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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 November 2016 (24.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/185008 A1

(51) International Patent Classification:
G07C 9/00 (2006.01)

(21) International Application Number:
PCT/EP2016/061392

(22) International Filing Date:
20 May 2016 (20.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/164,101	20 May 2015 (20.05.2015)	US
62/198,226	29 July 2015 (29.07.2015)	US
62/198,236	29 July 2015 (29.07.2015)	US

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; P.O. Box 70340, 107 23 Stockholm (SE).

(72) Inventor: **EINBERG, Fredrik**; Klyftvägen 8, 141 41 Huddinge (SE).

(74) Agent: **KRANSELL & WENNBORG KB**; P.O Box 27834, SE-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, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: CONFIGURATION REPORTING

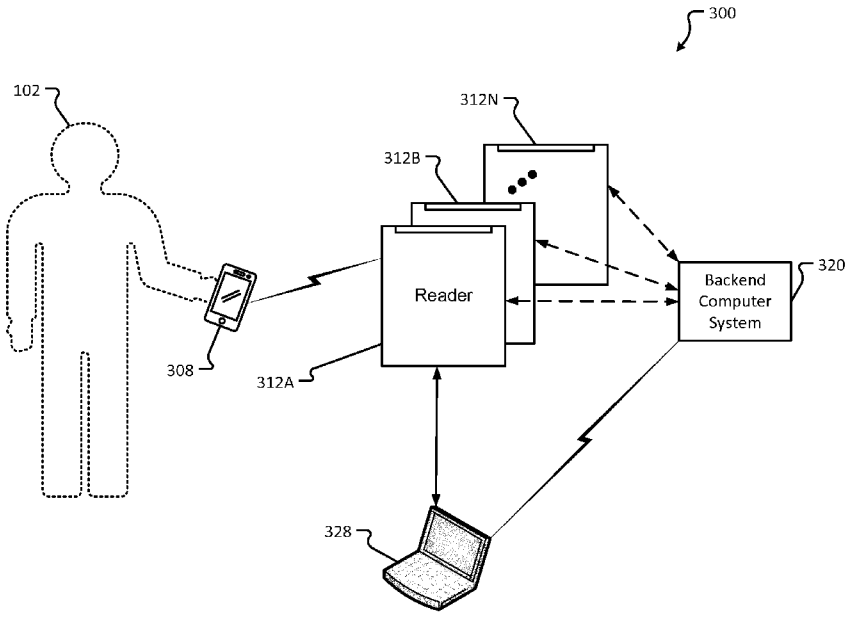

Fig. 3

(57) **Abstract**: A system and method for configuration reporting in an access control system is described. By using a mobile device to compare a reported configuration of an access control reader with a predetermined configuration, a system administrator can quickly confirm whether the configuration of the access control reader has been completed properly. Additionally, the reported configuration may be used by the access control reader in making a determination whether to grant or deny access to a user presenting credentials to the access control reader.

WO 2016/185008 A1

CONFIGURATION REPORTING

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. 62/164,101, filed on May 20, 2015, entitled "Configuration Reporting"; 62/198,236, filed on July 29, 2015, entitled "Reader Setup/Rekeying with Dedicated Card"; and 62/198,226, filed on July 29, 2015, entitled "Use Mobile Device to Configure a Lock." 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 communicate with each other within an access control system.

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, wearable device, 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 generating useful information and, in some instances, gathering the useful information. For example, an access control system may be configured to count the number of times access to a protected resource is granted 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 only be capable 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] Traditionally, RFID smart cards have been used as credential devices for access control systems. Many such cards are powered through electromagnetic induction, such that they are powered whenever (but only when) they are within the magnetic field surrounding, for example, a reader of the access control system. These cards do not need batteries to operate, and because they are powered only when placed in close proximity to a reader, they do not need any

components or circuitry for determining whether a reader is nearby and/or whether the user is attempting to gain access to the protected resource. These types of credentials are often referred to as passive credentials.

[0010] The same is not true, however, for mobile devices or smartphones that are used as credential devices. Mobile devices are typically battery-powered, and have other uses beyond their usefulness as credential devices. Rather than being powered on only when in close proximity to readers, mobile devices may be powered on at any time and in any location for any of a wide variety of purposes. Consequently, the mere fact that a mobile device has been powered on provides no indication of whether a user intends to presently use the mobile device as a credential device in an access attempt. Mobile devices are one example of an active credential, due to their inherent power source.

[0011] Physical access control systems typically comprise a reader configured to control an access point to a protected resource, and one or more credentials that, when presented to the reader, cause the reader to grant access to the protected resource. Many access control systems are customizable, such that they can be configured to provide the desired level of protection based on the unique characteristics of a particular protected resource and its authorized users. Some access control systems can be reconfigured after initial setup, and some can be provided with software or firmware updates that enhance functionality or fix bugs.

[0012] In a typical access control system implementation, a system administrator manages the configuration (including initial setup, subsequent reconfiguration, and updating) of an access control system, and more particularly of access control readers in the access control system. In some access control systems, configuration may occur via a user interface on the reader itself, or via a wired connection between the access reader and one of a computer, telephone, special-purpose device, or other user interface. In many access control systems, however, the reader has limited, if any, physical user interface elements (e.g. keypads, communication ports, etc.), whether for security or design purposes or otherwise. It is preferable, therefore, to enable configuration, reconfiguration, and updating of an access control reader over a wireless communication interface.

[0013] Regardless of whether configuration happens over a wired or wireless communication channel, and regardless of whether the individual responsible for configuring the reader and/or

the device through which configuration of a reader is being managed is physically located remotely or in the presence of the reader, it is possible for one or more errors to be made during the configuration process. When a protected resource has multiple access points, and the corresponding access control system has multiple readers, each of which controls one access point, the potential for making at least one configuration error increases.

[0014] In addition to inadvertent configuration errors, access control readers may also be susceptible to deliberate but unauthorized configuration changes, as made, for example, by a hacker who succeeds in gaining access to a reader's configuration programming. Such changes may or may not be recognizable to users of the access control system, and if not, can go undetected while diminishing the access control system's ability to secure the protected resource.

[0015] The present disclosure describes an access control system and method that utilizes configuration reporting to prevent configuration errors and detect unauthorized configuration changes. The system and method also encompass the use of configuration information to make an access control decision.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] As provided herein, a wearable device may be configured to operate in conjunction with one or more mobile devices. In some embodiments, a non-wearable mobile device used in an access control system may be provided by a manufacturer different from a wearable device also used in the access control system, and the two devices may utilize the same or different operating systems.

[0021] A wearable device may include its own power source or use power provided from another source. In some embodiments, a 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.

[0022] 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.

[0023] 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.

[0024] 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).

[0025] The term "a" or "an" entity refers to one or more of that entity. As such, the terms "a", "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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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.

[0030] 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

[0031] 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.

[0032] Fig. 1 is a diagram depicting an access control system in accordance with embodiments of the present disclosure;

[0033] Fig. 2 is a block diagram depicting a mobile device or components thereof in accordance with embodiments of the present disclosure;

[0034] Fig. 3 is a diagram depicting an access control system in accordance with other embodiments of the present disclosure;

[0035] Fig. 4 is a block diagram depicting an access control reader or components thereof in accordance with embodiments of the present disclosure;

[0036] Fig. 5 is a block diagram depicting a backend computer system or components thereof in accordance with embodiments of the present disclosure;

[0037] Fig. 6 is a flowchart depicting a method according to some embodiments of the present disclosure; and

[0038] Fig. 7 is a flowchart depicting another method according to some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0039] 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.

[0040] A configuration reporting method according to one embodiment of the present disclosure comprises: obtaining, at a processor, a configuration template from a backend computer system; storing the configuration template in a computer readable memory; establishing a communication channel with a reader via a communication interface; transmitting a signal via the communication channel to update a configuration setting of the reader based on the communication template to yield updated configuration information of the reader; receiving, at the processor and from the reader via the communication channel, a configuration signature based on the updated configuration information, wherein the configuration signature contains no information about the reader or any configuration setting thereof; and sending the configuration signature to the backend computer system. The method may also comprise receiving, at the processor, an indication of whether the configuration setting of the reader has been updated properly. The method may further comprise selectively sending, based on the indication, at least a portion of the updated configuration information to the backend computer system.

[0041] The configuration signature may be in the form of a hash, a checksum, a message authentication code based on symmetric encryption, or a digital signature based on asymmetric encryption. In some embodiments, a server may comprise the processor and the communication interface. In other embodiments, a mobile device may comprise the processor and the communication interface. The communication channel may be a secure communication channel. Establishing the communication channel may comprise completing an authentication process. The configuration setting of the reader may comprise one of an authentication requirement, an authorization requirement, an access control requirement; a reader behavior; a reader function; a software update; or a firmware update.

[0042] A mobile device according to another embodiment of the present disclosure comprises: a user interface; a reader interface for communicating with an access control reader; a processor; a memory storing instructions for execution by the processor. The instructions may be configured to cause the processor to: receive, from the access control reader and via the reader interface, information about a configuration setting of the access control reader; send, to a backend computer system, a signature of the configuration setting; and receive, from the backend computer system, an indication of whether the signature corresponds to a proper configuration setting.

[0043] The reader interface allows the mobile device to communicate with the access control reader using a wireless communication protocol. The instructions stored in the memory may be further configured to cause the processor to calculate the signature of the configuration setting. The instructions stored in the memory may also be further configured to cause the processor to request information from the access control reader about the configuration setting. The instructions stored in the memory may be still further configured to cause the processor to download a configuration template from the backend computer system; and update an initial configuration setting to yield the configuration setting. Additionally, the instructions stored in the memory may be further configured to cause the processor to send a credential to the access control reader via the reader interface.

[0044] According to still yet another embodiment of the present disclosure, an access control reader controlling access to a protected resource comprises: a communication interface; a processor; and a memory storing configurable settings. The memory may also store instructions for causing the processor to: update the configurable settings based on information received through the communication interface to yield updated configurable settings; send information corresponding to the updated configurable settings via the communication interface; and deny access to the protected resource based on a first indication, received via the communication interface, that the updated configurable settings of the access control reader do not match predetermined configurable settings.

[0045] The memory may store additional instructions for causing the processor to: receive a credential from a mobile device via the communication interface; determine whether the credentials is authorized; and selectively grant access to the protected resource based on the

determination and further based on a second indication, received via the communication interface, that the updated configurable settings of the access control reader match predetermined configurable settings. The information corresponding to the updated configurable settings may be a hash or a checksum of the updated configurable settings. The communication interface may be a wireless communication interface. The configurable settings may be associated with at least one of an authentication process, an authorization process, and an access control determination.

[0046] Before any embodiments of the disclosure are explained in greater 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.

[0047] One advantage of mobile devices as credential devices, 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., when it is more than 1.0m away from) the reader. As described herein, however, these advantages may be exploited to gain unauthorized or illicit access to access credentials or other sensitive information stored on a mobile device.

[0048] Fig. 1 is a diagram depicting an access control system 100 for authenticating a user 102 using a mobile device 108, in which embodiments of the present disclosure may be implemented. In one embodiment, the access control system 100 comprises at least one reading device 112 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 116 across a communication network 128. The access data memory 116 may be located remotely, locally, and/or locally and remotely, from the reading device 112.

[0049] 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 mobile device 108 and the reading device 112 may be established automatically when the mobile device 108 enters an active zone of an interrogating reading device 112. In one embodiment, the active zone of the reading device 112 may be defined as a three-dimensional space where the intensity of RF signals emitted by the reading device 112 exceeds a threshold of sensitivity of the mobile device 108 and the intensity of RF signals emitted by the mobile device 108 exceeds a threshold of sensitivity of the reading device 112.

[0050] In some embodiments, 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 or described herein.

[0051] In one embodiment, authentication may be required between the mobile device 108 and the reading device 112 before further communications are enabled. The further communications may include communications in which access control information (e.g., keys, codes, credentials, etc.) or sensitive information is shared. In some embodiments, the authentication may be provided via one-way or mutual authentication. Examples of authentication may include, but are not limited to, simple authentication based on site codes, trusted data formats, shared secrets, and/or the like. As can be appreciated, access control information is more sensitive and may require more involved validation via, for example, an encrypted exchange of access control information.

[0052] In some embodiments, the reading device 112 may be configured to request access control information from the mobile device 108. This access control information may be used to

validate the mobile device 108 to the reading device 112. Validation may include referring to information stored in access data memory 118 or some other memory associated with 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 mobile device 108 may be validated via one or more components of the access control system 100. Once the mobile device 108 is authenticated, credential information associated with the mobile device 108 may be validated. During this process, the reading device 112 may generate signals facilitating execution of the results of interrogating the mobile device 108 (e.g., signals that engage/disengage a locking mechanism, allow/disallow movement of a monitored article, temporarily disable the reading device 112, activate an alarm system, provide access to a computer system, provide access to a particular document, and the like). Alternatively, the access server 120 or some other system backend component may generate such signals.

[0053] 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 device. The access data memory 118 may comprise a hard disk drive or other random access memory.

[0054] 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.

[0055] 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 mobile device 108 via the reading device 112 or intended for the reading device 112.

[0056] Fig. 2 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 of Figs. 1 and 2 may be provided with a storage vault 212 that stores one or a plurality of mobile keys and/or other sensitive information. The key(s) and/or other sensitive information 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.

[0057] 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 112 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.

[0058] 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.* if 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.

[0059] The mobile device 108 is shown to include computer memory 204 that stores one or more Operating Systems (O/S) 208 and a storage vault 212, among other items. The mobile device 108 is also shown to include a processor 216, one or more drivers 220, a user interface 224, a reader interface 228, a network interface 232, and a power module 236. Suitable

examples of a mobile device 108 include, without limitation, smart phones, PDAs, laptops, PCs, tablets, netbooks, wearable devices, and the like.

[0060] The memory 204 may correspond to any type of non-transitory computer-readable medium. In some embodiments, the memory 204 may comprise volatile or non-volatile memory and a controller for the same. Non-limiting examples of memory 204 that may be utilized in the mobile device 108 include RAM, ROM, buffer memory, flash memory, solid-state memory, or variants thereof.

[0061] The O/S 208 may correspond to one or multiple operating systems. The nature of the O/S 208 may depend upon the hardware of the mobile device 108 and the form factor of the mobile device 108. The O/S 208 may be viewed as an application stored in memory 204 that is processor-executable. The O/S 208 is a particular type of general-purpose application that enables other applications stored in memory 204 (e.g., a browser, an email application, an SMS application, etc.) to leverage the various hardware components and driver(s) 220 of the mobile device 108. In some embodiments, the O/S 208 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 208 may provide a mechanism for viewing and accessing the various applications stored in memory 204 and other data stored in memory 204.

[0062] The processor 216 may correspond to one or many microprocessors that are contained within the housing of the mobile device 108 with the memory 204. In some embodiments, the processor 216 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 216 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 216 implements sequential digital logic as it has internal memory. As with most known microprocessors, the processor 216 may operate on numbers and symbols represented in the binary numeral system.

[0063] The driver(s) 220 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 224, reader interface 228, and network interface 232, may each have a dedicated driver 220 that provides appropriate control signals to effect their

operation. The driver(s) 220 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 220 of the reader interface 228 may be adapted to ensure that the reader interface 228 follows the appropriate proximity-based protocols (e.g., BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, etc.) such that the reader interface 228 can exchange communications with the reader. Likewise, the driver 220 of the network interface 232 may be adapted to ensure that the network interface 232 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 232 can exchange communications via the communication network 128. As can be appreciated, the driver(s) 220 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0064] As mentioned above, the user interface 224 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 224 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 224 include, without limitation, display screens, touchscreens, lights, speakers, etc. It should be appreciated that the user interface 224 may also include a combined user input and user output device, such as a touch-sensitive display or the like.

[0065] The reader interface 228 may correspond to the hardware that facilitates communications with the credential for the mobile device 108. The reader interface 228 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 228 is specifically provided to facilitate proximity-based communications with a credential via a communication channel or multiple communication channels.

[0066] The network interface 232 may comprise hardware that facilitates communications with other communication devices over the communication network 128. As mentioned above, the network interface 232 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 232 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.

[0067] The power module 236 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 236 may also include some implementation of surge protection circuitry to protect the components of the mobile device 108 from power surges.

[0068] Referring now to Fig. 3, in some embodiments, an access control system 300 includes one or more access control readers 312A-312N, one or more credential devices 308 (illustrated in Fig. 3 as a mobile device in the form of a smartphone or tablet), a configuration device 328 (also illustrated as a mobile device, in the form of a laptop), and a backend computer system 320. Although the configuration device 328 is depicted in Fig. 3 as a mobile device, the configuration device 328 may also be a server (e.g. an access server 120, a configuration server, or any other suitable server), a desktop computer, or another non-mobile computing device. Additionally, although the configuration device 328 is depicted in Fig. 3 as separate from the backend computer system 320, the backend computer system 320 may, in some embodiments, be used as the configuration device 328, in addition to providing the other features and functionality described herein. In operation, a system administrator uses the configuration device 328 to configure each of the readers 312A-312N. It should be appreciated that the readers may alternatively or additionally include any type of device having a reading capability including personal computers, laptops, smartphones, or any other device with interrogation capabilities.

[0069] The configuration device 328 may communicate with the backend computer system 320 to obtain the proper configuration for each reader, and/or to report to the backend computer system 320 that one or more of the readers 312A-312N have been configured, and/or to report the configuration of one or more of the readers 312A-312N to the backend computer system 320. The configuration device 328 may communicate with the backend computer system 320 wirelessly or over a wired connection. Additionally, the configuration device 328 may be in

constant communication with the backend computer system 320, or the configuration device 328 may periodically connect to the backend computer system 320 (whether wirelessly or via a wired connection) to obtain configuration information and/or to report configuration information.

[0070] A user 302 uses a credential device 308 to provide credentials to an access control system reader 312 for purposes of gaining access to a resource protected by the access control system 300. The communications between the credential device 308 and the reader 312 comprise information about the configuration of the reader 312. That information is utilized to determine whether access will be granted to the user 302. Additional details regarding the operation of the system 300 will be provided below, following a discussion of certain components of the system 300.

[0071] With reference to Fig. 4, each access control reader 312 may include a memory 404 and a processor 416, in addition to a communication interface 420 capable of communicating with a mobile device 308. Each access control reader may also include one or more drivers 424 and a power source 428.

[0072] The memory 404 of the reader 312 may correspond to any type of non-transitory computer-readable medium. 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 312 include RAM, DRAM, SDRAM, ROM, buffer memory, flash memory, solid-state memory, or variants thereof. The memory 404 may be used in connection with the execution of application programming or instructions by the processor 416. Indeed, the memory 404 stores instructions 412 for execution by the processor 416. Such instructions may comprise, for example, instructions providing a configuration interface to a connected configuration device 328, whereby the configuration device 328 can be used by a system administrator to selectively modify available settings of the reader 312 (e.g. the configurable settings 408). The memory 404 may also be used for the temporary or long term storage of data, including, for example, data about credentials reviewed by the reader 312, access attempts involving the reader 312, the number and timing of access granted decisions by the reader 312, the number and timing of access denied decisions by the reader 312, and so forth. Additionally, the memory 404 may store one or more configurable settings 408. The configurable settings 408 may be dispersed in multiple locations throughout the instructions 412 stored in the memory 404,

or they may be gathered in a single file, such as a .config file, that forms part of the instructions 412 stored in the memory 404 or that is referenced by the instructions 412. The reader 312 is configured to control an access point to a protected resource (e.g. by granting or denying access to the protected resource through the access point based upon one or more requirements).

[0073] The processor 416 may correspond to one or many microprocessors that are contained within the housing of the reader 312 with the memory 404. In some embodiments, the processor 416 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 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.

[0074] The communication interface 420 may correspond to the hardware that facilitates communications with the credential device 308 and/or with the configuration device 328. The communication interface 420 may include one or more of 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), an Ultrasonic interface (e.g., speaker, microphone, and associated circuitry), or any other suitable interface based on the communication protocol(s) that will be used to communicate with the credential device 308 and/or the configuration device 328. In some embodiments, the communication interface 420 is specifically provided to facilitate proximity-based communications with a credential device 308 or a configuration device 328 via a communication channel or multiple communication channels.

[0075] The driver(s) 424 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 communication interface 420 may have a dedicated driver 424 that provides appropriate control signals to effect its operation. The driver(s) 424 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 424 of the

communication interface 420 may be adapted to ensure that the communication interface 420 follows the appropriate protocols (e.g., Bluetooth, BLE, NFC, Infrared, Ultrasonic, IEEE 802.11N, TCP/IP (at one or more layers in the OSI model), UDP, RTP, GSM, LTE, Wi-Fi, etc.) for exchanging communications with a credential device 308 and/or a configuration device 328. As can be appreciated, the driver(s) 424 may also be configured to control wired hardware components (e.g., a USB driver, an Ethernet driver, etc.).

[0076] The power source 428 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 312. In some embodiments, the power source 428 may also include some implementation of surge protection circuitry to protect the components of the reader 312 from power surges.

[0077] A credential device 308 may have any form factor, including a card, a key fob, or a mobile device (e.g. a device that can be positioned within communication range of the reader and that comprises a memory, a processor for carrying out instructions stored in the memory, and a wireless communication capability). The credential device 308 may include some or all of the components of the mobile device 108.

[0078] The backend computer system 320, which may or may not be in wired or wireless communication with one or more of the reader(s) 312, includes a memory 504, a processor 516, a communication interface 520, one or more driver(s) 524, a power source 528, and a user interface 532.

[0079] The memory 504 of the backend computer system 320, like the memory 404 of the reader 312, may correspond to any type of non-transitory computer-readable medium. In some embodiments, the memory 504 may comprise volatile or non-volatile memory and a controller for the same. Non-limiting examples of memory 504 that may be utilized in the backend computer system 320 include RAM, DRAM, SDRAM, ROM, buffer memory, flash memory, solid-state memory, or variants thereof. In some embodiments, the memory 504 may be or comprise a hard disk. The memory 504 stores information relevant to the administration of the access control system, such as configuration information 508 and/or credential device information 516.

[0080] The configuration information 508 may comprise one or more configuration templates providing the proper values or settings for one or more configurable settings (e.g. the configurable settings 408) of one or more access control readers (e.g. the access control reader 312). A configuration template may be in the form of a computer-readable file that can be copied over an existing computer-readable configuration settings file, or it may be a table or spreadsheet populated with a value for one or more configurable settings, or it may be in any other format suitable for providing information about a proper or desired configuration to a configuration device 328. The configuration information 508 may also comprise information about the current configuration of the reader(s) 312, which information may be, or may be used to calculate, a hash or a checksum of the current configuration of the reader(s) 312, a message authentication code (e.g. a method authentication code used for symmetric encryption), or a digital signature based on asymmetric encryption. The configuration information 508 may further comprise historical information about the past configuration(s) of the reader(s) 312.

[0081] The credential device information 516 may comprise information about one or more currently authorized credential devices 308. Such information may include, for example, information about one or more authorized credentials that are linked with or have been provided to each authorized credential device 308. Such information may also include, for example, identification or descriptive information about each authorized credential device 308. The credential device information 516 may further comprise information about blacklisted credential devices (e.g. credential devices to which access will not be granted regardless of whether they provide authorized credentials to the access control reader 312).

[0082] The memory 504 may be used in connection with the execution of application programming or instructions by the processor 516. For example, the memory 504 may store instructions for execution by the processor 516. The memory 504 may also be used, for example, for the temporary or long term storage of data, including, for example, historical configuration information, historical credential information, and one or more metrics regarding the use and/or functioning of one or more readers 312.

[0083] The communication interface 520 may correspond to the hardware that facilitates communications with one or more of the reader(s) 312, the credential device 308, and/or the configuration device 328. The communication interface 520 may include one or more of 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), an Ultrasonic interface (e.g., speaker, microphone, and associated circuitry), or any other suitable interface based on the communication protocol(s) that will be used to communicate with the reader(s) 312, the credential device 308 and/or the configuration device 328. In some embodiments, the communication interface 520 is specifically provided to facilitate proximity-based communications with a credential device 308 or a configuration device 328 via a communication channel or multiple communication channels.

[0084] The user interface 532 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 532 include, without limitation, one or more of a keyboard, mouse, button, touch-sensitive surface, pen, camera, microphone, etc. Examples of suitable user output devices that may be included in the user interface 532 include, without limitation, display screens, touchscreens, lights, speakers, etc. It should be appreciated that the user interface 532 may also include a combined user input and user output device, such as a touch-sensitive display or the like. The user interface 532 may allow a system administrator to modify the configuration information 508, e.g. by selecting new or different configuration settings. The user interface 532 may also allow a system administrator to modify the credential device information 512, e.g. by adding information about newly authorized credential devices to the credential device information 512, removing information about no-longer-authorized credential devices from the credential device information 512, and so forth.

[0085] The processor 516, the driver(s) 524, and the power source 528 may be substantially similar or identical to the processor 416, the driver(s) 424, and the power source 428, respectively.

[0086] In embodiments, a system administrator uses a mobile device (such as a mobile device 108) as a configuration device 328 to configure an access control reader 312 of the access control system 300. The configuration device 328 may be a special purpose device intended specifically for configuring access control readers 312, or it may be a mobile device such as a smartphone, tablet, or laptop that is running configuration software or accessing a configuration interface of a

reader 312. The configuration device 328 may scan for readers 312 within communication range, and may allow the system administrator to select one of several readers 312 within communication range for configuration. The configuration device 328 may communicate with the reader 312 using any one or more of a variety of communication protocols, including but not limited to signal modulation (e.g., Amplitude Modulation, Frequency Modulation, Phase Modulation, combinations thereof, variants thereof, or the like); protocols defined in ISO 14443, ISO 15693, or ISO 18092; RFID; FeliCa; Near Field Communications (NFC); Bluetooth; Bluetooth low energy (BLE); Wi-Fi (e.g., 802.11N, variants thereof, or extensions thereto); ZigBee; GSM; infrared; sound; light; and so forth. Any of the foregoing protocols may be supported by the communication interface 420 of the reader 312, and or by the communication interface 520 of the backend computer system 320.

[0087] To protect against unauthorized configuration changes, the reader 312 may be configured (e.g. may include instructions 412 for causing the processor 416) to require the configuration device 328 to successfully complete one or more authentication and/or authorization processes before the configuration device 328 may be used to modify the configurable settings 408 of the reader 312. The reader 312 may also be configured to require that a secure communication channel be established with a configuration device 328 before the configuration device 328 may be used to modify the configurable settings 408. Security may be provided using any suitable security protocol, including, without limitation, HTTPS, SNMP, SSL, and/or TLS.

[0088] Once a communication channel (secured, if necessary) has been established between the configuration device 328 and the reader 312, the system administrator can configure the configurable settings 408 of the reader 312 as necessary using the configuration device 328. Configuration may include, without limitation, loading one or more new or replacement mobile keys into the memory 404 of the reader 312, or selecting one or more mobile keys from among a plurality of available mobile keys; setting or changing authentication requirements (e.g. the requirements that must be satisfied for the reader 312 to trust a credential device 308 and/or vice versa); setting or changing authorization requirements (e.g. the requirements that must be met to determine whether a system user (e.g. user 302) is authorized to enter the protected resource); setting or changing access control requirements (e.g. additional requirements, if any, that must be

met before the reader 312 will grant access to an authorized user (e.g. user 302)); setting or changing behaviors of the reader 312 (e.g. how the reader 312 responds to certain inputs or events); setting or changing functions of the reader 312 (e.g. what the reader 312 can do and/or how the reader 312 can utilize the various components thereof); and updating software or firmware to add new features and/or to provide bug fixes for the reader 312. Configuration may involve selecting, from a graphical user interface 532 on the configuration device 328, one of two or more configuration options for a given configurable setting 408. Configuration may also involve directly editing instructions and/or files (e.g. a .config file) stored in the memory 404 of a reader 312, for example by using a text editor. In embodiments, once the system administrator has modified the configurable settings 408 of the reader 312, the reader 312 sends information to the configuration device 328 corresponding to its updated configuration.

[0089] The configuration device 328 then reports the updated configuration of the reader 312 to the backend computer system 320. The reporting may happen, for example, every time a single configurable setting 408 of the reader 312 is changed, or at the end of a given configuration session (e.g. when a communication channel between the configuration device 328 and the access control reader 312 is closed, whether or not all of the configurable settings 408 of the access control reader 312 have been configured, or when the new configuration of the configurable settings 408 is saved), or after every configurable setting 408 has been configured. The reporting may be fully automatic, or it may automatically happen once the system administrator saves the new or updated configuration to the memory 404 of the reader 312 or to a memory of the configuration device 328, or once the reader 312 sends information to the configuration device 328 corresponding to the updated configuration of the reader 312. The reporting may also happen only if the system administrator executes a specific command on the configuration device 328.

[0090] Regardless of when it happens, the reporting may include information about the configuration of the reader 312 (e.g. the selected option, value, etc. for each configurable setting 408) and may also include information about whether the reader 312 is fully configured (including, for example, a percentage representing the completeness of the configuration of the reader 312). This information may be used by the system administrator to ensure that a given reader 312 is fully configured before it is introduced (or re-introduced) into service, to track the

progress of configuration or reconfiguration of a plurality of readers 312, and/or to identify and fix errors in the configuration of a given reader 312. The backend computer system 320 may be configured to automatically compare received configuration information regarding one or more readers 312 with a predetermined configuration template, and to indicate to the configuration device 328 whether the configurable settings of the reader 312 match the predetermined configuration.

[0091] In some embodiments, the reporting from the configuration device 328 to the backend computer system 320 may include, or may consist only of (at least initially), a signature of the configurable settings 408 (e.g. a hash or other checksum calculated with at least some reader parameters or configuration parameters as inputs thereto, a message authentication code, or a digital signature based on asymmetric encryption). The parameters that may be provided as inputs to the signature calculation may include, without limitation, software/firmware version number, an identification number of the reader 312, a location of the reader 312, a date of the configuration update, a time of the configuration update, a time of configuration expiration, a number of subroutines or functions available to the reader 312, a number of states available to the reader 312, driver identifiers, a read counter value, and any other configurable setting 408 available to the reader software or firmware. The signature may be calculated by the reader 312 and sent to the configuration device 328, or it may be calculated by the configuration device 328.

[0092] If the received signature is a hash or checksum, the backend computer system 320 can then compare the received signature with a hash or checksum of the proper configuration calculated by the backend computer system 320 (and more specifically, by the processor 516 of the backend computer system 320), to determine whether the configurations match. If the received signature is a message authentication code, the backend computer system 320 can compare the received message authentication code with a calculated method authentication code (e.g. a message authentication code calculated by the backend computer system 320 using the proper configuration as an input and based on a symmetric key shared by the reader 312 and the backend computer system 320) to determine whether the received and calculated message authentication codes, and thus the actual reader configuration and the proper configuration, match.. If the received signature is a digital signature based on asymmetric encryption, then the reader 312 generates the digital signature based on its configuration and using a private key.

Once the digital signature is received from the reader 312, the backend computer system 320 uses a public key received from the reader 312 as well as the proper configuration (which it may have stored in memory 504, or which it may receive from the reader 312 together with the digital signature based on asymmetric encryption) to verify the digital signature from the reader 312 and determine whether the configurations match. If the configurations do not match, then the configuration device 328 may obtain from the reader 312 (if necessary) and send to the backend computer system 320 more detailed information about the configurable settings 408, so that the backend computer system 320 can determine which configurable setting(s) 408 is configured improperly.

[0093] One benefit of using a configuration signature as described herein is that the configuration signature can be calculated in such a way that no information about the actual configuration of the reader 312 or about the reader 312 itself can be extracted from the configuration signature. Thus, while the configuration signature may be used to verify that the actual configuration of the reader 312 matches a desired configuration, it may also be communicated from a reader 312 to a configuration device 328, or from a configuration device 328 to a backend computer system 320, without risk of revealing the configuration of the reader 312 to bad actors.

[0094] Alternatively, the configuration device 328 may make a similar determination regarding whether the configurations match by comparing the configuration signature to a signature of the proper configuration as received from the backend computer system 320, or by comparing the configuration signature to a signature of another reader 312, or by comparing the configuration signature to a signature calculated by the configuration device 328 based on configuration information provided to the configuration device 328 by the backend computer system 320. The configuration device 328 may, for example, calculate the signatures of each reader configuration that is modified through the configuration device 328, and compare two or more of those signatures to each other. The purpose of the determination may be to verify that a recent configuration was completed properly, or it may be simply to verify that two or more access control readers 312 have the same configuration.

[0095] When the backend computer system 320 makes the signature match determination, the backend computer system 320 then sends the result of the determination to the configuration

device 328. If the configuration signature does not correspond to the correct configuration, then the backend computer system 320 may provide the configuration device 328 with information about which configurable settings 408 are improperly configured. Depending on how much information about the configurable settings 408 can be determined from the configuration signature, the backend computer system 320 may need to request additional information from the configuration device 328 about the configurable settings 408 before it can provide specific information to the configuration device 328 about how to correct the configuration of the reader 312. The configuration device 328 may, in turn, need to request additional information from the access control reader 312 about the configurable settings 408 of the access control reader 312 before it can provide the needed information to the backend computer system 320.

[0096] In some embodiments according to the present disclosure, including in particular embodiments where a plurality of readers 312 will be updated with the same configurable settings 408, the backend computer system 320 may calculate a configuration signature for the proper configuration, and may provide the calculated configuration signature to the configuration device 328, which may in turn store the configuration signature in the memory 404 of the reader 312. Then, the reader 312 may provide the stored configuration signature to a credential device 308 as part of making an access control decision, as described below.

[0097] In accordance with some embodiments of the present disclosure and referring again to Fig. 3, the configuration signature of a given reader 312 may be considered as part of an access control decision. More specifically, the reader 312 may transmit its configuration signature to a credential device 308 presented to the reader 312 by a user 302 seeking access to the protected resource. The credential device 308 may then evaluate whether the configuration signature of the reader 312 corresponds to a predetermined configuration. The predetermined configuration (or information about the predetermined configuration, such as a hash or checksum) may have been stored in the credential device 308 previously (e.g. in conjunction with authorizing the credential device 308 within the access control system), or it may have been provided to the credential device 308 by the reader 312 or by another reader in the same access control system. Once the credential device 308 has evaluated whether the configuration signature of the reader 312 corresponds to the predetermined configuration, the credential device 308 may send that determination to the reader 312. The credential device 308 may itself provide the determination

to the reader 312, or it may provide an access granted or an access denied decision to the reader 312, which access granted or access denied decision may be based on whether the configuration signature of the reader 312 corresponds to the predetermined configuration.

[0098] Alternatively, the credential device 308 may be in wireless communication with the backend computer system 320 (whether directly or via a communication network, such as the Internet or a cellular network), and may transmit the configuration signature from the reader 312 to the backend computer system 320. The backend computer system 320 can then determine whether the configuration signature corresponds to the predetermined configuration and send the result of the determination to the credential device 308, which can then report the result of the determination to the reader 312.

[0099] As another alternative, the credential device 308 may transmit a configuration signature of the predetermined configuration to the reader 312. The transmission of the configuration signature of the predetermined configuration may also comprise one or more credentials or other access control information from which the reader 312 can evaluate whether the credential device 308 is authorized to access the resource protected by the reader 312. Upon receiving the configuration signature of the predetermined configuration, the reader 312 may determine whether the predetermined configuration signature matches an actual configuration signature (e.g. a signature generated using the actual configuration of the reader 312) stored in a memory 404 of the reader 312. If the predetermined configuration signature matches the actual configuration signature, then the reader 312 may proceed to process one or more credentials or other access control information received from the credential device 308. If the predetermined configuration signature does not match the actual configuration signature, then the reader 312 may send a notification to the credential device 308 and/or to the backend server 320 indicating that it is improperly configured, and/or the reader 312 may be configured not to process any more access requests from any other credential devices until the configuration of the reader 312 is updated.

[00100] If the configuration signature of the reader 312 is determined to correspond with the predetermined configuration, then the reader 312 may operate normally (e.g. by granting access to a user 302 who presents valid credentials via an authorized credential device 308). If the configuration signature of the reader 312 is determined not to correspond with the predetermined

configuration—suggesting either that the reader 312 was inadvertently configured improperly, or has been tampered with—then the reader 312 may deny access even to holders of authorized credential devices such as the credential device 308 until its configuration is corrected. In this way, an unauthorized individual cannot gain access to the protected resource by, for example, first reconfiguring the access control reader 312 to accept unauthorized credentials (e.g. mobile keys) or to accept authorized credentials from unauthorized credential devices, and then using the unauthorized credentials and/or credential devices to cause the access control reader 312 to grant access.

[00101] Referring now to Fig.6, a method 600 of configuring an access control reader 312 according to one embodiment of the present disclosure comprises downloading an updated configuration template from a backend computer system 320 (step 610). The downloading may happen via a wired or a wireless connection. A system administrator may, for example, prepare the configuration template using the backend computer system 320, and then download the configuration template to a configuration device 328. Alternatively, the system administrator may establish a communication channel with the backend computer system 320 using a configuration device 328, then use an interface hosted by the backend computer system 320 to prepare a configuration template from the configuration device 328, and then save the configuration template to the backend computer system 320. The configuration device 328 may authenticate with the backend computer system 320 before downloading the configuration template from the backend computer system 320, and the configuration device 328 may also be required to supply a password or other credentials to the backend computer system 320 before downloading the configuration template from the backend computer system 320.

[00102] The method 600 also comprises establishing a communication channel between the configuration device 328 and a reader 312 (step 620). The communication channel may be established using any suitable communication protocol(s), including one or more protocols specifically identified herein. Establishing the communication channel with the reader 312 may require authentication of the configuration device 328 with the reader 312, authentication of the reader 312 with the configuration device 328, or both. Establishing the communication channel with the reader 312 may also comprise an exchange of a password, mobile key, or other

credentials, whether from the configuration device 328 to the reader 312, from the reader 312 to the configuration device 328, or both.

[0100] The method 600 further comprises updating the configurable settings 408 of the reader 312 based on the configuration template (step 630). This may occur automatically once a communication channel is established between the configuration device 328 and the reader 312, or it may require user input. For example, a system administrator using the configuration device 328 may press a button or select an option or run an application or other program on the configuration device 328 that causes the configuration device 328 to modify the configurable settings 408 of the reader 312 based on the configuration template. In some embodiments, the system administrator may be required to manually update the configurable settings 408 based on the configuration template and using the configuration device 328.

[0101] The method 600 further includes receiving updated configuration information from the reader 312 (step 640). The updated configuration information may comprise a signature of the updated configurable settings 408, calculated by the processor 416 of the reader 312, or the updated configuration information may comprises a direct copy of the updated configurable settings 408, or the updated configuration information may comprise information about the updated configurable settings 408. The reader 312 may send the updated configuration information to the configuration device 312 automatically after every configurable setting 408 has been updated, or after the configurable settings 408 have been saved to the memory 404 of the reader 312, or upon receipt of an indication from the configuration device 328 that all necessary changes to the configurable settings 408 have been made. The latter indication may comprise a command from the configuration device 328 to the reader 312 to send the configuration device 328 the updated configuration information. Alternatively, the indication may comprise a read or download request from the configuration device 328 to the reader 312, to which the reader 312 responds by sending the updated configuration information to the configuration device 328.

[0102] The configuration device 328 then reports the configuration update of the reader 312 to the backend computer system 320 (step 650). The report may comprise a copy of the updated configurable settings 408, or a signature of the updated configurable settings 408, or other information about the updated configurable settings 408. The report may be made immediately

after the configurable settings 408 of the reader 312 have been updated and/or immediately after the configuration device 328 has received the updated configuration information from the reader 312, or the report may be made after all needed configuration changes have been made, or when the configuration device 328 is again connected to the backend computer system 320 (whether wirelessly or via a wired connection). The reporting may happen automatically or after a command to initiate the reporting has been entered by the system administrator on the configuration device 328.

[0103] After reporting the configuration update of the reader 312 to the backend computer system 320, the configuration device 328 receives from the backend computer system 320 a confirmation that the updated configuration of the reader 312 is correct (step 660). Alternatively, if the updated configuration of the reader 312 is not correct, the configuration device 328 may receive an indication from the backend computer system 320 that the updated configuration is not correct, which may include information about which configurable setting 408 is not properly configured and/or a request to provide more information so that the backend computer system 320 can determine which configurable setting 408 is not properly configured. In embodiments, one or both of the configuration device 328 and the backend computer system 320 may keep a log in which information about each configuration update is tracked.

[0104] Referring now to Fig. 7, a method 700 of utilizing configuration reporting in an access control decision according to another embodiment of the present disclosure comprises establishing a communication channel between a credential device 308 and a reader 312 (step 710). Establishing the communication channel may be initiated automatically based upon a predetermined trigger, which may be, for example and without limitation, detection of the reader 312 by the credential device 308; detection of the credential device 308 by the reader 312; or determination by the credential device that it is in a location corresponding to the location of the reader 312. Alternatively, establishing the communication channel may be initiated manually, for example by a user 302 tapping the credential device 308 on the reader 312, or manipulating the credential device 308 (or any component thereof, including a user interface such as the user interface 124 thereof) to cause the credential device 308 to establish a communication channel with the reader 312. Establishing the communication channel may comprise completing an authentication process.

[0105] The credential device 308 also receives, from the reader 312, information about the configuration of the reader 312 (step 720). The information about the configuration of the reader 312 may comprise a copy of the configurable settings 408 of the reader 312, or the information about the configuration of the reader 312 may comprise a signature (e.g. a hash or checksum) the configurable settings 408 of the reader 312. The reader 312 may be configured to send the information about its configurable settings immediately upon establishment of a communication channel with a credential device 308, or the reader 312 may send the information about its configurable settings in response to a request, command, or other signal from the credential device 308.

[0106] After receiving the configuration information from the reader 312, the credential device 308 determines whether the reader 312 has the proper configuration (step 730). Determining whether the reader 312 has the proper configuration may comprise comparing the configuration information received from the reader 312 with information about or corresponding to the proper configuration that is stored on the credential device 308. For example, the credential device 308 may have stored in a memory thereof a copy of the configuration template for the reader, and may compare the configuration information received from the reader 312 with the configuration template to determine whether the configurable settings 408 of the reader 312 are properly configured. Alternatively, the credential device 308 may received a configuration signature (e.g. a hash or checksum) from the reader 312, and may compare the received configuration signature with a stored configuration signature (e.g. a hash or checksum) corresponding to the proper configuration to determine whether the received and stored configuration signatures do or do not match. The stored configuration signature, as well as the stored copy of the configuration template referenced above, may have been received from the backend computer system 320 prior to or during the method 700.

[0107] In some embodiments, the credential device 308 determines whether the reader 312 has the proper configuration by sending the configuration information received from the reader 312 to the backend computer system 320. The backend computer system 320 may then compare the received configuration information from the reader 312 with stored information about the last authorized configuration of the reader 312, or with a stored configuration template, or with a stored or calculated configuration signature (e.g. a hash or checksum), to determine whether the

reader 312 has the proper configuration. Once the backend computer system 320 has made such a determination, it provides the determination to the credential device 312, which makes or adopts the same determination based on the information received from the backend computer system 320.

[0108] Once the credential device 312 has determined that the reader 312 has the proper configuration, the credential device 312 sends the determination to the reader 312 (step 740). If the determination confirms that the reader 312 has the proper configuration, then the reader 312 operates normally (e.g. grants access to a holder or user of a credential device 308 from which it receives proper credentials). If the determination confirms that the reader 312 does not have the proper configuration, then the reader 312 denies access until its configurable settings 408 have been properly configured. In the latter scenario, the reader 312 may continue to process access requests (e.g. examine presented credentials from credential devices 308), or it may enter a sleep mode or other reduced functionality mode in which it does not examine presented credentials.

[0109] The credential device 328 also sends its credentials to the reader 312 (step 750). The credential device 328 may be configured to send its credentials to the reader 312 only if it determines that the reader 312 is properly configured, or the credential device 328 may be configured to send its credentials to the reader 312 regardless of whether the reader 312 is properly configured. If the credentials provided by the credential device 328 are accepted by the reader 312 (and if the reader 312 is properly configured), then the reader 312 may grant the user 302 access to the protected resource that the reader 312 protects. If the credentials provided by the credential device 328 are not accepted by the reader 312 (or if the reader 312 is not properly configured), then the reader 312 may not grant the user 302 access to the protected resource that the reader 312 protects.

[0110] The exemplary systems and methods of this disclosure have been described in relation to mobile 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.

[0111] 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.

[0112] 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.

[0113] 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.

[0114] 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.

[0115] 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.

[0116] In yet other embodiments, 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.

[0117] 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.

[0118] 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.

[0119] 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.

[0120] 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.

[0121] 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.

[0122] Any of the steps, functions, and operations discussed herein can be performed continuously and automatically.

[0123] Examples of the processors as described herein may include, but are not limited to, at least one of Qualcomm® Snapdragon® 800 and 801, Qualcomm® Snapdragon® 610 and 615 with 4G LTE Integration and 64-bit computing, Apple® A7 processor with 64-bit architecture, Apple® M7 motion coprocessors, Samsung® Exynos® series, the Intel® Core™ family of processors, the Intel® Xeon® family of processors, the Intel® Atom™ family of processors, the Intel Itanium® family of processors, Intel® Core® i5-4670K and i7-4770K 22nm Haswell, Intel® Core® i5-3570K 22nm Ivy Bridge, the AMD® FX™ family of processors, AMD® FX-4300, FX-6300, and FX-8350 32nm Vishera, AMD® Kaveri processors, Texas Instruments® Jacinto C6000™ automotive infotainment processors, Texas Instruments® OMAP™ automotive-grade mobile processors, ARM® Cortex™-M processors, ARM® Cortex-A and ARM926EJ-S™ processors, other industry-equivalent processors, and may perform computational functions using any known or future-developed standard, instruction set, libraries, and/or architecture.

What Is Claimed Is:

1. A configuration reporting method comprising:

obtaining, at a processor, a configuration template from a backend computer system;

storing the configuration template in a computer readable memory;

establishing a communication channel with a reader via a communication interface;

transmitting a signal via the communication channel to update a configuration setting of the reader based on the communication template to yield updated configuration information of the reader;

receiving, at the processor and from the reader via the communication channel, a configuration signature based on the updated configuration information, wherein the configuration signature contains no information about the reader or any configuration setting thereof; and

sending the configuration signature to the backend computer system for verification and storage.

2. The configuration reporting method of claim 1, further comprising:

receiving, at the processor, an indication of whether the configuration setting of the reader has been updated properly.

3. The configuration reporting method of claim 2, further comprising:

based on the indication, selectively sending at least a portion of the updated configuration information to the backend computer system.

4. The configuration reporting method of claim 1, wherein the configuration signature is in the form of a hash, a checksum, a message authentication code based on symmetric encryption, a digital signature based on asymmetric encryption, or any combination thereof.

5. The configuration reporting method of claim 4, wherein a server comprises the processor and the communication interface.

6. The configuration reporting method of claim 1, wherein a mobile device comprises the processor and the communication interface.

7. The configuration reporting method of claim 1, wherein the communication channel is a secure communication channel.

8. The configuration reporting method of claim 1, wherein establishing the communication channel comprises completing an authentication process.

9. The configuration reporting method of claim 1, wherein the configuration setting of the reader comprises one of an authentication requirement, an authorization requirement, an access control requirement; a reader behavior; a reader function; a software update; or a firmware update.

10. A mobile device, comprising:

a user interface;

a reader interface for communicating with an access control reader;

a processor;

a memory storing instructions for execution by the processor, the instructions configured to cause the processor to:

receive, from the access control reader and via the reader interface, information about a configuration setting of the access control reader;

send, to a backend computer system, a signature of the configuration setting; and

receive, from the backend computer system, an indication of whether the signature corresponds to a proper configuration setting.

11. The mobile device of claim 10, wherein the reader interface allows the mobile device to communicate with the access control reader using a wireless communication protocol.

12. The mobile device of claim 10, wherein the instructions stored in the memory are further configured to cause the processor to:

calculate the signature of the configuration setting.

13. The mobile device of claim 10, wherein the instructions stored in the memory are further configured to cause the processor to:

request information from the access control reader about the configuration setting.

14. The mobile device of claim 10, wherein the instructions stored in the memory are further configured to cause the processor to:

download a configuration template from the backend computer system; and

update an initial configuration setting to yield the configuration setting.

15. The mobile device of claim 10, wherein the instructions stored in the memory are further configured to cause the processor to:

send a credential to the access control reader via the reader interface.

16. An access control reader controlling access to a protected resource, comprising:

a communication interface;

a processor; and

a memory storing configurable settings, the memory further storing instructions for causing the processor to:

update the configurable settings based on information received through the communication interface to yield updated configurable settings;

send information corresponding to the updated configurable settings via the communication interface; and

deny access to the protected resource based on a first indication, received via the communication interface, that the updated configurable settings of the access control reader do not match predetermined configurable settings.

17. The access control reader of claim 16, wherein the memory stores additional instructions for causing the processor to:

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

determine whether the credentials is authorized; and

selectively grant access to the protected resource based on the determination and further based on a second indication, received via the communication interface, that the updated configurable settings of the access control reader match predetermined configurable settings.

18. The access control reader of claim 16, wherein the information corresponding to the updated configurable settings is a hash or a checksum of the updated configurable settings.

19. The access control reader of claim 16, wherein the communication interface is a wireless communication interface.

20. The access control reader of claim 16, wherein the configurable settings are associated with at least one of an authentication process, an authorization process, and an access control determination.

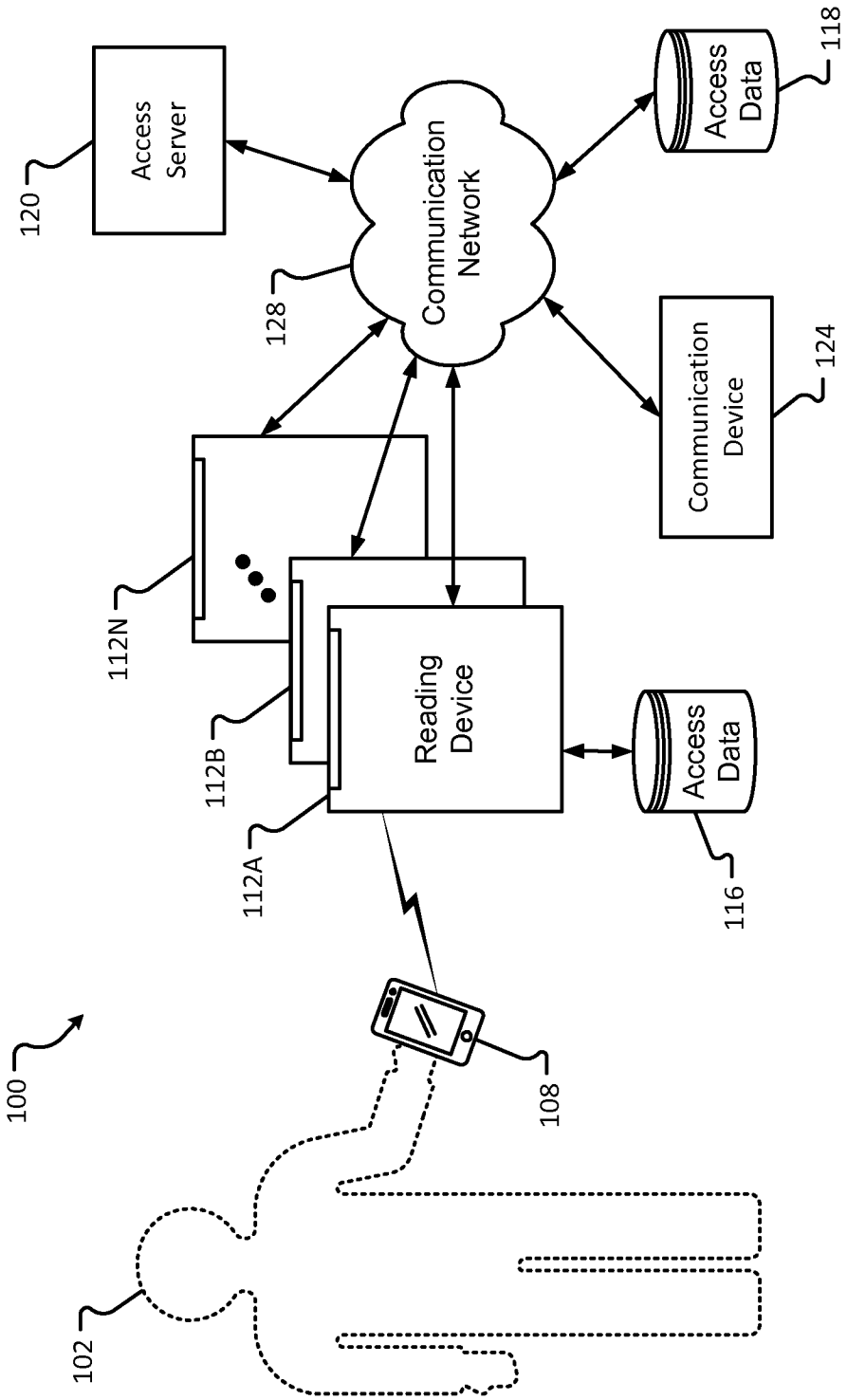
Access Server
120
Communication Network
128
Access Data
118
Communication Device
124
112N
112B
112A
Reading Device
Access Data
116
108
100
102

Fig. 1

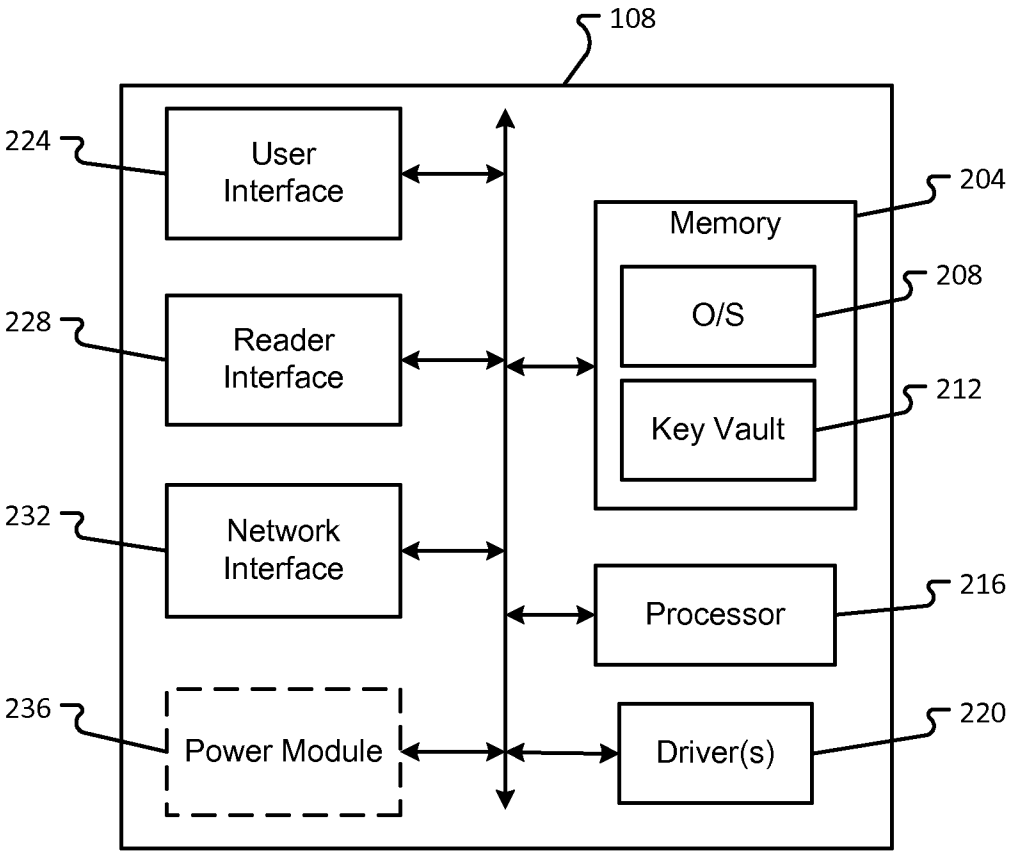
108
224
User Interface
228
Reader Interface
232
Network Interface
236
Power Module
204
Memory
208
O/S
212
Key Vault
216
Processor
220
Driver(s)

Fig. 2

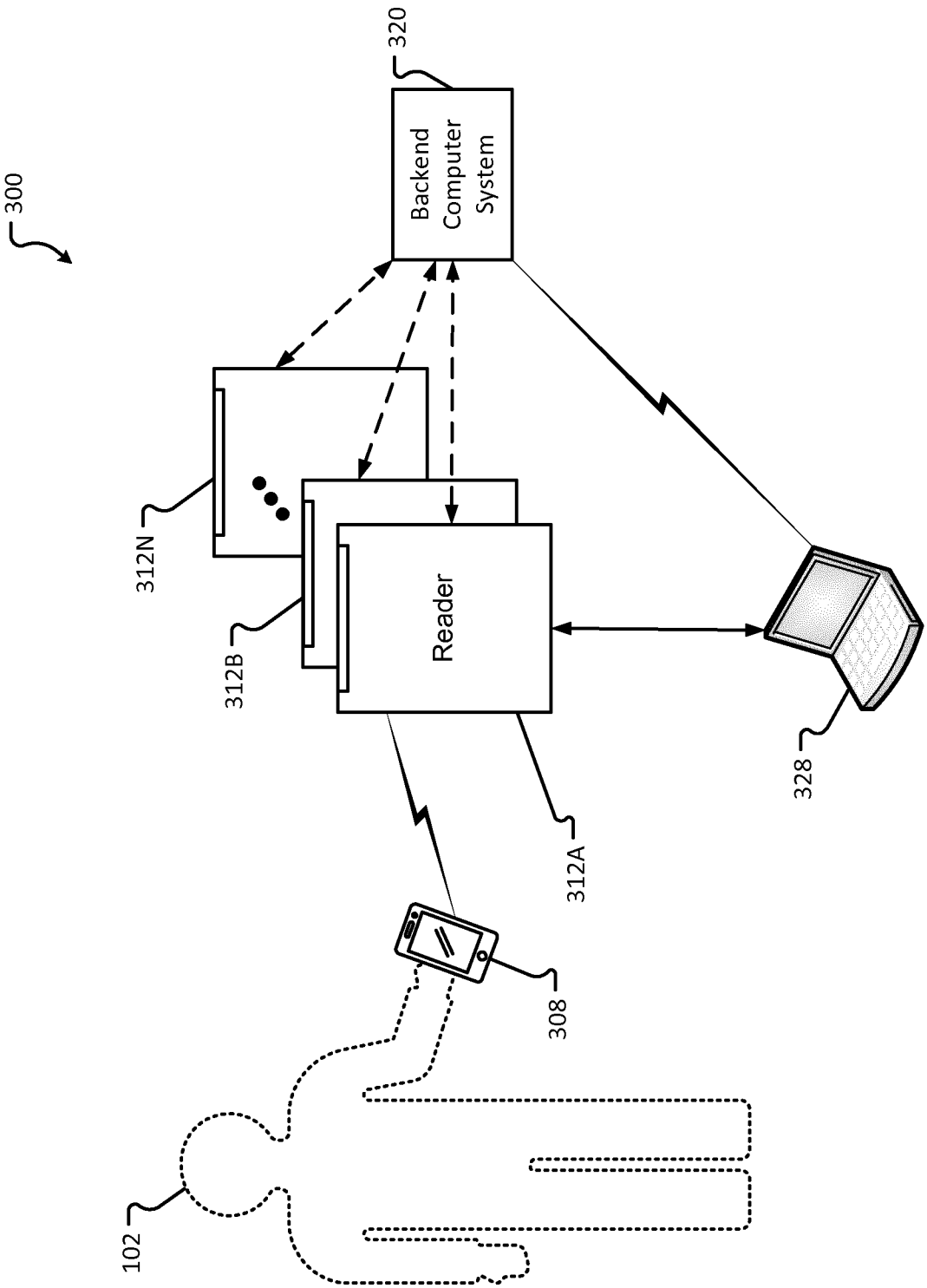
300
320
Backend Computer System
312N
312B
Reader
312A
328
308
102

Fig. 3

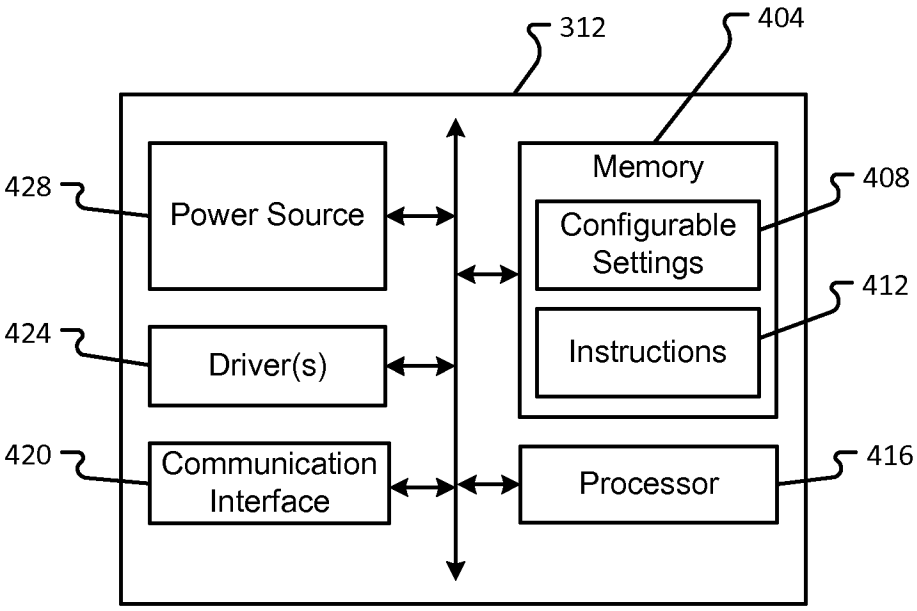
312
404
428
Power Source
Memory
408
Configurable Settings
412
424
Driver(s)
Instructions
420
Communication Interface
Processor
416

Fig. 4

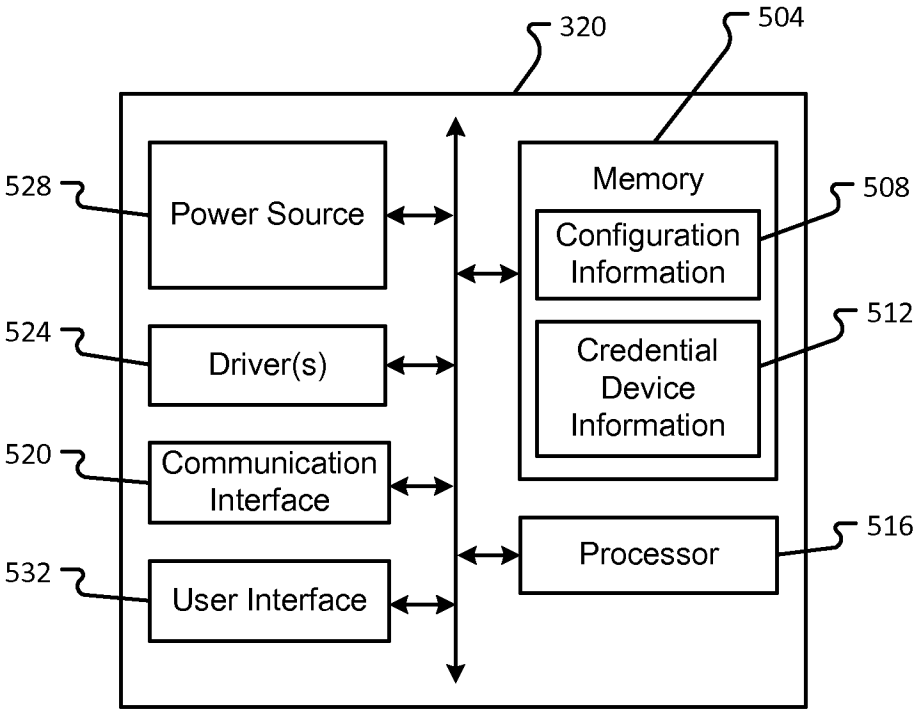
320
504
528
Power Source
Memory
508
Configuration Information
512
524
Driver(s)
Credential Device Information
520
Communication Interface
Processor
516
532
User Interface

Fig. 5

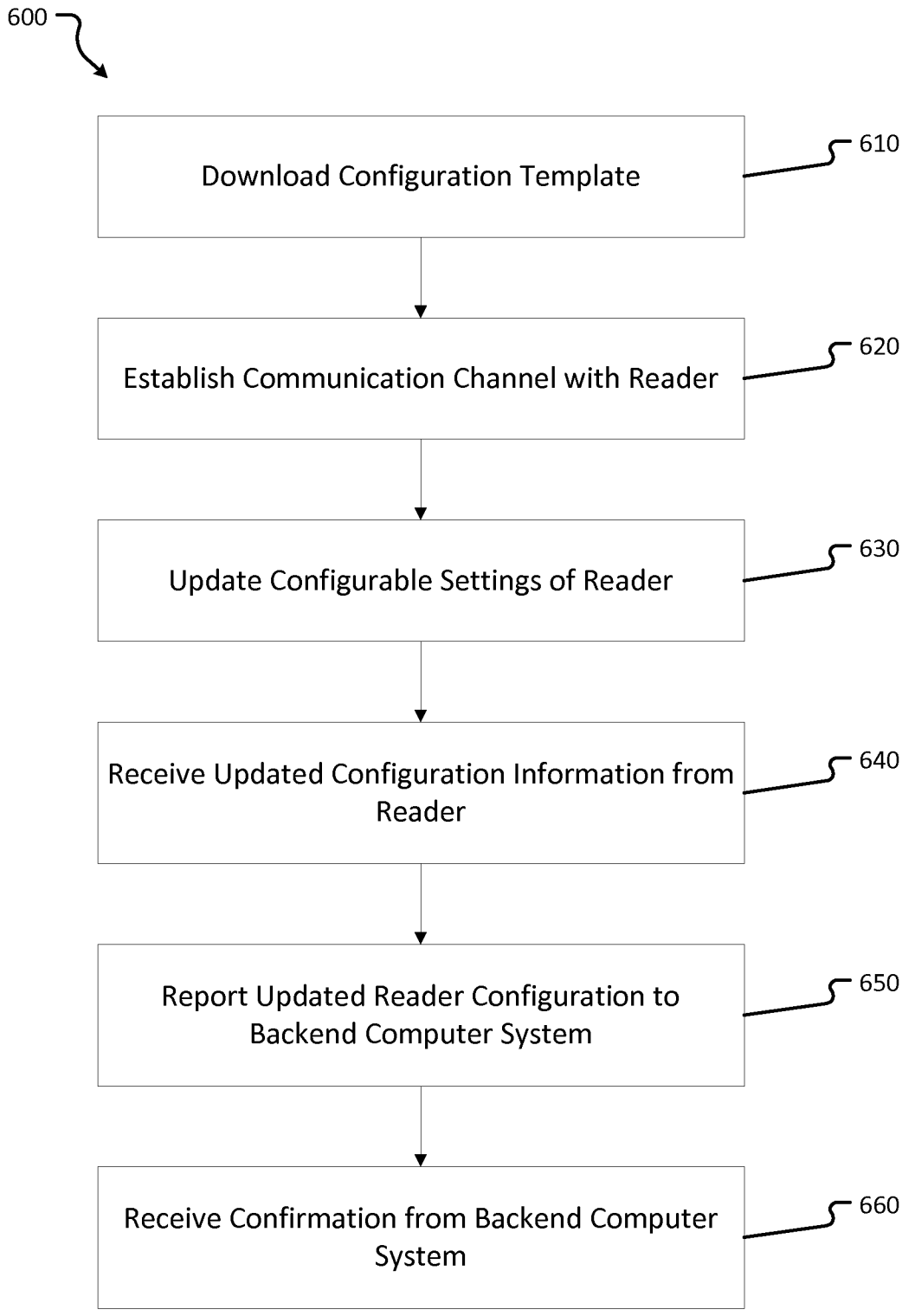
600
Download Configuration Template
610
Establish Communication Channel with Reader
620
Update Configurable Settings of Reader
630
Receive Updated Configuration Information from Reader
640
Report Updated Reader Configuration to Backend Computer System
650
Receive Confirmation from Backend Computer System
660

Fig. 6

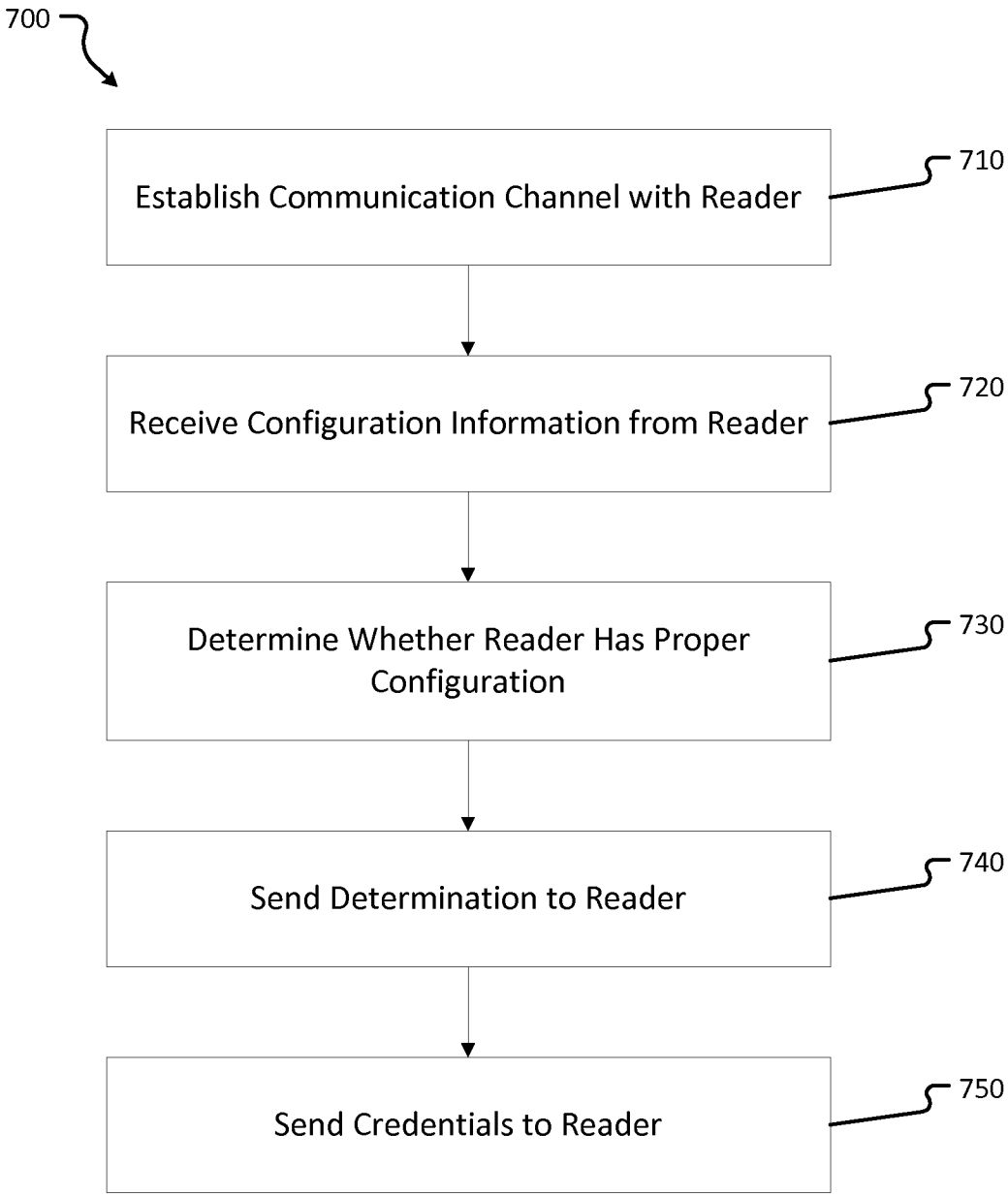
700
Establish Communication Channel with Reader
710
Receive Configuration Information from Reader
720
Determine Whether Reader Has Proper Configuration
730
Send Determination to Reader
740
Send Credentials to Reader
750

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2016/061392

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/061392

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00
ADD.

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)
G07C H04W

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	US 2014/028438 A1 (KUENZI ADAM [US] ET AL) 30 January 2014 (2014-01-30)	1-15
Y	abstract; figures 1,4 paragraphs [0016] - [0052]	16-20
X	US 2012/213362 A1 (BLIDING OLLE [SE] ET AL) 23 August 2012 (2012-08-23)	1-15
Y	paragraphs [0047] - [0052] paragraphs [0062] - [0082]	16-20
X	US 2014/051407 A1 (AHEARN JOHN ROBERT [US] ET AL) 20 February 2014 (2014-02-20)	1-15
A	abstract; figures 1,4 paragraphs [0010] - [0021] paragraphs [0027] - [0044]	16-20

-/--

[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
12 August 2016	22/08/2016

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	Pfyffer, Gregor

4

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

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 2014/052777 A1 (EBERWINE TODD [US] ET AL) 20 February 2014 (2014-02-20)	1-15
A	abstract; figures 1,3 paragraphs [0009] - [0032]	16-20
X	US 2013/318519 A1 (COOLIDGE FRANK L [US]) 28 November 2013 (2013-11-28)	1-15
A	abstract paragraphs [0011] - [0055]	16-20

4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/061392

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014028438 A1	30-01-2014	NONE	
US 2012213362 A1	23-08-2012	EP 2478496 A1	25-07-2012
		SE 0950680 A1	18-03-2011
		US 2012213362 A1	23-08-2012
		WO 2011034482 A1	24-03-2011
US 2014051407 A1	20-02-2014	AU 2013302378 A1	02-04-2015
		EP 2885167 A1	24-06-2015
		NZ 706026 A	26-02-2016
		US 2014051407 A1	20-02-2014
		US 2014051425 A1	20-02-2014
		WO 2014028897 A1	20-02-2014
US 2014052777 A1	20-02-2014	AU 2013302381 A1	02-04-2015
		CA 2886378 A1	20-02-2014
		CN 104798111 A	22-07-2015
		EP 2885168 A1	24-06-2015
		NZ 706032 A	31-03-2016
		US 2014049370 A1	20-02-2014
		US 2014052777 A1	20-02-2014
		WO 2014028900 A1	20-02-2014
US 2013318519 A1	28-11-2013	AU 2013259563 A1	15-01-2015
		CA 2873271 A1	14-11-2013
		EP 2847402 A1	18-03-2015
		US 2013318519 A1	28-11-2013
		US 2016026456 A1	28-01-2016
		WO 2013169887 A1	14-11-2013

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-20

   Configuration reporting

1.1. claims: 1-9

   A configuration reporting method

1.2. claims: 10-15

   A mobile device

1.3. claims: 16-20

   An access control reader
