, lighting sensors, temperature sensors, pressure sensors, contact sensors, air quality sensors, humidity sensors, audio sensors, combinations thereof, and the like. It is an aspect of the present disclosure that the processor 416 of the reader 412 may receive information from the one or more sensors 424 and determine whether the environment surrounding the reader 412 satisfies the trusted environment definition 414. One or more sensors 424 may also be used to gather information required by the first or second sets of access requirements 408 and 410. By way of example, if the trusted environment definition 414 is not met, then the first set of access requirements 408 may require a fingerprint or retina scan using a biometric sensor 424 to determine whether a person seeking access to a resource protected by the reader 412 is authorized to obtain such access. A biometric sensor 424 may be configured to obtain many other kinds of biometric information, including, e.g., a heart rate, a blood pressure, a body temperature, etc.

[0093] The sensor(s) 424 may also be or include a motion sensor, including, for example, one or more of a gyroscope, accelerometer, transducer, and/or other mechanical detection component configured to detect a force and/or motion associated with the reader 412. Although readers such as reader 412 are typically affixed to a building wall or other stationary surface and are therefore unlikely to be in motion, the detection of motion using a motion sensor 424 may be an indication that the environment is not trusted. Additionally, motion sensors 424 may be utilized on readers 412 that are used to protect access to portable or semi-portable devices or to secure spaces in vehicles or other transportation means, such as ATM machines, airplane cockpits, cargo containers, cruise ships, and the like. In these applications, detection of motion by a motion sensor 424 may be a requirement of a trusted environment definition, or a factor that leads to (or mandates) a non-trusted environment determination. Additionally, the trusted environment definition 414 may require that motion sensed by a motion sensor 424 match or otherwise correspond with a motion profile stored in the memory 404 and/or received from another device (e.g. a mobile device 108 or a wearable device 104). Comparing motion profiles (as measured by, for example, a motion sensor 424 and a motion sensor 224) may be used to determine whether the reader 412 is in an expected environment (e.g. one in which a certain motion pattern is expected, such as the rocking motion of a ship) or is in the same environment as a mobile device 108 or wearable device 104 that seeks access through the reader 412.

[0094] The one or more sensors 424 may also be or include a location sensor. The location sensor may be configured to determine a geographical location and/or position of the reader 412. In one embodiment, this location may be based on Global Positioning System (GPS) data provided by a GPS module of the reader 412. In some embodiments, the location of the reader 412 may be provided or determined based on cell tower data, WiFi information, iBeacon information, and/or some other location information sensed by the one or more sensors 424 of the reader 412. Although location information may not always be available inside buildings or other structures, location information provided by the one or more sensors 424 may be used, where available, as part of the trusted environment determination and/or to satisfy one or both of the first and second sets of access control requirements 408 and 410.

[0095] The device interface 428 may correspond to the hardware that facilitates communications between the reader 412 and one or more mobile devices 108 or wearable devices 104. The device interface 428 may include a Bluetooth interface (e.g., antenna and associated circuitry), a Wi-Fi/802.11N interface (e.g., an antenna and associated circuitry), an

NFC interface (e.g., an antenna and associated circuitry), an Infrared interface (e.g., LED, photodiode, and associated circuitry), and/or an Ultrasonic interface (e.g., speaker, microphone, and associated circuitry). In some embodiments, the device interface 428 is specifically provided to facilitate proximity-based communications with a credential via a communication channel or multiple communication channels.

[0096] As with other components of the reader 412, the device interface 428 may be used to gather information needed to make a trusted environment determination (e.g. to determine whether the trusted environment definition 414 is satisfied at a particular point in time) and/or to gather information required to meet the first or second sets of access control requirements 408 and 410. For example, the trusted environment definition may include a requirement that multiple recognized mobile devices 108 and/or 104 be communicating with the reader 412 via the device interface 428. Alternatively, the first set of access requirements 408 may require that both a primary mobile device (e.g. a mobile device 108) and a secondary mobile device (e.g. a wearable device 104) provide one or more credentials to the reader 412 via the device interface 428.

[0097] The network interface 432 may comprise hardware that facilitates communications with other devices over a communication network such as the communication network 128. The reader 412 may, for example, maintain communications with an access server such as access server 120, with other readers like reader 412, and/or with one or more services or data sources accessible via the communication network 128 (e.g. a web-based clock service, a remote memory such as access data memory 132, and so forth). As mentioned above, the network interface 432 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 432 may further be configured to encode and decode communications (e.g., packets) according to a protocol utilized by the communication network 128, and/or to encrypt or decrypt secure communications.

[0098] The network interface 432 may also be used to gather information necessary to make a trusted environment determination, and/or to satisfy one or more requirements of the first or second sets of access requirements 408 and 410. For example, the trusted environment definition 414 may include a requirement that the reader 412 have Internet access via the network interface 432 (e.g. so that the reader 412 can maintain up-to-date authorization information, which may include, without limitation, lists of authorized users, or lists of blacklisted users). Additionally or alternatively, the first or second set of access

control requirements 408 or 410 may require that information obtained from one or more mobile devices 108 and/or 104 be compared with information obtained on demand from an access server such as the access server 120 via the network interface 432.

[0099] The power module 436 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 reader 412. In some embodiments, the power module 436 may also include some implementation of surge protection circuitry to protect the components of the mobile device 436 from power surges.

[0100] Although in some embodiments one or both of the two sets of access control requirements 408 and 410 is stored in a memory 404 of the reader 412, in other embodiments, one or both sets of access control requirements 408 and 410 may be stored in a device other than the memory 404, such as an access server 120 or an access data memory 116 or 118. The one or more sets of access control requirements 408 and 410 may then be communicated to (or accessed by) the reader 412 as necessary, whether indirectly (e.g. through a communication network 128) or directly.

[0101] As depicted in Fig. 4, the trusted environment definition 414, containing the particular characteristics of a trusted environment, may be stored in the reader 412 (and, more specifically, in the memory 404 of the reader 412). The memory 404 may store multiple trusted environment definitions 414, any one of which may be sufficient to cause the processor 416 of the reader 412 to apply the second set of access control requirements 410. The reader 412 may identify a trusted environment based on, for example, the wireless access point(s) with which the reader 412 is connected via the network interface 432; the cellular network towers with which the reader 412 can communicate via the network interface 432, or with which a mobile device 108 or 104 can communicate via a network interface 332 or a communications module 216, respectively, as reported to the reader 412 via the device interface 428; the Bluetooth device(s) with which the reader 412 can communicate via the device interface 428; the mobile devices 108 and/or 104 with which the reader 412 can communicate via the device interface 428; the other reader(s) with which the reader 412 can communicate, whether via the device interface 428 or the network interface 432; and the wireless networks from which the reader 412 receives SSID broadcasts via the network interface 432. The reader 412 may also identify a trusted environment based on information it receives from a mobile device 108 or 104 or from any other device to which it is connected via the device interface 428, including, e.g., other readers, a host computer (which may be,

for example, an access server such as the access server 120), or a reader control panel. Such information may correspond to the connected device's physical environment (e.g. sound, brightness, temperature, etc.); the connected device's electromagnetic environment (e.g. a measured cellular telephone signal strength, the wireless network(s) from which the connected device receives SSID broadcasts; the wireless network(s) to which the device is connected, etc.); and/or the connected device's location (e.g. as determined from GPS signals, multilateration, etc.). The foregoing information may be measured by one or more sensors on the connected device. Additionally, the reader 412 may receive, via the device interface 428, information about a connected device's own identifying characteristics (e.g. a serial number associated with the device, the device's IP address, settings, etc.), and may rely on such information in make a trusted environment determination. The information obtained from outside devices may be obtained over any type of connection or connection protocol supported by both the reader 412 and the outside device in question, including, e.g., a Weigand connection or a connection utilizing the Open Supervised Device Protocol (OSDP), as well as other connection or communication protocols identified herein and/or other known communication protocols.

[0102] In some embodiments, the memory 404 of a reader 412 may store instructions for execution by the processor 416 that, when executed by the processor 416, cause the processor 416 to apply the second set of access control requirements 410 (e.g. the set of access control requirements corresponding to a trusted environment) unless the processor 416 detects (based on information received via the various sensors 424 and interfaces 428 and 432 of the reader 412) one or more indicators that the trusted environment definition 414 is not satisfied, in which case the processor 416 applies the first set of access control requirements 408. Such indicators may include, for example, the inability of the reader 412 (through any appropriate component thereof) to connect to a known wireless network; the inability of the reader 412 (through any appropriate component thereof) to detect one or more specific wireless networks, or any wireless networks at all; the inability of the reader 412 (through any appropriate component thereof) to detect or communicate with another reader; detection of an unknown WiFi access point, Bluetooth device, or mobile device by the reader 412 (through any appropriate component thereof); the inability of the reader 412 (through any appropriate component thereof) to authenticate a mobile device; detection of a known mobile device with changed settings or a changed configuration by the reader 412 (through any appropriate

component thereof); detection by the reader 412 (through any appropriate component thereof) of a mobile device in a locked condition; and so forth.

[0103] With reference now to Figs. 5A and 5B, in accordance with some embodiments of the present disclosure, a user 502 holds a mobile device 508 in proximity to a reader 512 in an attempt to gain access to a resource protected by the reader 512. The user 502 also has a second mobile device, which is wearable device 504. In the illustrated embodiments, the mobile device 508 is configured to determine whether the environment is trusted, and to communicate that information to the access control reader 512. In these embodiments, the wearable device 504 may have the same or similar components as the wearable device 104. Likewise, the access control reader 512 may have the same or similar components as the reader 412 or the reader 112.

[0104] The mobile device 508 has many of the same components as the mobile device 108. Additionally, however, the mobile device 508 includes one or more sensors 526, to which the description of the one or more sensors 424 applies with equal force. The mobile device also includes in its memory 304 not just an operating system 308 and a key vault 312, but also a trusted environment definition 510, which may be the same as or similar to the trusted environment definition 414. Although not shown, the memory 534 may also store a first set of access control requirements (similar to the first set of access control requirements 408) and/or a second set of access control requirements (similar to the second set of access control requirements 410). Still further, the mobile device 508 may include, in some embodiments, a control module 530, which is described in greater detail below.

[0105] As with other embodiments, the characteristics of a trusted environment (or, in other words, the particulars of the trusted environment definition 510) in the embodiments represented by Figs. 5A and 5B may be tailored to a particular protected resource, and may reflect one or more of the security needs and challenges associated with the protected resource, the culture of the entity that owns and/or uses the protected resource, and the types of credentials and credential devices held by authorized users of the protected resource. The trusted environment definition 510 may include one or more indicators that may be identified by the mobile device 508 (and, more specifically, by the processor 316 of the mobile device 508). Such indicators may include any one or more of the factors discussed above. Additionally or alternatively, indicators of a trusted environment may include any one or more of the following: whether the mobile device 508 is in relatively close proximity (e.g. on the same person) to the second mobile device 504 (as determined using, for example, RSSI or

time of flight information, or by evaluating whether communications between the mobile device 508 and the second mobile device 504 can be established using a short range communication protocol such as NFC or RFID); whether measurements by the sensors 526 on the mobile device 508 and/or by one or more sensors on the second mobile device 504 of one or more environmental characteristics (e.g. of temperature, sound, motion, brightness, air quality, etc.) are consistent with being on the same person and/or in close proximity to each other; whether the location of the mobile device 508, as determined using GPS, multilateration, or other locating signals or techniques (where needed signals are received by the one or more sensors 526 and/or the device interface 328 and/or the network interface 332, and the signals are analyzed by the processor 316) is the same or approximately the same as the location of a second mobile device 504; and so forth. The information used to make the trusted environment determination may be gathered during the determination process, or it may be or include information stored by one or both mobile devices 508 and 504 in a given time period preceding the trusted environment determination. For example, if the mobile device 508 and the second mobile device 504 each have an accelerometer capable of measuring or counting steps, then the mobile device 508 may compare data recorded by both devices 508 and 504 over the preceding minute, five minutes, or other time interval. If the recorded data match (e.g. in number of steps, timing of steps, etc.), then the comparison may satisfy a trusted environment requirement.

[0106] Once the mobile device 508 determines that it is in a trusted environment, it communicates the determination to the reader 512, which then applies the trusted environment access control requirements (e.g. the second set of access requirements 410). Alternatively, the mobile device 508 may determine, and communicate to the reader 512, that it is not in a trusted environment, such that the reader 512 applies the non-trusted environment access control requirements (e.g. the first set of access requirements 408). A determination that the mobile device 508 is in a non-trusted environment may be based on one or more factors similar to those discussed above, where the factor in question suggests that an unauthorized user may be in control of the mobile device 508. For example, if the sensors 526 on the mobile device 508 and one or more additional sensors on the second mobile device 504 measure values for a given environmental characteristic that differ by more than a threshold amount, then the two mobile devices 508 and 504 are likely not in the possession of the same individual. The same conclusion may be drawn, for example, if the mobile device 508 recognizes different wireless networks than the second mobile device 504,

or if the mobile device 508 cannot communicate with or at least discover a known second mobile device 504 at all.

[0107] As noted above, in some embodiments of the present disclosure, the mobile device 508 has a control module 530 comprising the processor 316 and configured to determine whether the environment is trusted, and to control certain device functions or behaviors based on that determination, using the processor 316. For example, once the mobile device 508 determines that it is in a trusted environment, the control module 530 may allow one or more mobile keys from the key vault 312 to be communicated to another device (e.g. a reader 512). On the other hand, once the mobile device 508 determines that it is not in a trusted environment, the control module 530 may prohibit the communication of the one or more mobile keys to another device (including, e.g., the reader 512), or disable the one or more mobile keys. As another example, in a trusted environment, the control module 530 may reduce encryption requirements (or remove them altogether) for access control-related functions, while in a non-trusted environment, the control module 530 may require the use of encryption, or of more stringent encryption. In a trusted environment, the control module 530 may enable or delay the expiration of a mobile key for a greater period of time than in a non-trusted environment, or enable a mobile key (or allow the transmission of a mobile key) without requiring that a user 502 unlock the mobile device 508. In some embodiments, the mobile device 508 receives one or more sets of access control requirements corresponding to one or more potential trusted environment determinations from the reader 512 or from another device (e.g. an access server such as access server 120, a host computer, or a control panel), directly or indirectly, and the control module 530 applies the appropriate set of access control requirements based on the trusted environment determination. Although shown as a separate component, the control module 530 may comprise, in some embodiments, instructions stored in the memory 304 and executed by the processor 316. In other embodiments, however, the control module 530 may have a dedicated processor and dedicated memory, and may be protected by a firewall, by physical or electronic switches, by limited physical connections to other components of the mobile device 508, or by other means to minimize the likelihood that someone will obtain unauthorized access to the one or more credentials stored in the key vault 312.

[0108] Illustrative implementations of embodiments of an access control system according to the present disclosure will now be discussed, with continuing reference first to Fig. 6A, in which a user 602 presents a mobile device 608 to a reader 612 to initiate an access attempt.

The reader 612 has at least the same components as the reader 412. Thus, the reader 612 may be capable of storing a trusted environment definition 414 in a memory 404 thereof, together with two sets of access requirements—a first set 408 for use in a non-trusted environment, and a second set 410 for use in a trusted environment. Among the sensors 424 of the reader 612 is a biometric sensor 424a in the form of a retina scanner. The first set of access requirements 408 allows access only after receiving an authorized mobile key from an unlocked mobile device 608 and only after confirming that a retina scan of the user 602 matches the known holder of the key. In a trusted environment, however, the reader 612 is configured to grant access upon receipt of an authorized mobile key. In this implementation, a trusted environment is defined to exist when the reader 612 is in communication with two mobile devices (e.g. the mobile devices 604 and 608) belonging to a user (e.g. the user 602) (or with one mobile device belonging to a user (e.g. mobile device 608 of the user 602), which can confirm to the reader 612 that a second mobile device belonging to the user (e.g. wearable device 604 of the user 602) is in close proximity to the first mobile device), and when at least one of the two mobile devices (e.g. one of mobile device 608 and wearable device 604) has been in communication with the reader 612 during the preceding twelve hours. Thus, if the trusted environment definition is satisfied, the user 602 need not unlock his or her mobile device 608, and need not submit to a retina scan from scanner 424a, thus reducing the inconvenience to the user 602 and the effort required from the user 602. At the same time, the existence of a trusted environment provides a high degree of confidence that the holder of the mobile devices (here, the user 602) is an authorized user, because, for example, the system administrator may determine that it is unlikely that someone would successfully steal both mobile devices 608 and 604 from their true owner (the authorized user), and that it is even more unlikely that someone would successfully steal both mobile devices 608 and 604 and then present them to the reader 612 within less than twelve hours.

[0109] Referring now to Fig. 6B, in the same implementation, a trusted environment may also exist when the reader 612 is in communication with three or more mobile devices (e.g. the mobile devices 608a, 608b, and 608c) storing authorized credentials for different authorized users (e.g. the users 602a, 602b, and 602c). When such a trusted environment exists, the second set of access requirements 410 can be applied without significantly affecting security because, for example, the system administrator (who determines the trusted environment definition and the corresponding access requirements) may determine that it is unlikely that more than one of the credentials 608a, 608b, and 608c would be in the

possession of an unauthorized user, and that it is even more unlikely that an unauthorized user would attempt to access the protected resource when other persons are present. To the extent such an attempt was made, the burden would shift from the access control system to the authorized users 602a, 602b, and/or 602c to identify the unauthorized user and prevent the unauthorized user from accessing the protected resource. (Consequently, this particular trusted environment definition and related access control requirements would be best suited for smaller organizations (or for subsets of large organizations) where authorized users are likely to recognize one another.)

[0110] Referring now to Fig. 7, in another implementation, an access control system protects an office 700, which is divided into a plurality of rooms or zones 703a-n, each protected by a reader 712a-n having different access control requirements. Visitors to the office 700 may need to meet with individuals in a subset of the plurality of protected rooms or zones 703a-n, e.g. rooms 703b, 703c, and 703n. So, a visitor's mobile device may be authorized as a credential for rooms 703b, 703c, and 703n by loading the appropriate mobile keys therein. The mobile keys may be tied to a trusted environment definition, such that as long as the visitor's mobile device is within the trusted environment, the mobile keys remain valid. However, once the visitor's mobile device is no longer in a trusted environment, the mobile keys are either temporarily or permanently disabled. The trusted environment definition in this implementation may require that the visitor's mobile device be in communication with one or more wireless access points 706a-n in the office building, that the visitor's mobile device be in communication range of a plurality of known access control readers 712a-n, that the visitor's mobile device sense a temperature within a certain temperature range that corresponds to the temperature range inside the office (e.g. as measured by a thermometer in one or more access control readers 712a-n or wireless access points 706a-n, that the visitor's mobile device sense the same sounds as a microphone on one or more readers 712a-n in the office; and/or any other such requirement or combination thereof. In this implementation, once the visitor's mobile device leaves the office 700 (and therefore leaves the trusted environment), the mobile keys to the office 700 may no longer be used.

[0111] In other embodiments of the present disclosure, a mobile device or reader may be configured to identify multiple levels of trusted and/or non-trusted environments, and each level may be associated with a specific set of access control requirements. The access control requirements associated with a given trusted environment may include those requirements

that verify a particular piece of information that is not verified (or that is not sufficiently verified) by the trusted environment determination.

[0112] With respect to Fig. 8, an access control system according to embodiments of the present disclosure may comprise an access server 820 (which may be the same as or similar to the access server 120). The access server 820 may include a policy engine 804, a processor 816, one or more drivers 822, a user interface 824, a reader interface 828, a network interface 832, and, in embodiments, a power module 836.

[0113] Although Fig. 8 depicts the policy engine 804 as a component of an access server 820, the policy engine 804 may be hosted on a mobile device, a laptop, another server, or any other device. The policy engine host (here, access server 820) is in wired or wireless communication with at least one of a reader (e.g. a reader 112, 412, 512, 612, or 712) and/or a mobile device (e.g. a mobile device 108, 508, 608, 104, 504, or 604) of the access control system, via the reader interface 828 and/or the network interface 832. Working through the user interface 824, a system administrator may use the policy engine 804 to manage the trusted environment definition(s) 808 and related access control requirements 814 on the reader(s) in the access control system. The system administrator may manually create or modify trusted environment definitions and related access control requirements, or the policy engine 804 may create or manage the same automatically, based on criteria defined by the system administrator. For example, the policy engine 804 may have a list 812 of trusted environment indicia, which may be organized into groups based on whether they provide a strong indication of a trusted environment, a weak indication of a trusted environment, or something in between. The system administrator may then select specific indicia to incorporate into a trusted environment definition 808, or the system administrator may simply specific that the trusted environment definition 808 should be strong, thus leaving the policy engine 804 (upon execution by the processor 816) to select an appropriate number of strong trusted environment indicia to incorporate into the trusted environment definition 808.

[0114] Additionally, the policy engine 804 may be configured, for example, to gather information about the environment in which access control decisions are made from one or more readers and/or mobile devices, and to then use that information to identify characteristics of a trusted environment (e.g. characteristics that are present when an access request is granted but not when an access request is denied). The policy engine 804 may be further configured to create sets of access control requirements corresponding to one or more trusted environments. In particular, the policy engine 804 may be configured to remove an

access control requirement intended to verify that an authorized user has or knows something if the trusted environment determination already confirms (albeit perhaps in a different way) that the authorized user has or knows the thing in question.

[0115] The remaining components of the access server 820 are similar to or the same as their counterparts in the mobile devices 108 or 508 and/or the reader 412. For example, the processor 816, like the processors 316 and 416, may correspond to one or many microprocessors that are contained within the housing of the access server 820. In some embodiments, the processor 816 incorporates the functions of a Central Processing Unit (CPU) on a single Integrated Circuit (IC) or a few IC chips. The processor 816 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 816 implements sequential digital logic as it has internal memory. As with most known microprocessors, the processor 816 may operate on numbers and symbols represented in the binary numeral system.

[0116] The driver(s) 822 may correspond to hardware, software, and/or controllers that provide specific instructions to hardware components of the access server 820, thereby facilitating their operation. For instance, the user interface 824, reader interface 828, and network interface 832 may each have a dedicated driver 822 that provides appropriate control signals to effect their operation. The driver(s) 822 may also comprise the software or logic circuits that ensure the various hardware components are controlled appropriately and in accordance with desired protocols. For example, the driver 822 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 832 can exchange communications via the communication network 128. As can be appreciated, the driver(s) 822 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0117] The user interface 824 may comprise one or more user input devices and/or one or more user output devices, just like the user interface 324.

[0118] The reader interface 828 may correspond to the hardware and/or software that facilitates communications between the access server 820 and the various readers of the access control system of which the access server 820 is a part. Such communications may

use a proprietary communication protocol or any of the standard communication protocols identified herein.

[0119] The network interface 832 may comprise hardware and/or software that facilitates communications with other communication devices over the communication network 128, just like the user interface 332. Also, the power module 336 may include a built-in power supply (e.g., a 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 access server 820, similarly to the power module 336.

[0120] The present disclosure also includes methods for identifying a trusted environment and utilizing that identification. Turning now to Fig. 9, a method 900 according to embodiments of the present disclosure begins at step 904, which may correspond with the receipt by a reader (for purposes of illustration, a reader 612) of a signal from a mobile device (for purposes, again, of illustration, a mobile device 608) indicating that the mobile device 608 (or a user 602 thereof) would like to obtain access to a resource protected by the reader 612. Alternatively the method 900 may begin upon an indication to the reader 612 (or more specifically, to a processor thereof) that a mobile device 608 or a user 602 would like to gain access to the protected resource.

[0121] The reader 612 then gathers information about the environment from one or more available sources (step 908). Such sources may include, for example but without limitation, one or more sensors on the reader 612; one or more interfaces on the reader 612 (which may, for example, receive signals indicative of the environment of the reader 612, including Wi-Fi radio signals, cellular radio signals, commercial radio signals, and the like); and one or more external devices in communication with the reader 612 via the one or more interfaces of the reader 612 (including, for example, one or more mobile devices, an access control server 120, and other such devices). The reader 612 may store the gathered environmental information in a memory thereof, and may use the gathered environmental information to populate a database in the memory or in a memory accessible to the reader 612 via a communication network 128.

[0122] The reader 612 compares the gathered environmental information with a trusted environment definition (step 912). The trusted environment definition may be stored in a memory of the reader 612, or it may be obtained from a memory accessible to the reader 612 via a communication network 128, or it may be provided by another device, such as an access server 120, in communication with the reader 612. In some embodiments, the comparison

may include a simple determination of whether each aspect of the trusted environment definition has been satisfied. In other embodiments, the comparison may include a calculation of the difference between one or more aspects of the trusted environment definition and one or more measured aspects of the environment. For example, if one aspect of the trusted environment definition is that the temperature be 68° F, the reader 612 (or more specifically, the processor of the reader 612) may calculate the difference between the measured temperature and the defined temperature of 68° F. The calculated difference can then be used to determine whether the measured value is within an acceptable range of the defined value. (In embodiments, the trusted environment definition includes a tolerance associated with one or more aspects thereof, which defines the range of measured values that will still satisfy the trusted environment requirement).

[0123] Based on the comparison of the measured environment values and the trusted environment definition, the reader 612 determines whether a trusted environment exists (step 916). This determination may involve a simple determination of whether every aspect of the trusted environment definition has been satisfied, or, for more complex trusted environment definitions, it may involve a determination of a minimum number of requirements within the trusted environment definition were satisfied, and/or whether one of several alternative requirements within the trusted environment definition was satisfied. For example, the trusted environment definition may include 10 requirements, but specify that a trusted environment exists if any 5 of those requirements are satisfied.

[0124] Once a trusted environment determination is made, the reader 612 can select a set of access requirements that corresponds to the determined environment (whether trusted or non-trusted) (step 920). In embodiments, the reader 612 selects between a first predetermined set of access requirements to be used when the environment is not trusted, and a second predetermined set of access requirements to be used when the environment is trusted. In other embodiments, the reader 612 selects specific access requirements from among a plurality of predetermined access requirements based on which aspects of the trusted environment definition were met and which were not. For example, if the reader 612 determined that a trusted environment definition was not met because a second mobile device 604 (e.g. a wearable device) was not determined to be in close proximity to the mobile device 608 and/or the reader 612 (or was not detected by the reader 612 at all), then the reader 612 may select an access requirement that requires a mobile key to be sent from the mobile device 608 of the user 602 only after the user 602 has unlocked the mobile device 608. Thus, while

the identity of the user 602 could not be confirmed by detecting the presence of two mobile devices belonging to the user (e.g. the mobile device 608 and the mobile device 604), the identity of the user 602 is instead confirmed by requiring the user 602 to unlock the mobile device 608—something that only the user 602 should be able to do.

[0125] The reader 612 next gathers access information (step 924). The access information may be gathered solely from the mobile device 608, and may comprise a mobile key or other credential. The access information may also include, for example, a biometric scan of a fingerprint, retina, face, or other distinguishing feature of the user 602, e.g. using a biometric sensor on the reader 612.

[0126] Once the reader has gathered the access information, the reader 612 compares the access information to the selected set of access requirements (step 928). This may involve, for example, determining whether a mobile key or other credential received from the mobile device 608 is authorized (e.g. by comparing the mobile key to a stored key, or determining whether the mobile key is on a list of authorized mobile keys, or inputting the mobile key to an algorithm and determining whether the output of the algorithm matches a stored output. This may also involve, for example, determining whether scanned biometric information matches stored biometric information and other such comparisons. In embodiments, the reader 612 may receive information such as a list of authorized mobile keys, stored biometric information, and the like from an external source such as an access data memory 116, an access data memory 132, and/or an access server 120 or 820.

[0127] After comparing the access information obtained by the reader 612 with the selected set of access requirements, the reader 612 makes an access determination (step 932). If the access determination is to grant access, the reader 612 may, for example, send an unlock signal to a lock mechanism, automatically open a door, provide an access granted indication, or deactivate an alarm. If the access determination is to deny access, the reader 612 may do nothing, may provide an access denied indication, or may activate an alarm. Once the access determination has been made, the method 900 terminates (step 936).

[0128] In a method 1000 according to another embodiment of the present disclosure, illustrated in Fig. 10, a mobile device such as the mobile device 508 may make the trusted environment determination. The method 1000 begins at step 1004, which may correspond or otherwise coincide with the initiation of an access attempt by the mobile device 508 (whether at the direction of a user 502 of the mobile device 508 or automatically).

[0129] In the method 1000, the mobile device 508 gathers environment information from one or more available sources (step 1008). Such sources may include, for example but without limitation, one or more sensors on the mobile device 508 (including, for example, motion sensors, location sensors, lighting sensors, biometric sensors, temperature sensors, audio sensors, humidity sensors, pressure sensors, and the like); one or more interfaces on the mobile device 508 (which may, for example, receive signals indicative of the electromagnetic environment of the mobile device 508, including Wi-Fi radio signals, cellular radio signals, commercial radio signals, and the like); and one or more external devices in communication with the mobile device 508 via the one or more interfaces of the mobile device 508 (including, for example, a wearable mobile device 504 or other mobile devices, a reader 512, and other such devices). The gathered environmental information may correspond to an environmental characteristic, such as a temperature, pressure, noise level, noise profile, lighting level, electromagnetic signal availability, and so forth. The mobile device 508 may store the gathered environmental information in a memory thereof, and may use the gathered environmental information to populate a database in that memory.

[0130] The mobile device 508 compares the gathered environmental information with a trusted environment definition (step 1012). The trusted environment definition may be stored in a memory of the mobile device 508, or it may be stored in and obtained from a memory or other device accessible to the mobile device 508 via a connection with the reader 512 or via a communication network such as the communication network 128. The comparison of the gathered environmental information with the trusted environment definition may involve the same kinds of determinations discussed above with respect to step 912 of the method 900.

[0131] Based on the comparison of the measured or obtained environmental information and the trusted environment definition, the mobile device 508 determines whether a trusted environment currently exists (step 1016). Again, this determination may involve the same aspects as those discussed above with respect to step 916 of the method 900.

[0132] Once a trusted environment determination has been made, the mobile device 508 selectively transmits the contents of a key vault of the memory thereof to the reader 512 based on the determination (step 1020). Thus, if a trusted environment is determined to currently exist, then the mobile device 508 may transmit a mobile key stored in the key vault of its memory to the reader 512. If a trusted environment is determined not to currently exist, then the mobile device 508 may not transmit its mobile key or other credentials to the reader 512. The mobile device 508 may also selectively disable any communications with the key

vault of the mobile device 508 if a trusted environment does not currently exist, so as to protect the contents thereof. In other embodiments, the mobile device may transmit credentials from its key vault to the reader 512 in the absence of a current trusted environment, but only after taking one or more precautions, such as establishing a secure communication channel with the reader 512. The method 1000 terminates once step 1020 is complete (step 1036).

[0133] The exemplary systems and methods of this disclosure have been described in relation to mobile and 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.

[0134] 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.

[0135] 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.

[0136] 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.

[0137] 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.

[0138] 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.

[0139] 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.

[0140] 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.

[0141] 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.

[0142] 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.

[0143] 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.

[0144] 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.

[0145] Any of the steps, functions, and operations discussed herein can be performed continuously and automatically.

[0146] 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 reader, comprising:

a processor;

a communication interface; and

a memory storing instructions that, when executed by the processor, cause the processor to:

obtain information about an environment surrounding the reader;

compare the information about the environment with a trusted environment definition; and

select, based on the comparison, one of a first and a second set of access control requirements for use in making an access determination.

2. The access control reader of claim 1, wherein the information about the environment surrounding the reader includes at least one of: information about a physical environment of the reader; information about an electromagnetic environment of the reader; and information about a location of the reader.

3. The access control reader of claim 2, wherein the information about the physical environment of the reader includes at least one of: temperature information, lighting information, audio information, and humidity information.

4. The access control reader of claim 2, wherein the information about the electromagnetic environment of the reader includes at least one of: information about a wireless network from which the reader receives a wireless signal; information about a cellular network tower from which the reader receives a wireless signal; and information about a mobile device from which the reader receives a wireless signal.

5. The access control reader of claim 1, wherein the information about the environment surrounding the reader includes at least one of: information about a detected mobile device's physical environment; information about the detected mobile device's electromagnetic environment; information about the detected mobile device's location; and identifying characteristics of the detected mobile device.

6. The access control reader of claim 1, wherein the information about the environment surrounding the reader is obtained from one or more sensors on the reader.

7. The access control reader of claim 1, wherein the first set of access control requirements corresponds to a trusted environment.

8. The access control reader of claim 1, wherein the first set of access control requirements is a subset of the second set of access control requirements.

9. The access control reader of claim 1, wherein the information about the environment surrounding the reader corresponds to at least one of: an inability to connect to a known wireless network; an inability to detect a specific wireless network; an inability to detect any wireless networks; an inability to communicate with another device; an inability to detect a specific device; the reader's detection of an unknown device; a detection of a known mobile device having one or more settings that do not match one or more predetermined settings; and a detection of a mobile device in a locked condition.

10. The access control reader of claim 1, wherein at least one of the first and second sets of access control requirements is stored on a device other than the reader.

11. The access control reader of claim 10, wherein the device is an external memory, a host computer, or a control panel.

12. An access control system, comprising:

a processor;

a communication interface; and

a computer readable memory storing:

a trusted environment definition that comprises information about one or more characteristics of a trusted environment;

a primary set of access control requirements and a secondary set of access control requirements; and

access control instructions that cause the processor to:

obtain at least one current environmental characteristic;

selectively apply the primary set of access control requirements or the secondary set of access control requirements based on whether the at least one current environmental characteristic corresponds to a trusted environment definition;

receive a credential from a mobile device via the communication interface; and

make an access determination based on the credential and the selectively applied primary set of access control requirements or secondary set of access control requirements.

13. The access control system of claim 12, wherein a reader receives the current environmental characteristic from the mobile device.

14. The access control system of claim 12, wherein the primary set of access control requirements comprises fewer requirements than the secondary set of access control requirements.

15. A method, comprising:

enabling an access control reader to communicate with a first and second mobile device;

based on environmental information received at the reader from the first and second mobile device, selecting whether to apply a first set of access control requirements or a second set of access control requirements; and

applying the selected first or second set of access control requirements at the reader with respect to making an access control decision for a holder of either the first or second mobile device.

16. The method of claim 15, further comprising:

determining, based on the environmental information, that a trusted environment exists; and

in response to determining that a trusted environment exists, selecting the first set of access control requirements.

17. The method of claim 16, wherein the trusted environment is determined to exist in response to receiving substantially similar environmental information from both the first mobile device and the second mobile device.

18. The method of claim 15, wherein the environmental information describes at least one of a temperature, sound profile, or light profile in proximity to the first mobile device and the second mobile device.

19. The method of claim 15, wherein the environmental information describes network information available to the first mobile device and the second mobile device.

20. The method of claim 15, wherein the environment information relates to at least one of a temperature, a noise level, a noise profile, a lighting level, an electromagnetic signal, and a wireless connection.

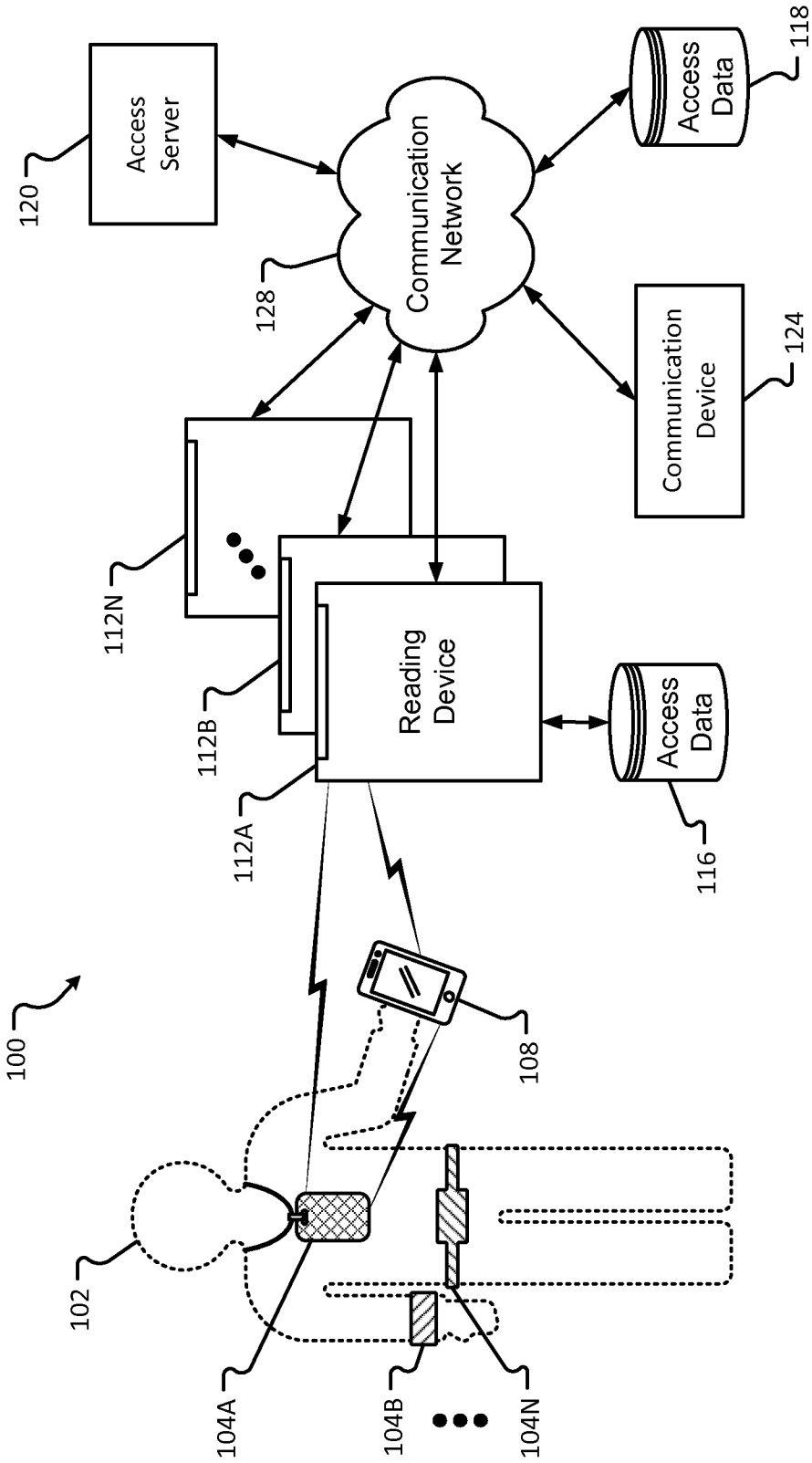

Access Server
120
Communication Network
128
Access Data
118
Communication Device
124
112N
112B
112A
Reading Device
Access Data
116
100
108
102
104A
104B
104N

Fig. 1

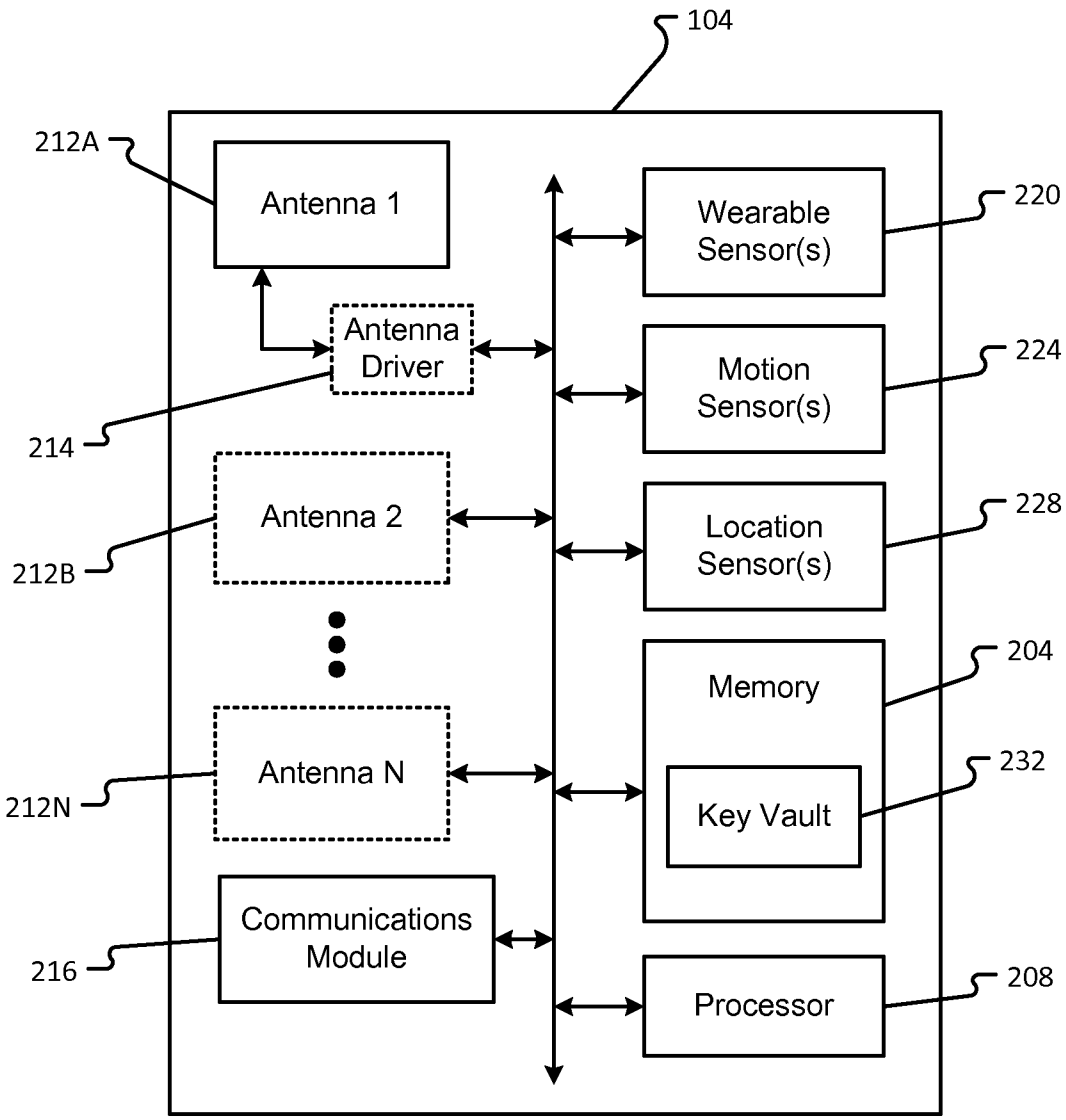

104
212A
Antenna 1
Antenna Driver
214
Antenna 2
212B
Antenna N
212N
Communications Module
216
Wearable Sensor(s)
220
Motion Sensor(s)
224
Location Sensor(s)
228
Memory
204
Key Vault
232
Processor
208

Fig. 2

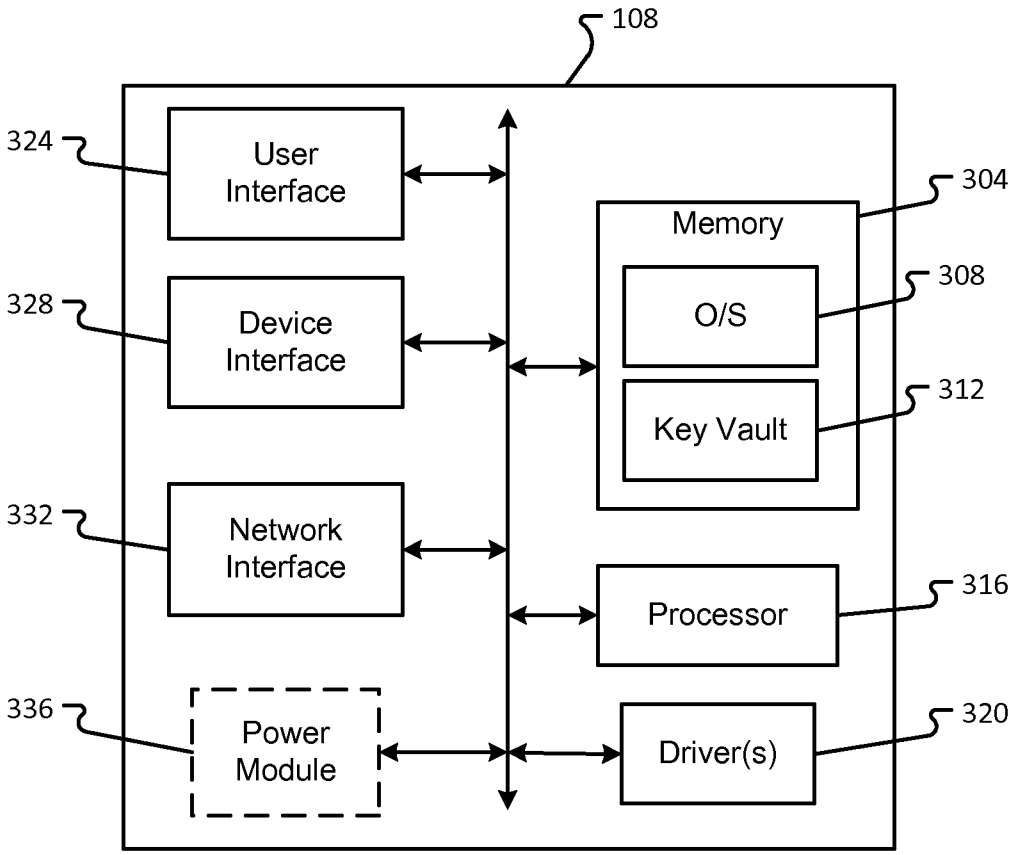

108
324
User Interface
328
Device Interface
332
Network Interface
336
Power Module
304
Memory
308
O/S
312
Key Vault
316
Processor
320
Driver(s)

Fig. 3

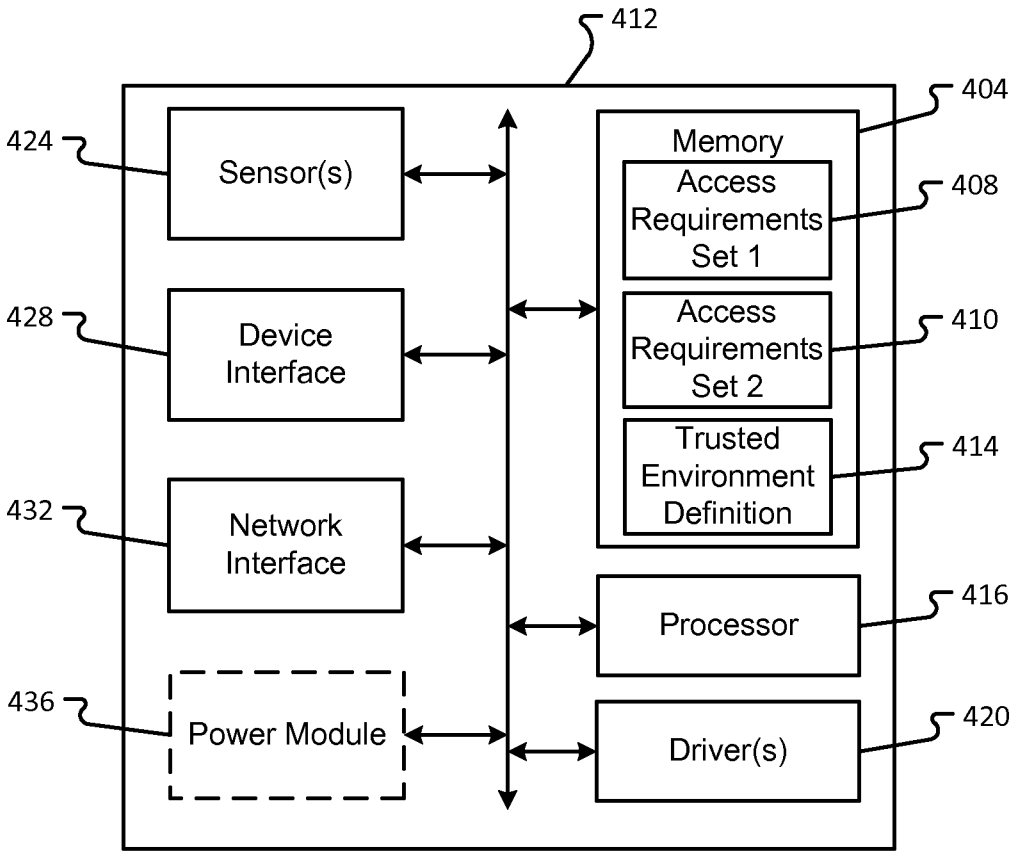

412
404
424
Sensor(s)
Memory
Access Requirements Set 1
408
428
Device Interface
Access Requirements Set 2
410
Trusted Environment Definition
414
432
Network Interface
Processor
416
436
Power Module
Driver(s)
420

Fig. 4

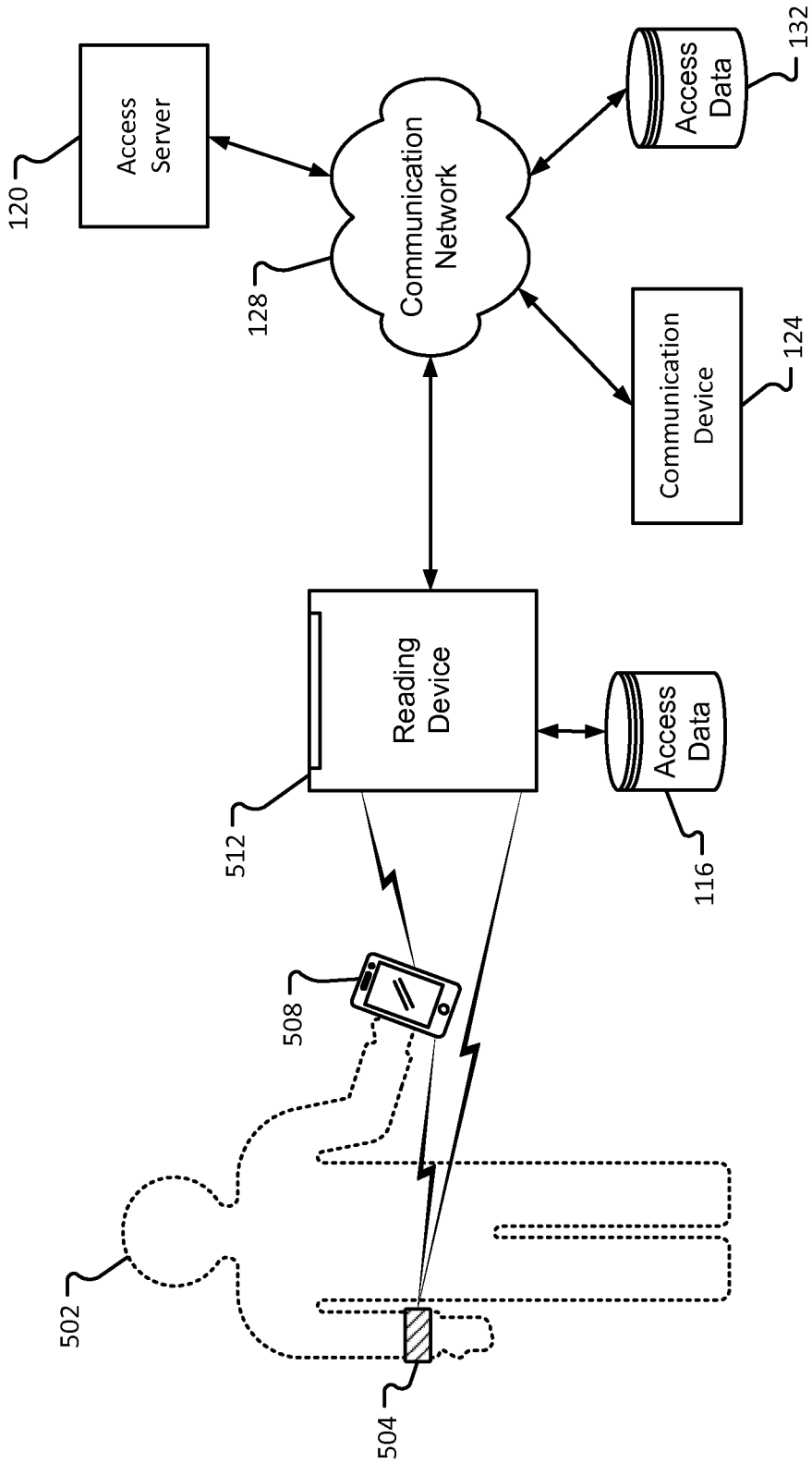

Access Server
120
Communication Network
128
Access Data
132
Communication Device
124
Reading Device
512
Access Data
116
508
502
504

Fig. 5A

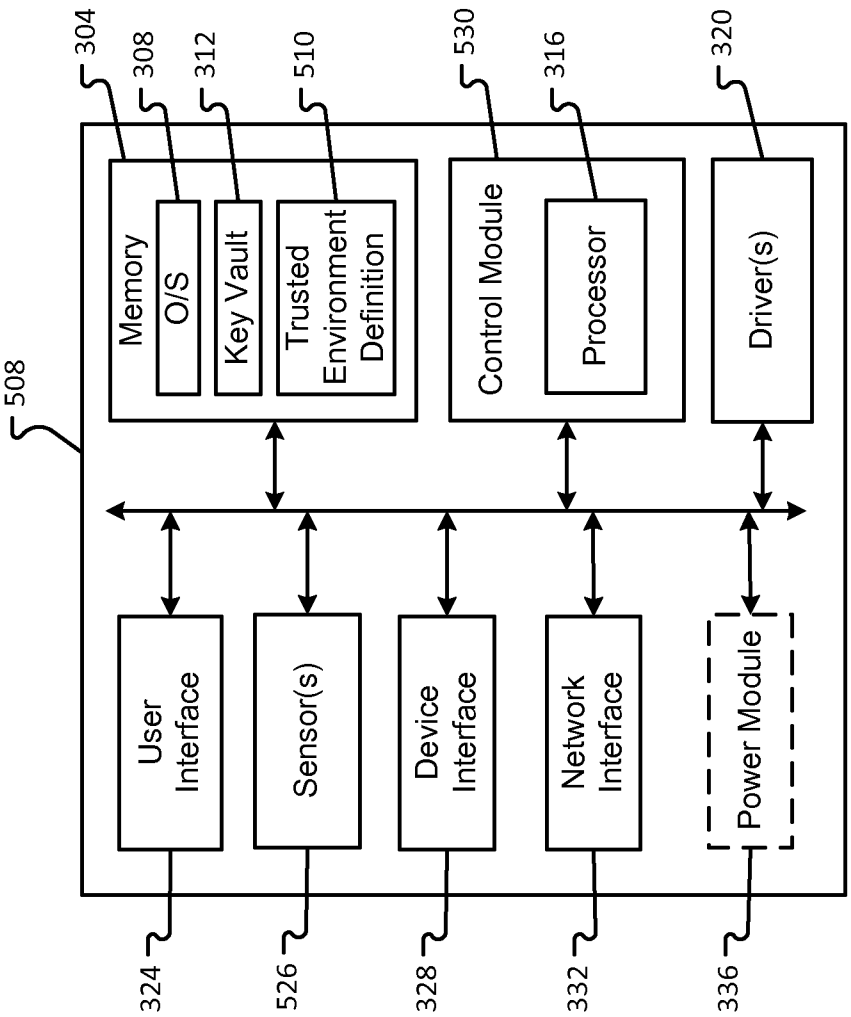

508
304
308
312
510
530
316
320
Memory
O/S
Key Vault
Trusted Environment Definition
Control Module
Processor
Driver(s)
User Interface
Sensor(s)
Device Interface
Network Interface
Power Module
324
526
328
332
336

Fig. 5B

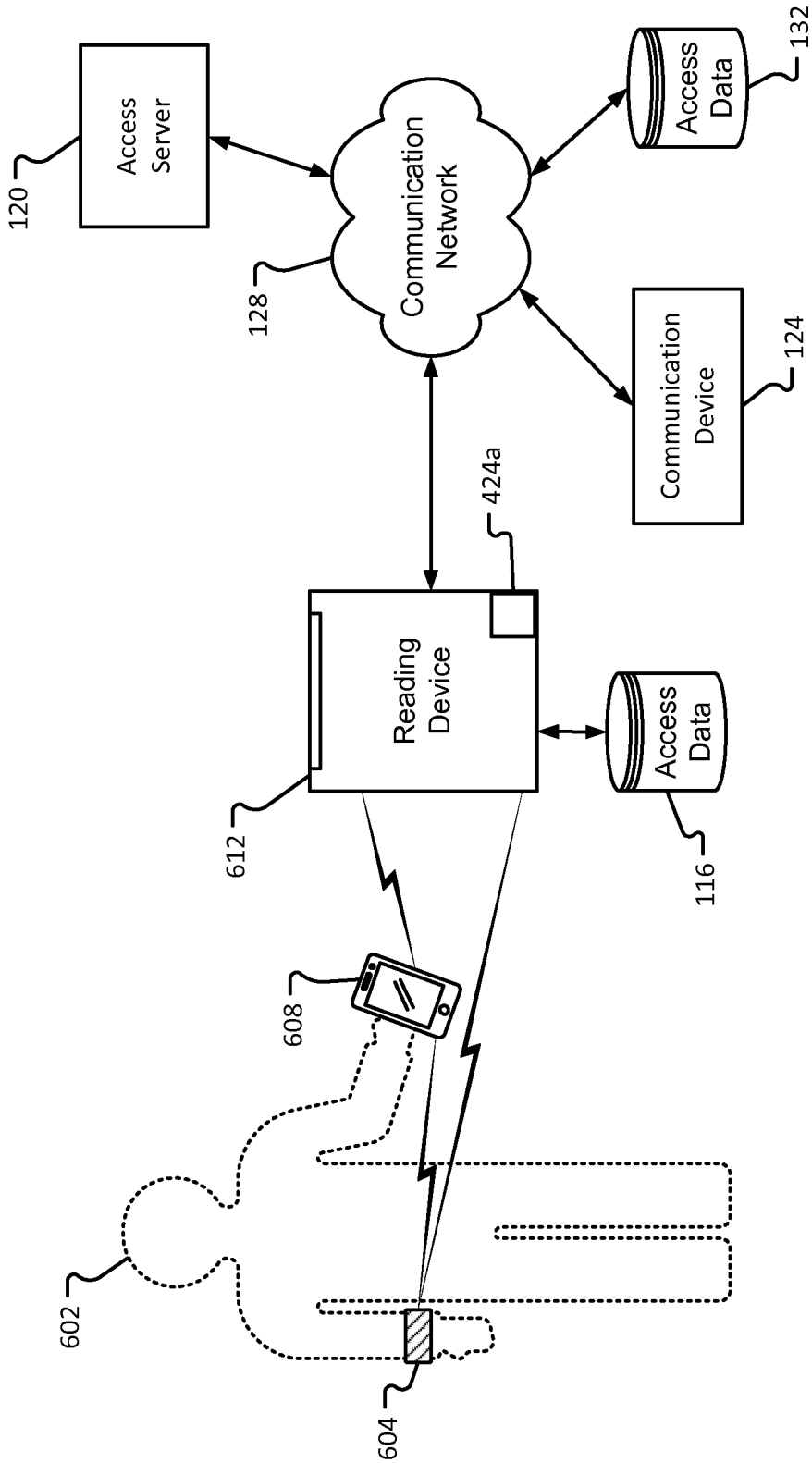

Access Server
120
Communication Network
128
Access Data
132
Communication Device
124
424a
Reading Device
612
Access Data
116
608
602
604

Fig. 6A

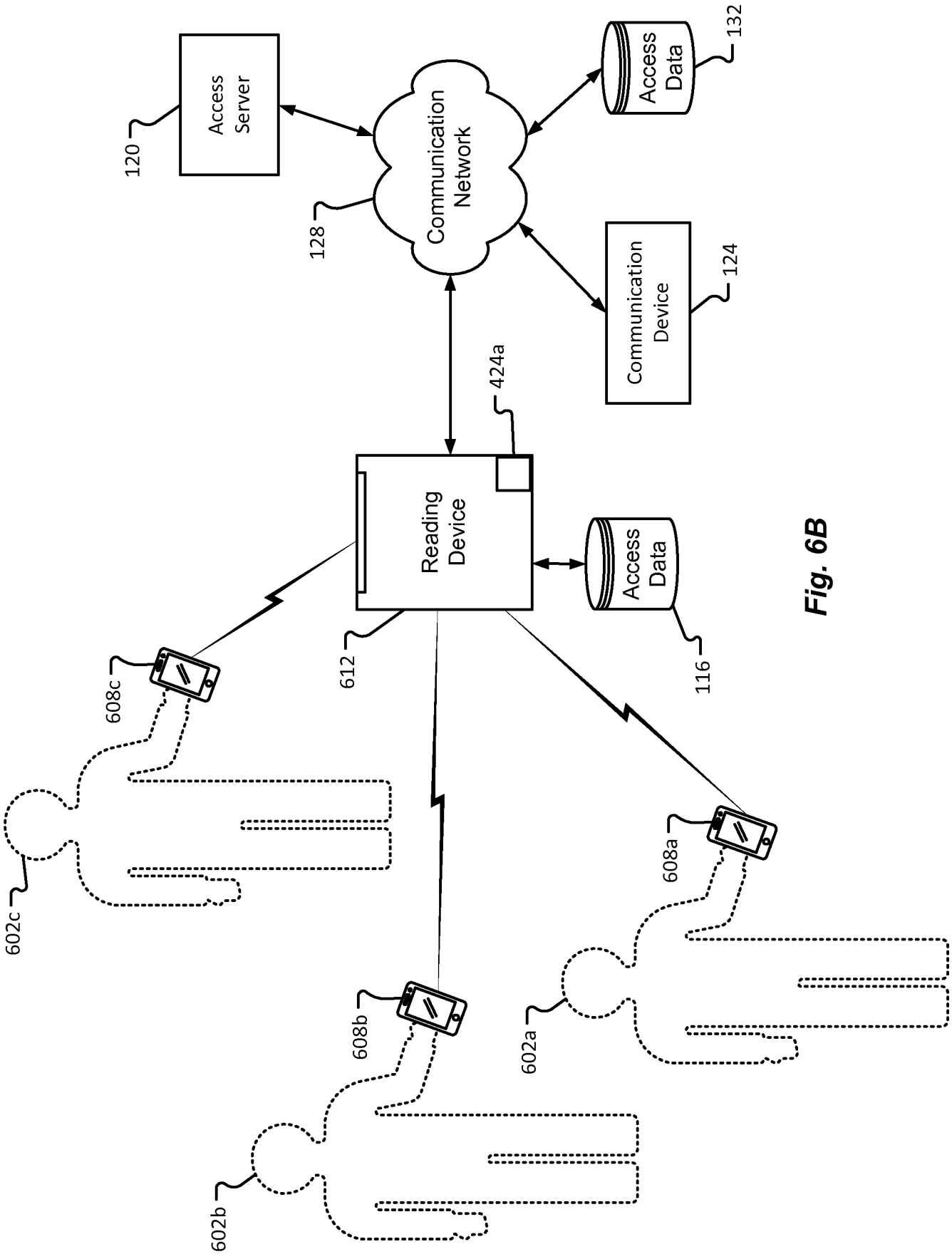

Access Server
120
Communication Network
128
Access Data
132
Communication Device
124
424a
Reading Device
612
Access Data
116
608c
602c
608b
602b
608a
602a

Fig. 6B

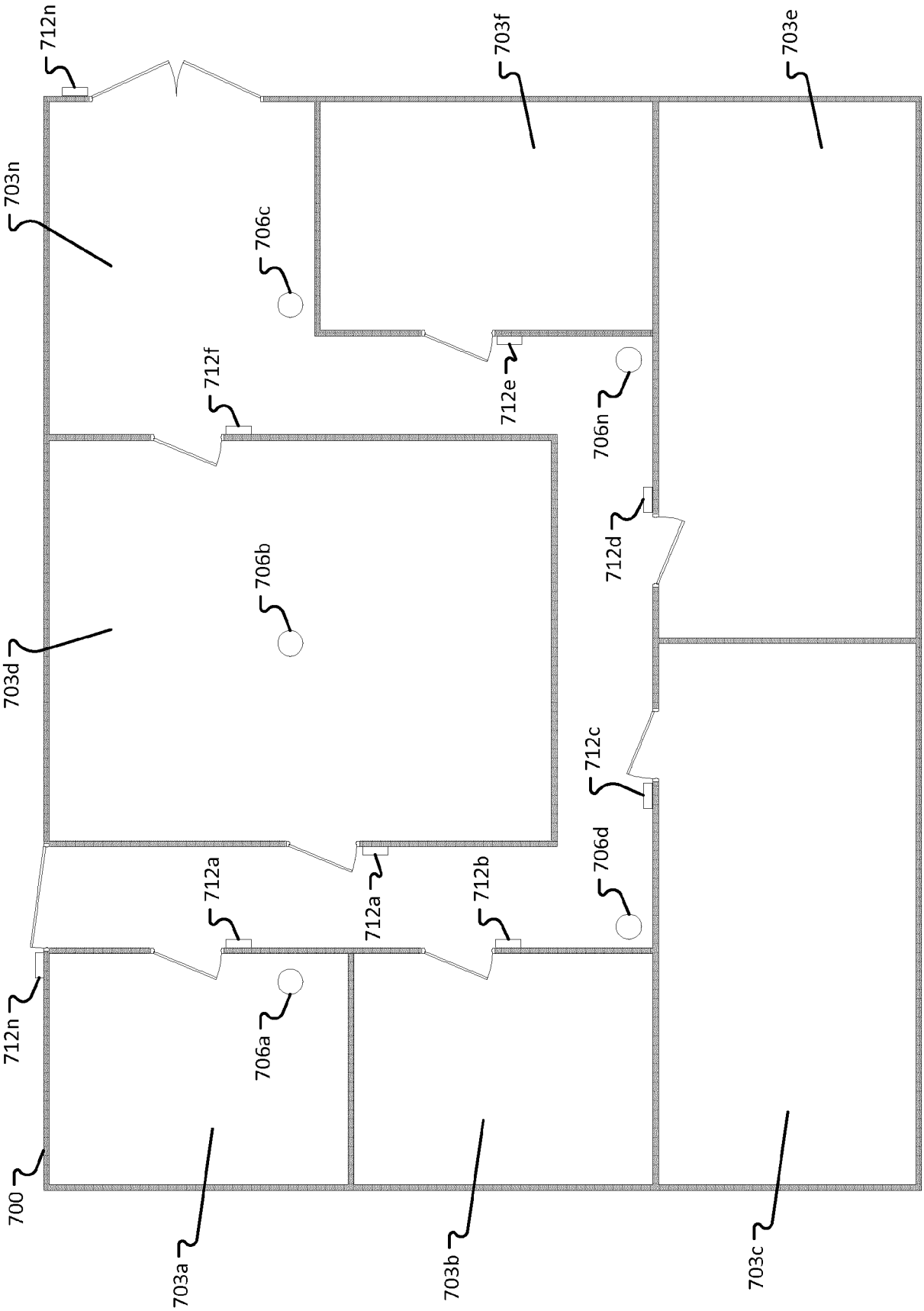

712n
703f
703e
703n
706c
712f
712e
706n
706b
712d
703d
712c
706d
712a
712a
712b
712n
706a
700
703a
703b
703c

Fig. 7

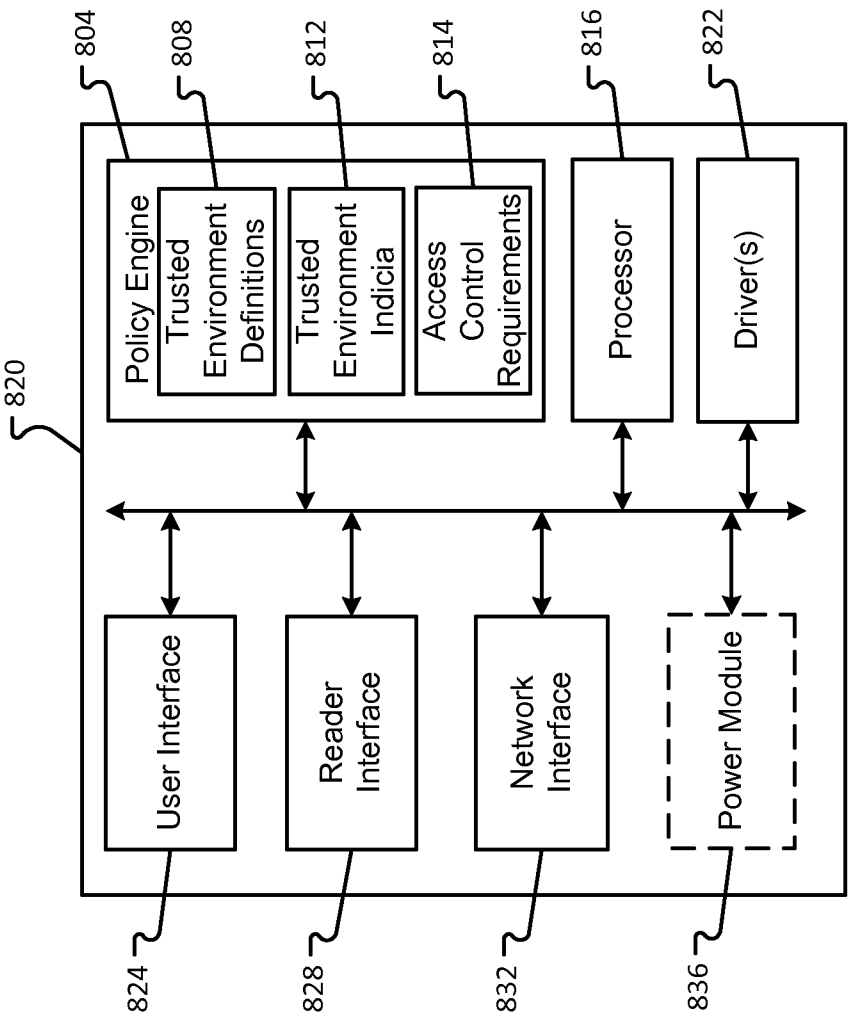

804
808
812
814
816
822
820
Policy Engine
Trusted Environment Definitions
Trusted Environment Indicia
Access Control Requirements
Processor
Driver(s)
User Interface
Reader Interface
Network Interface
Power Module
824
828
832
836

Fig. 8

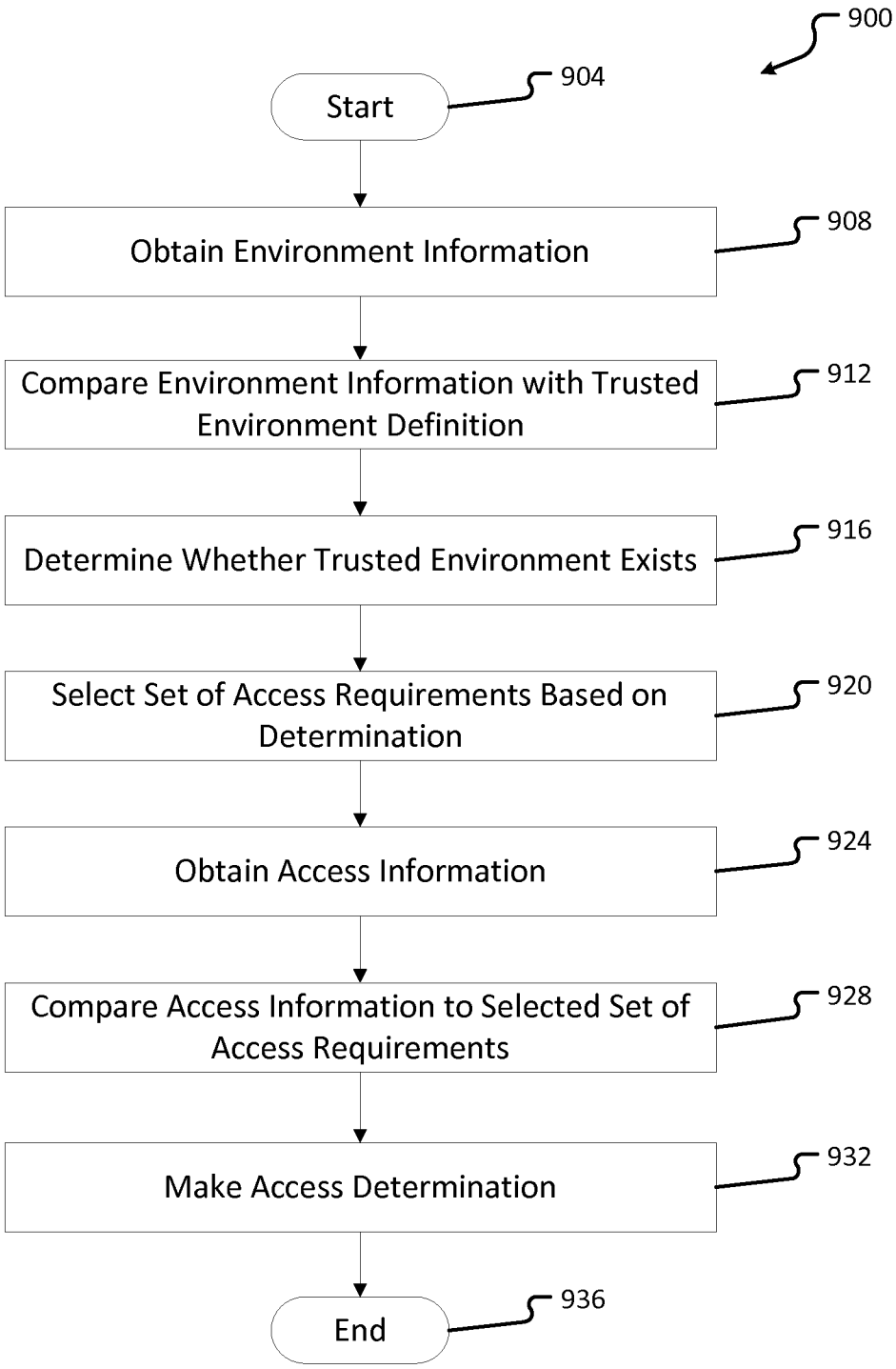

900
Start
904
Obtain Environment Information
908
Compare Environment Information with Trusted Environment Definition
912
Determine Whether Trusted Environment Exists
916
Select Set of Access Requirements Based on Determination
920
Obtain Access Information
924
Compare Access Information to Selected Set of Access Requirements
928
Make Access Determination
932
End
936

Fig. 9

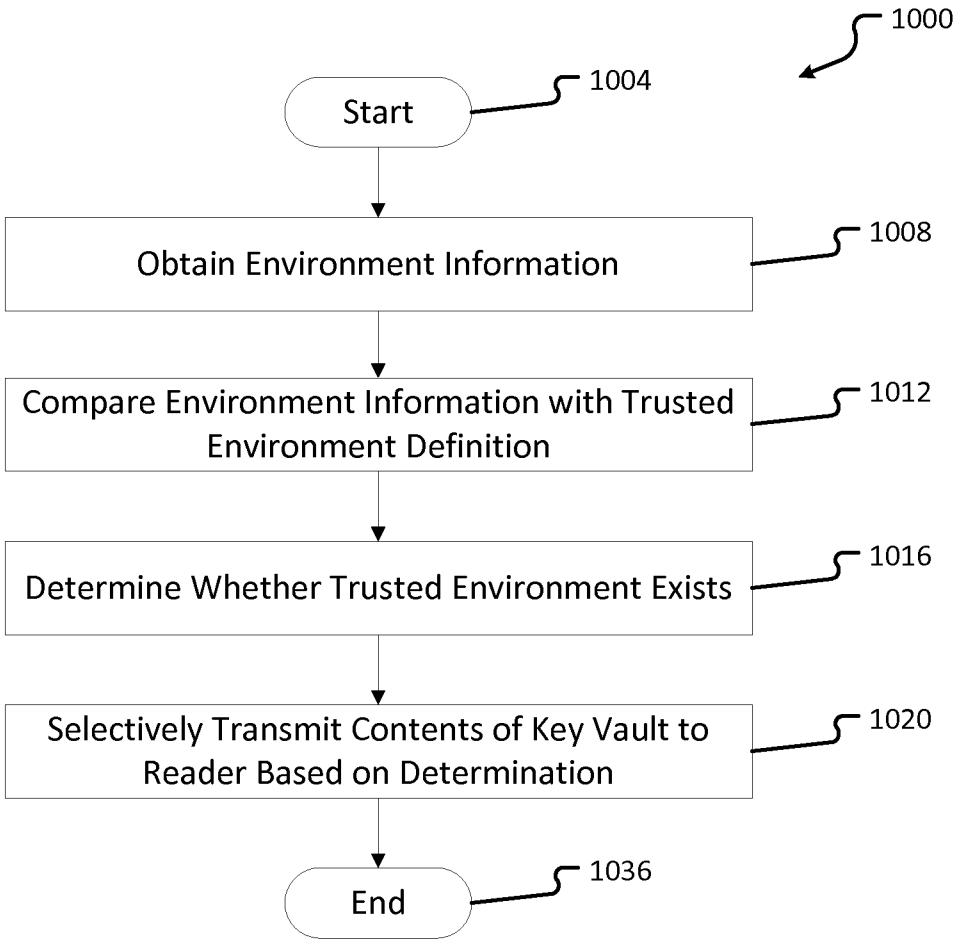

1000
Start
1004
Obtain Environment Information
1008
Compare Environment Information with Trusted Environment Definition
1012
Determine Whether Trusted Environment Exists
1016
Selectively Transmit Contents of Key Vault to Reader Based on Determination
1020
End
1036

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/059752

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/34 H04L29/06 H04W12/08
ADD. G06F1/16 H04W4/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06F H04M G07C

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 809 046 A1 (BLACKBERRY LTD [CA]) 3 December 2014 (2014-12-03) abstract; figures 1-3 paragraphs [0008] - [0010], [0012] - [0015], [0019] - [0020], [0022], [0028], [0029] paragraphs [0031] - [0033], [0038] - [0040], [0044] - [0045], [0050], [0052] - [0060] paragraphs [0063] - [0065], [0068] - [0075] ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
19 July 2016	26/07/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hristova, Ana

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/059752

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/282877 A1 (MAHAFFEY KEVIN PATRICK [US] ET AL) 18 September 2014 (2014-09-18) abstract; figures 2, 3 paragraphs [0007] - [0011], [0031] - [0078], [0085], [0087], [0089], [0174] - [0184] paragraphs [0192] - [0194], [0217] - [0219], [0229] -----	1-20
X	US 2015/121465 A1 (BERNS ADAM MICHAEL [US] ET AL) 30 April 2015 (2015-04-30) abstract; figures 1, 2 paragraphs [0002], [0003], [0015], [0018], [0020], [0025] - [0032] paragraphs [0034], [0035] -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/059752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2809046 A1	03-12-2014	EP 2809046 A1	03-12-2014
		US 2014359750 A1	04-12-2014
US 2014282877 A1	18-09-2014	US 2014282877 A1	18-09-2014
		WO 2014165230 A1	09-10-2014
US 2015121465 A1	30-04-2015	NONE	