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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2018 (12.07.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/128754 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/04* (2009.01)
H04W 12/06 (2009.01) *H04W 4/02* (2018.01)
H04W 12/08 (2009.01) *H04L 9/08* (2006.01)
G07C 9/00 (2006.01) *G06Q 50/12* (2012.01)

(21) International Application Number:
PCT/US2017/065682

(22) International Filing Date:
12 December 2017 (12.12.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/444,017 09 January 2017 (09.01.2017) US

(71) Applicant: **CARRIER CORPORATION** [US/US]; 17900 Beeline Highway, Jupiter, Florida 33478 (US).

(72) Inventor: **KUENZI, Adam**; c/o GSP-Supra (UFS), 4001 Fairview Industrial Dr.SE, Salem, Oregon 06032 (US).

(74) Agent: **WISZ, David L.**; Bachman & LaPointe, PC, 900 Chapel Street, Suite 1201, New Haven, Connecticut 06510 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

(54) Title: ACCESS CONTROL SYSTEM WITH LOCAL MOBILE KEY DISTRIBUTION

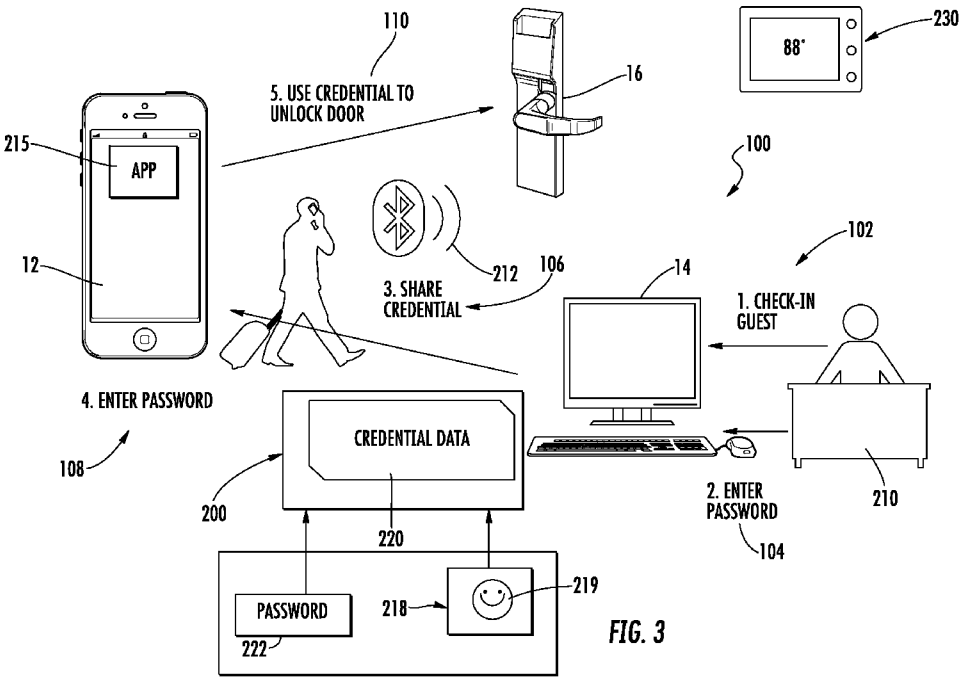


FIG. 3

(57) Abstract: A system includes an application on a mobile device operable to communicate with a local portal, the application is operable to receive a mobile key from the local portal and from that to retrieve a mobile credential for authorizing a user to access an access control. A method of local key distribution can include entering a pre-shared password to a local portal to encrypt a mobile credential; communicating the encrypted mobile credential to an application on the mobile device; and entering the pre-shared password to the application on the mobile device to decrypt the mobile credential.

WO 2018/128754 A1

[Continued on next page]

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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

ACCESS CONTROL SYSTEM WITH LOCAL MOBILE KEY DISTRIBUTION

BACKGROUND

[0001] The present disclosure relates generally to access control systems, and more particularly, to a method of local mobile key distribution.

[0002] A credential service, which can issue mobile credentials (secure, encrypted, verifiable data that encodes access rights) to a mobile device for opening an electronic lock, is usually hosted in a cloud or off-premise location. Sometimes a front desk, or reservation system, or local portal can issue mobile credentials to a mobile device. Credentials are issued after identifying the guest with their account. Usually guests create and manage an account associated to the credential service through a hotel loyalty program.

[0003] Account creation is required so that the front desk can identify the guest in the system and then issue mobile credentials to their account. The guest is identified in the credential service with a unique identifier, with their phone number, or with an email address, for example. This account setup and management process that is required for guest identification also requires relatively complex interactions to manage each guest account. Complex account setup and management processes include initial account setup, account management, password management (change password, expire password, forgot password), account recovery, and account deletion.

SUMMARY

[0004] A system according to one disclosed non-limiting embodiment of the present disclosure can include an application on a mobile device operable to communicate with a local portal, the application is operable to receive a mobile key from the local portal and from that to retrieve a mobile credential for authorizing a user to access an access control.

[0005] A further embodiment of the present disclosure may include the local portal is operable to receive a pre-shared password to encrypt the mobile credential after generating the mobile credential to make a mobile key.

[0006] A further embodiment of the present disclosure may include the application is operable to decrypt the mobile credential from a mobile key in response to entering the pre-shared password into the application.

[0007] A further embodiment of the present disclosure may include generating the mobile credential is performed utilizing a local database of encryption keys.

[0008] A further embodiment of the present disclosure may include generating the mobile credential is performed utilizing a centralized cloud service to which the local portal has access.

[0009] A further embodiment of the present disclosure may include the mobile credential is operable to operate an access control.

[0010] A further embodiment of the present disclosure may include 1 the mobile credential is operable to access a service.

[0011] A further embodiment of the present disclosure may include the service is a thermostat.

[0012] A further embodiment of the present disclosure may include the mobile key is operable to reskin the mobile application.

[0013] A further embodiment of the present disclosure may include the application on the mobile device is operable to communicate with the local portal via at least one of Bluetooth, NFC, email, and SMS text messaging.

[0014] A further embodiment of the present disclosure may include a mobile key card, the mobile key communicated from the mobile key card to the mobile application.

[0015] A further embodiment of the present disclosure may include the mobile key is first communicated from the mobile key card to an access control and from thence to the mobile application.

[0016] A further embodiment of the present disclosure may include a display operable to present an image to be scanned by the mobile device the image is generated based upon the mobile key.

[0017] A method of local key distribution according to one disclosed non-limiting embodiment of the present disclosure can include entering a pre-shared password to a local portal to encrypt a mobile credential; communicating the encrypted mobile credential to an application on the mobile device; and entering the pre-shared password to the application on the mobile device to decrypt the mobile credential.

[0018] A further embodiment of the present disclosure may include entering the pre-shared password includes entering a drive's license number.

[0019] A further embodiment of the present disclosure may include entering the pre-shared password includes entering a confirmation number.

[0020] A further embodiment of the present disclosure may include communicating the encrypted mobile credential includes communicating via Bluetooth.

[0021] A further embodiment of the present disclosure may include communicating the encrypted mobile credential includes communicating via SMS Text messaging.

[0022] A further embodiment of the present disclosure may include communicating the encrypted mobile credential includes communicating via email.

[0023] The foregoing features and elements may be combined in various combinations without exclusivity, unless expressly indicated otherwise. These features and elements as well as the operation thereof will become more apparent in light of the following description and the accompanying drawings. It should be understood, however, the following description and drawings are intended to be exemplary in nature and non-limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] Various features will become apparent to those skilled in the art from the following detailed description of the disclosed non-limiting embodiment. The drawings that accompany the detailed description can be briefly described as follows:

[0025] Figure 1 is a general schematic system diagram of a user authentication system;

[0026] Figure 2 is a block diagram of an electronic lock system;

[0027] Figure 3 is a flowchart for local communication of a credential method according to one embodiment; and

[0028] Figure 4 is a flowchart for local communication of a credential method according to another embodiment;

[0029] Figure 5 is a flowchart for local communication of a credential method according to another embodiment; and

[0030] Figure 6 is a flowchart for local communication of a credential method according to another embodiment.

DETAILED DESCRIPTION

[0031] Figure 1 schematically illustrates a user authentication system 10. The system 10 generally includes a mobile device 12, a local portal 14, and a plurality of access controls 16, schematically illustrated as 16a, 16b, ..., 16n. It should be appreciated that, although particular systems are separately defined in the schematic block diagrams, each or any of the systems may be otherwise combined or separated via hardware and/or software.

[0032] The mobile device 12 is a wireless capable handheld device such as a smartphone device that is operable to communicate with the local portal 14 and the access controls 16 via an application "app" that runs on the smartphone device (also referred to herein as the mobile device 12). The local portal 14 may provide mobile credentials and other data to the mobile device 12, such as firmware or software updates, to be communicated to one or more of the access controls 16. Although the local portal 14 is depicted herein as a single device (for example a computer, a tablet, a phone, or in general a single computing device with inputs and outputs for use by a person to use, generate mobile keys 200, and so forth as described herein), it

should be appreciated that the local portal 14 may alternatively be embodied as a multiplicity of systems, from which the mobile device 12 receives credentials and other data.

[0033] Each access control 16 is a wireless-capable, restricted-access, or restricted-use device such as wireless locks, access control readers for building entry, electronic banking controls, data transfer devices, key dispenser devices, tool dispensing devices, vehicle ignition system, vehicle door lock or compartment lock, and other restricted-use machines. The mobile device 12 submits credentials to the access controls 16, thereby selectively permitting a user to access or activate functions of the access controls 16. A user may, for example, submit a credential to an electromechanical lock to unlock it, and thereby gain access to a restricted area. In another example, a user may submit a credential to an electronic banking control to withdraw funds. In still another example, the user may submit the credential to a unit that dispenses key cards with data associated with or data retrieved from the credential. In yet another example, the user may submit the credential to a unit that enables access to a computer system. The mobile device 12 may store credentials for one or all or other of the examples noted above, and in addition may store a plurality of credentials for each type of application at the same time. Some credentials may be used for multiple access controls 16. For example, a plurality of electronic locks in a facility may respond to the same credential. Other credentials may be specific to a single access control 16.

[0034] With reference to Figure 2, a block diagram of an example electronic lock system 20 includes the access control 16a, the mobile device 12, and the local portal 14. The access control 16a generally includes a lock actuator 22, a lock controller 24, a lock antenna 26, a lock transceiver 28, a lock processor 30, a lock memory 32, a lock power supply 34, a lock

card reader 90 and a credential module 36. The access control 16a is responsive to credentials from the mobile device 12, and may, for example, be the lock of a lockbox, a door lock, or a lock core. Although the present disclosure focuses primarily on credentials for access control, it should be appreciated that other systems wherein credentials are transmitted from a mobile device to an access control so as to identify the user to an online system or validate user access rights or permissions in an offline system will benefit herefrom. Such systems include virtual or electronic banking systems, machine operation systems, dispensing systems, data access systems and computer access systems.

[0035] Upon receiving and authenticating an appropriate credential from the mobile device 12 using the credential module 36, or after receiving card data from lock card reader 90, the lock controller 24 commands the lock actuator 22 to lock or unlock a mechanical or electronic lock. The lock controller 24 and the lock actuator 22 may be parts of a single electronic or electromechanical lock unit, or may be components sold or installed separately.

[0036] The lock transceiver 28 is capable of transmitting and receiving data to and from at least the mobile device 12. The lock transceiver 28 may, for instance, be a near field communication (NFC), Bluetooth, or Wi-Fi transceiver, or another appropriate wireless transceiver. The lock antenna 26 is any antenna appropriate to the lock transceiver 28. The lock processor 30 and lock memory 32 are, respectively, data processing, and storage devices. The lock processor 30 may, for instance, be a microprocessor that can process instructions to validate card data and determine the access rights contained in the card data or to pass messages from a transceiver to a credential module 36 and to receive a response indication back from the credential module 36 with card data. The lock memory 32 may be RAM, EEPROM, or other

storage medium where the lock processor 30 can read and write data including but not limited to lock configuration options and the lock audit trail. The lock audit trail may be a unified audit trail that includes events initiated by accessing the lock via the lock card reader 90 or the mobile device 12. The lock power supply 34 is a power source such as line power connection, a power scavenging system, or a battery that powers the lock controller 24. In other embodiments, the lock power supply 34 may only power the lock controller 24, with the lock actuator 22 powered primarily or entirely by another source, such as user work (e.g. turning a bolt).

[0037] The credential module 36 is in communication with the lock processor 30 and is operable to decrypt and validate a credential to extract virtual card data communicated into the lock controller 24 as a "virtual card read." That is, the access control 16a has essentially two readers, one reader 90 to read a physical key card 92 and the credential module 36 to communicate with the mobile device 12 via the lock processor 30 and the transceiver 28 and antenna 26.

[0038] The mobile device 12 generally includes a key antenna 40, a key transceiver 42, a key processor 44, a key memory 46, a GPS receiver 48, an input device 50, an output device 52, and a key power supply 54. The key transceiver 42 is a transceiver of a type corresponding to the lock transceiver 28, and the key antenna 40 is a corresponding antenna. In some embodiments, the key transceiver 42 and the key antenna 40 may also be used to communicate with the local portal 14. In other embodiments, one or more separate transceivers and antennas may be included to communicate with local portal 14. The key memory 46 is of a type to store a plurality of credentials locally on the mobile device 12.

[0039] With reference to Figure 3, a method 100 is disclosed in terms of functional block diagrams. It should be appreciated that these functions may be enacted in either dedicated hardware circuitry or programmed software routines capable of execution in various microprocessor based electronics control embodiments.

[0040] The method 100 does not require the local portal 14 to identify the guest but does distribute a mobile key 200 to a mobile device 12 in a local manner such as at a property front desk 210 without requiring complex interactions to manage guest accounts. The method 100 permits the local portal 14 to 'encode' the mobile key 200 and deliver the mobile key 200 securely to the mobile device 12 by, for example, Bluetooth 212 directly to their application 215; by email to an email address accessible to the mobile device 12 such that the pertinent mobile key data 200 can be transferred by copy from the email and paste into the application 215; and/or sent by SMS text messages to the mobile device 12 and again copied from the text message and pasted into application 215. In the case of email or SMS, mobile key data 200 may also be transferred into the application 215 utilizing a specialized link that when 'clicked' or is accessed, the mobile device launches application 215 and transfers data 200 into the application. Alternatively, data 200 can be rendered into an image 219 such as QR Code, image, picture, etc. and the application 215 can utilize the mobile device 12 to scan the image 219 that is presented in, for example, a kiosk or screen or display 218 near the front desk 210 and part of or included with the local portal 14. The application 215 can then processes the image 219 to obtain mobile key data 200.

[0041] To securely transfer mobile credential data 220, the data 220 is encrypted (e.g., like an encrypted ZIP file or other encrypted file format) with the pre-shared password 222

such as a driver's license number, property confirmation number, image, credit card number (e.g that was used to pay for the hotel stay), phone number, email address, other piece of pre-shared data or a combination of any of these. Ideally the password 222 is determined based on information shared with the property before the guest's arrival so that the password is not shared when the guest is present at the front desk 210 and when the mobile key 200 is sent from the local portal 14 to the mobile device 12. This encrypted mobile credential data 220 is also called a mobile key 200. By entering the pre-shared password 222 into the application 215, the credential data 220 can be decrypted from mobile key data 200 and can then be utilized.

[0042] Initially, guest check-in (step 102) permits a property manager (i.e. Hotel front desk agent), via standard property tools/methods including centralized reservation systems, property management systems, etc., to check in the guest. That is, the property staff will validate the guest's real identity using standard methods such as manual review of a driver's license or other identification.

[0043] Once the guest is checked in, the pre-shared password 222 is selected from available information and entered (step 104) into the local portal 14. That is, in addition to selecting the guest room and/or indicating standard additional authorizations to include, but not be limited to, parking, pool, etc., the property staff may set the pre-shared password 222. The pre-shared password 222 can be agreed upon at the moment (e.g. use of the drivers license number), based upon a prior known value (e.g. property confirmation number) or other information. The local portal 14 then generates the mobile key data 200 therefrom. This generation can, for example, be performed with a local database of encryption keys and associated access control 16 information for the property to create the credential data 220. These

encryption keys may be of a symmetric form, where each of the local portal 14 and access control 16 have a copy of the same encryption key and a mobile credential data 220 is generated by the local portal 14 and can be verified by the access control 16 based upon knowing the same key. Alternatively, the encryption keys may be of an asymmetric form where, for example, the local portal 14 may hold a private key that is used to construct a mobile credential data 220 that may be verified by the access control 16 based upon knowing the corresponding public key. Further, as is well known to those skilled in the art, the credential data 220 may be composed of multiple credentials that may also include certificates that can create a chain of trust where the local portal 14 has a public/private key pair that is declared as trust-worthy by a certifying party who holds a certifying private key. If the access control 16 knows the certifying public key, it can verify a certificate declaring the local portal 14 public key as trustworthy. Verifying a certificate is done by using the encryption key to verify the digital signature of the certificate where the signature would only be verifiable if the contents of the certificate have not changed. Then, after verifying the local portal 14 public key is trustworthy, the access control can additionally verify that the credential data 220 is valid by using the local portal 14 public key. The aforementioned example outlines how one certifier could vouch for the local portal, but those skilled in the art a chain or hierarchy of certifiers can be created where one certifier vouches for another until finally the last has vouched for the local portal. As long as the access control 16 has the root public key, the whole chain of certificates can be traversed and verified. Alternatively, instead of generating the credential data 200 locally, the local portal 14 can access another service, for example hosted in the cloud or on a secure network, to request to generate the mobile credential data 220. The credential data 220 is then encrypted with the pre-shared

password 222 resulting in the mobile key data 200, which can then be made available for the guest and their appropriately designated access control 16. The credential data 220 can include, for example, data such as:

[0044] a. Credential data for authorizing guest to open the associated guest room access control, including but not limited to the same data that would be encoded onto a physical plastic magnetic strip or RFID card.

[0045] b. Credential data for other access points such as required for wi-fi network access, other access control systems (for example, a badge id), or authentication information for use with credential module 36 which is required for credential module 36 to validate, decrypt and retrieve credential data to open the associated guest room access control.

[0046] c. Logos, pictures, URLs, or other data that can be utilized to 'reskin' or customize the visual look of the mobile application 215 as displayed on the mobile device 12 such as for a particular property. This 'reskin' may happen after the mobile key data 200 has been received by the mobile app 215 and the data has been decrypted with password 222, or it may happen on receiving mobile key data 200 if parts of the 'reskin' data is included with mobile key data 200 but is not encrypted with password 222. Further, the 'reskin' may happen when the mobile key data 200 is loaded in combination with determining the current location of the mobile device 12 (for example, GPS coordinates) a determination that the mobile device must be at a property (e.g. Hotel) that is at that location and the 'reskin' data is retrieved separately from a public location (for example a Hotel website).

[0047] d. Remote programming data for an access control 16 such as the guest door lock to change a programmable parameter (for example to change encryption keys, to update a

time table, to correct a real time clock, or any other typical access control parameter). This remote programming data may be sent to the access control 16 by the application 215 without knowledge of the guest and may be part of a lock management system method of using a 'sneaker net.'

[0048] e. Credential data for authenticating other services (e.g. a thermostat 230 in the guest room).

[0049] Next, the mobile key data 200 is shared (step 106). That is, the mobile key data 200 is sent to the mobile device 12 from the local portal 14 directly, without routing through a cloud hosted credential service. Additionally, a guest can share their mobile key data 200 along with their pre-shared password 222, such that the credential 220 can be additionally transferred to another mobile device 12. The guest can send the same mobile key data 200 and password 222 as provided by the local portal 14, or they can use the app 215 to re-encrypt credential data 220 into a separate mobile key data 200 and with a different password 222. The mobile key data 200 can be shared from one mobile device 12 to another mobile device 12 using the same methods that the local portal 14 uses for local distribution. For example, a guest can email the data 200 to a friend. Or they could send it via SMS. Or their phone could present a picture or image 219 that their friend's mobile device 12 could view/receive with use of a camera on the friend's device. This provides an efficient way of distributing the credential data 220 locally to a friend without requiring account management or other cloud services.

[0050] In detail, there are several methods to share the mobile key 200:

[0051] a. Bluetooth: In this embodiment, the local portal 14 is utilized to send the mobile key 200 to the application 215 directly on the mobile device 12 via Bluetooth. In the

application 215, the guest can select a feature such as 'get my key' and/or the property staff would select a feature on the local portal 14 to 'send key.' Once activated, the local portal 14 and mobile device 12 would discover each other, establish a Bluetooth connection, and transfer mobile key 200 from the local portal 14 to the application 215 on the mobile device 12.

[0052] b. Email: In this embodiment, the local portal 14 is utilized to send the mobile key 200 to an email address as a file attachment. Once received, the file attachment could then be copy/pasted into the application 215. This can also be performed by associating a particular file type with the associated application 215 so that when the file is 'opened' from the email client on the mobile device 12, the application 215 is launched. Alternatively, the mobile key 200 could be sent as a pre-formatted link in the email. The guest clicking on the link would activate the link and encoded in the link is contained the mobile key 200 and the mobile device would identify and launch the application 215 utilizing information encoded in the link identifying the application 215.

[0053] c. SMS: In this embodiment, the local portal 14 is utilized to send the mobile key 200 as a text message to the mobile device 12 as per the email embodiment.

[0054] d. Image: In this embodiment, the mobile app 215 can utilize a camera or scanner on the mobile device 12 to scan an image 219 presented on a display that is part of or associated with local portal 14 such as a kiosk 218 adjacent to the front desk 210. Scanning the image 219 allows the mobile device 12 to receive the mobile key 200 after the app 215 processes the image to retrieve the data.

[0055] e. NFC: In this embodiment, the mobile app 215 utilizes Near Field Communication (NFC) capability of the mobile device 12 to transfer the mobile key 200 from

the local portal 14. NFC can operate in several modes and this embodiment could be used with any of the 3 modes. The mobile device 12 and local portal 14 could transfer the mobile key 200 in peer-to-peer mode. Or, they could transfer the mobile key 200 by the mobile device 12 reading a 'virtual card' from a reader device attached to the local portal 14 that emulates an ISO14443 data card that appears to mobile device 12 as a physical card. Or, the local portal 14 could operate in 'reader/writer' mode and write an ISO14443 card image to the mobile device with is emulating an ISO14443 data card. In all cases, the data is transferred using NFC from the local portal 14 to the mobile device 12 and mobile app 215.

[0056] This local compunction may, by including sending data from the application 215 back to the local portal 14, provide for the communication of guest preferences or control data to the front desk 210. This enhances the guest experience, for example, to communicate their preference for soft pillows, no wake up calls, etc. That is, the application 215 on the mobile device 12 may include preference selections that are communicated through the local portal 14 back to the front desk 210. This sending of such preferences data may be part of a response back to the local portal 14 confirming receipt of mobile key data 200. Or, this preferences data may be sent any time upon request of front desk 210 and by the guest activating a feature in the mobile app 215 to effect the process of sending preferences data back to the front desk.

[0057] Once the mobile key 200 is received in the application 215, the guest then enters the pre-shared password 222 to decrypt, the mobile key 200 (step 108). This decrypts the credential data 220 and stores into the application 215 so that the credential data can be used to operate the appropriate access control 16.

[0058] Finally, the credential data 220 is utilized by the mobile device 12 to provide access to the associated access controls 16 (step 110). The credential data 220 is then resident on the mobile device 12 and the user can then operate the appropriate access control 16 in an offline mode at any later time.

[0059] With reference to Figure 4, in another embodiment of the method 100A, residential home access is affected by opening a residential door lock 16 with a home owner's mobile device 12. The method of delivering the key to the phone is associated with the original purchase and installation of the access control 16. That is, the pre-shared password 222 in this embodiment may be associated with the printed packaging of the access control, provided on a sales receipt, and/or otherwise communicated to the homeowner. The residential door lock 16 could itself then send (e.g., over Bluetooth) a mobile key 200 that is encrypted with this pre-shared password. The homeowner can then enter the pre-shared password 222 into the app 215 and activate the mobile key 200. The sending of the mobile key 200 may be done only in a manner that the homeowner can activate, for example by pushing a button on the 'secure' side of the lock when it is unmounted from a door and in a sense this causes the door lock 16 to operate momentarily as a local portal 14 and send the mobile key 200.

[0060] With reference to Figure 5, in another embodiment of the method 100B, the access control 16 can be paired with an intrusion system, which is the sender of the mobile key. In this case, the intrusion system acts as local portal 14. The pre-shared password 222 is then entered into or retrieved from the intrusion system. Alternatively, the pre-shared password 222 is displayed on the intrusion panel display and entered into the application 215.

[0061] With reference to Figure 5, in another embodiment of the method 100C, the guest is issued a mobile key card at the front desk that is associated with a pre-shared password for a use with a particular access control 16. The pre-shared password would be entered when the mobile key card is encoded with a mobile key 200. After inserting the mobile key card into the access control 16, the mobile key 200 is loaded from the card and then sent (for example, by Bluetooth) from the access control 16 into the application 215 on the mobile device 12 of the guest. The pre-shared password that was encoded on the mobile key card is then entered into the application 215 to decrypt the credential 220. Alternatively, if the mobile device 12 supports the capability, the mobile key card can be read directly by the mobile device 12 to retrieve the mobile key data 200, for example if the mobile device 12 supports reading an RFID card using NFC.

[0062] The local credential distribution does not require a centralized service to be used by the mobile device 12 without requiring complex account management or cloud services. The mobile key 200 is secured by the pre-shared password 222 and the user does not need to manage yet another account and associated password. The property also does not need a cloud service or be required to pay a subscription fee to provide more streamlined operations. The elements described and depicted herein, including in flow charts and block diagrams throughout the figures, imply logical boundaries between the elements. However, according to software or hardware engineering practices, the depicted elements and the functions thereof may be implemented on machines through computer executable media having a processor capable of executing program instructions stored thereon as a monolithic software structure, as standalone software modules, or as modules that employ external routines, code, services, and so forth, or

any combination of these, and all such implementations may be within the scope of the present disclosure.

[0063] The use of the terms "a," "an," "the," and similar references in the context of description (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless otherwise indicated herein or specifically contradicted by context. The modifier "about" used in connection with a quantity is inclusive of the stated value and has the meaning dictated by the context (e.g., it includes the degree of error associated with measurement of the particular quantity). All ranges disclosed herein are inclusive of the endpoints, and the endpoints are independently combinable with each other.

[0064] Although the different non-limiting embodiments have specific illustrated components, the embodiments of this invention are not limited to those particular combinations. It is possible to use some of the components or features from any of the non-limiting embodiments in combination with features or components from any of the other non-limiting embodiments.

[0065] It should be appreciated that like reference numerals identify corresponding or similar elements throughout the several drawings. It should also be appreciated that although a particular component arrangement is disclosed in the illustrated embodiment, other arrangements will benefit herefrom.

[0066] Although particular step sequences are shown, described, and claimed, it should be understood that steps may be performed in any order, separated or combined unless otherwise indicated and will still benefit from the present disclosure.

[0067] The foregoing description is exemplary rather than defined by the limitations within. Various non-limiting embodiments are disclosed herein, however, one of ordinary skill in the art would recognize that various modifications and variations in light of the above teachings will fall within the scope of the appended claims. It is therefore to be understood that within the scope of the appended claims, the disclosure may be practiced other than as specifically described. For that reason the appended claims should be studied to determine true scope and content.

CLAIMS

What is claimed:

1. A system, comprising:

a local portal; and

an application on a mobile device operable to communicate with the local portal, the application is operable to receive a mobile key from the local portal and from that to retrieve a mobile credential for authorizing a user to access an access control.

2. The system as recited in claim 1, wherein the local portal is operable to receive a pre-shared password to encrypt the mobile credential after generating the mobile credential to make the mobile key.

3. The system as recited in claim 2, wherein the application is operable to decrypt the mobile credential from the mobile key in response to entering the pre-shared password into the application.

4. The system as recited in claim 2, wherein generating the mobile credential is performed utilizing a local database of encryption keys.

5. The system as recited in claim 2, wherein generating the mobile credential is performed utilizing a centralized cloud service to which the local portal has access.

6. The system as recited in claim 1, wherein the mobile credential is operable to operate an access control.

7. The system as recited in claim 1, wherein the mobile credential is operable to access a service.

8. The system as recited in claim 7, wherein the service is a thermostat.

9. The system as recited in claim 1, wherein the mobile key is operable to reskin the mobile application.

10. The system as recited in claim 1, wherein the application on the mobile device is operable to communicate with the local portal via at least one of Bluetooth, NFC, email, and SMS text messaging.

11. The system as recited in claim 1, further comprising a mobile key card, the mobile key communicated from the mobile key card to the mobile application.

12. The system as recited in claim 11, wherein the mobile key is first communicated from the mobile key card to an access control and from thence to the mobile application.

13. The system as recited in claim 1, further comprising a display operable to present an image to be scanned by the mobile device, wherein the image is generated based upon the mobile key.

14. A method of local key distribution, the method comprising:

entering a pre-shared password to a local portal to encrypt a mobile credential;

communicating the encrypted mobile credential to an application on a mobile device; and entering the pre-shared password to the application on the mobile device to decrypt the mobile credential.

15. The method as recited in claim 14, wherein entering the pre-shared password includes entering a drive's license number.

16. The method as recited in claim 14, wherein entering the pre-shared password includes entering a confirmation number.

17. The method as recited in claim 14, wherein communicating the encrypted mobile credential includes communicating via Bluetooth.

18. The method as recited in claim 14, wherein communicating the encrypted mobile credential includes communicating via SMS Text messaging.

19. The method as recited in claim 14, wherein communicating the encrypted mobile credential includes communicating via email.

20. The method as recited in claim 14, wherein entering the pre-shared password to the local portal occurs at check in.

21. The method as recited in claim 14, further comprising communicating with the local portal to indicate a guest preference in response to communicating the encrypted mobile credential to the mobile device.

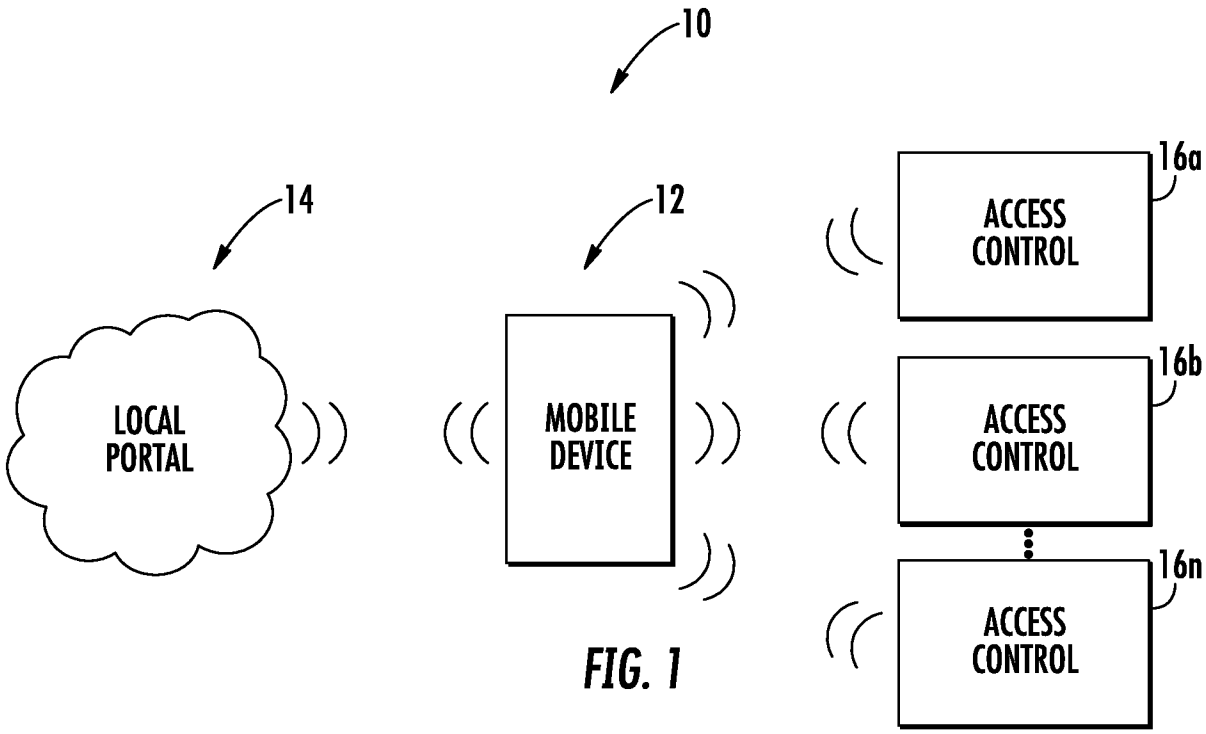

10
14
12
16a
ACCESS CONTROL
LOCAL PORTAL
MOBILE DEVICE
16b
ACCESS CONTROL
16n
ACCESS CONTROL

FIG. 1

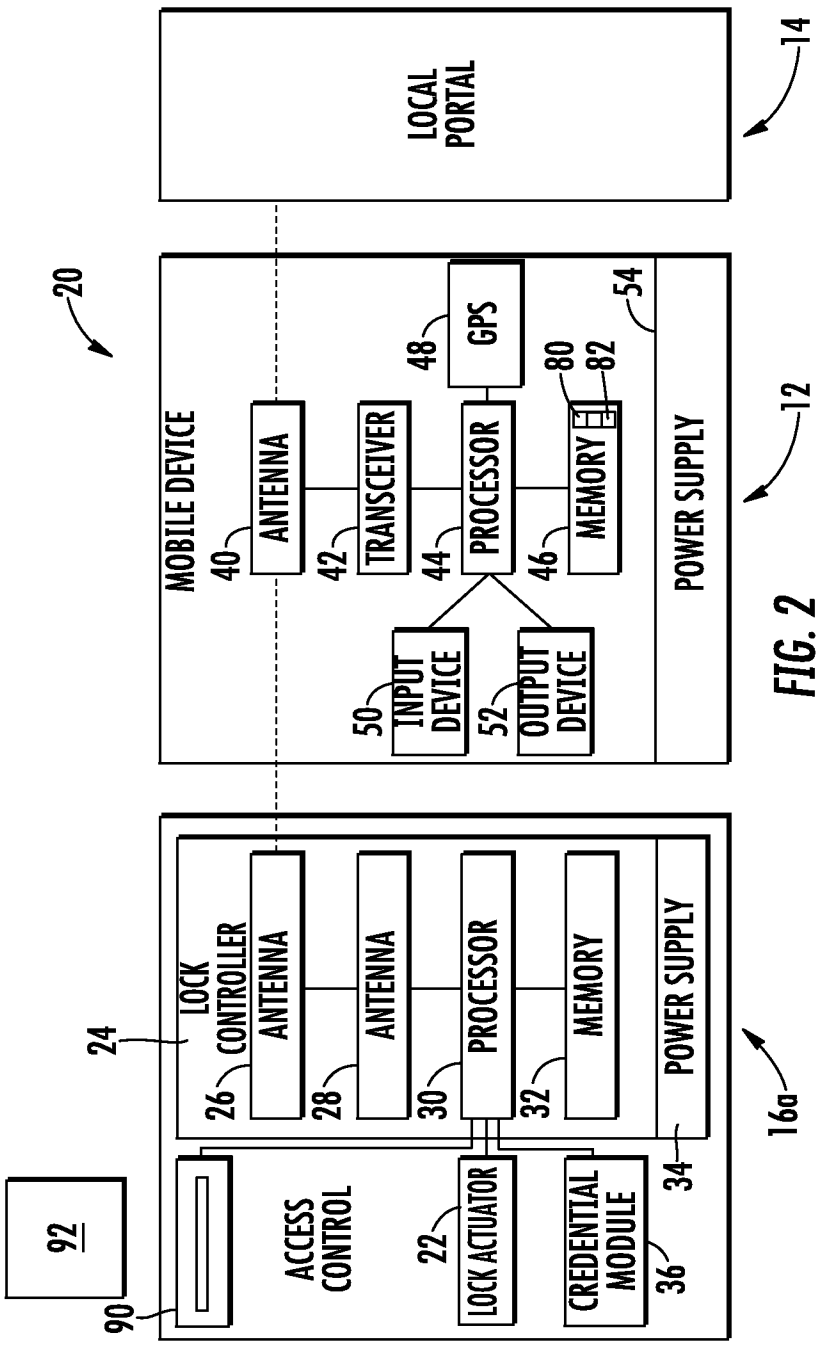

LOCAL PORTAL
14
20
MOBILE DEVICE
ANTENNA
40
TRANSCEIVER
42
PROCESSOR
44
MEMORY
46
GPS
48
80
82
INPUT DEVICE
50
OUTPUT DEVICE
52
POWER SUPPLY
54
12
LOCK CONTROLLER
24
ANTENNA
26
ANTENNA
28
PROCESSOR
30
MEMORY
32
POWER SUPPLY
34
16a
92
90
ACCESS CONTROL
LOCK ACTUATOR
22
CREDENTIAL MODULE
36

FIG. 2

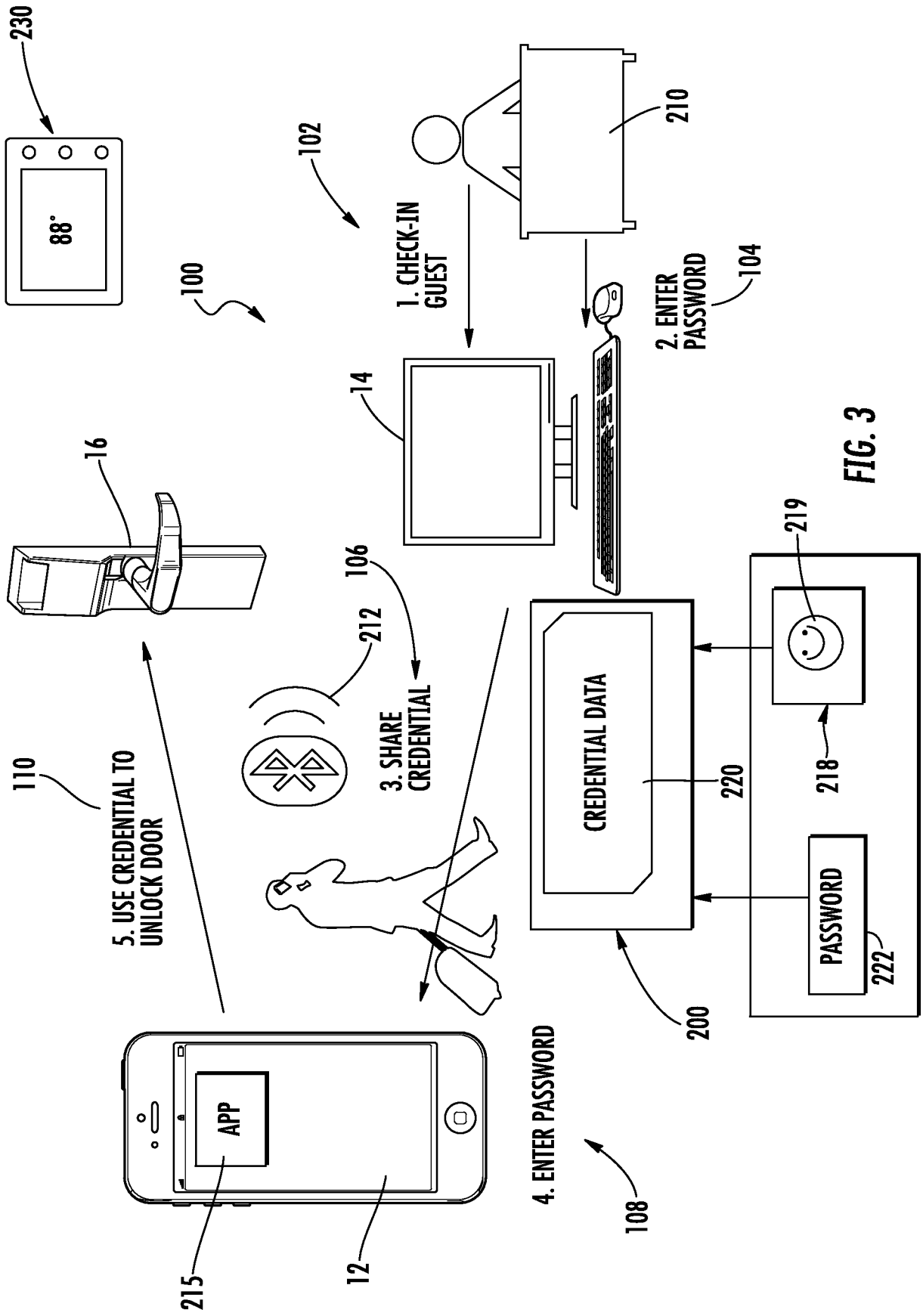

230
88°
102
100
1. CHECK-IN GUEST
210
2. ENTER PASSWORD
104
14
16
106
212
3. SHARE CREDENTIAL
110
5. USE CREDENTIAL TO UNLOCK DOOR
CREDENTIAL DATA
220
219
218
PASSWORD
222
200
4. ENTER PASSWORD
108
APP
215
12

FIG. 3

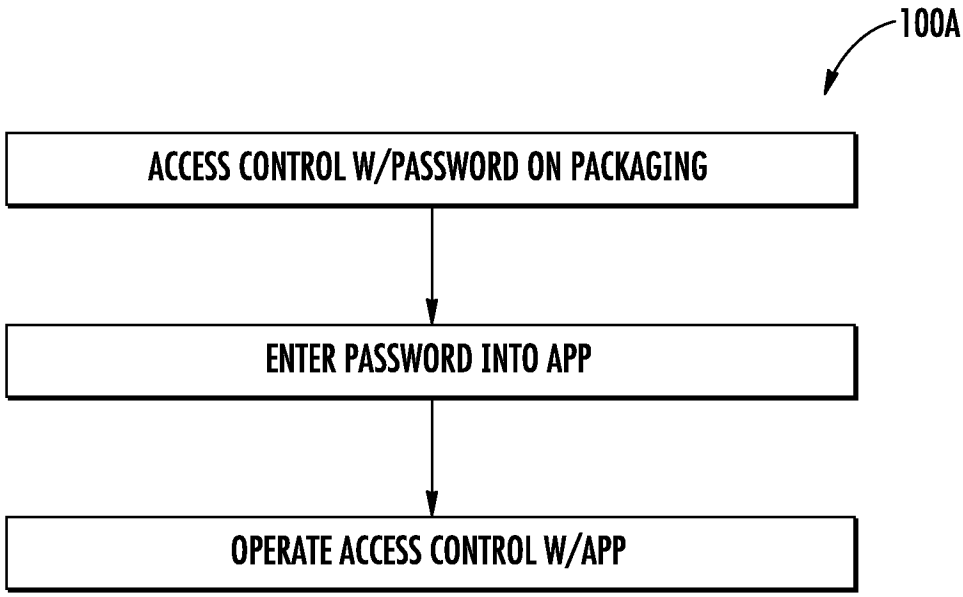

100A
ACCESS CONTROL W/PASSWORD ON PACKAGING
ENTER PASSWORD INTO APP
OPERATE ACCESS CONTROL W/APP

FIG. 4

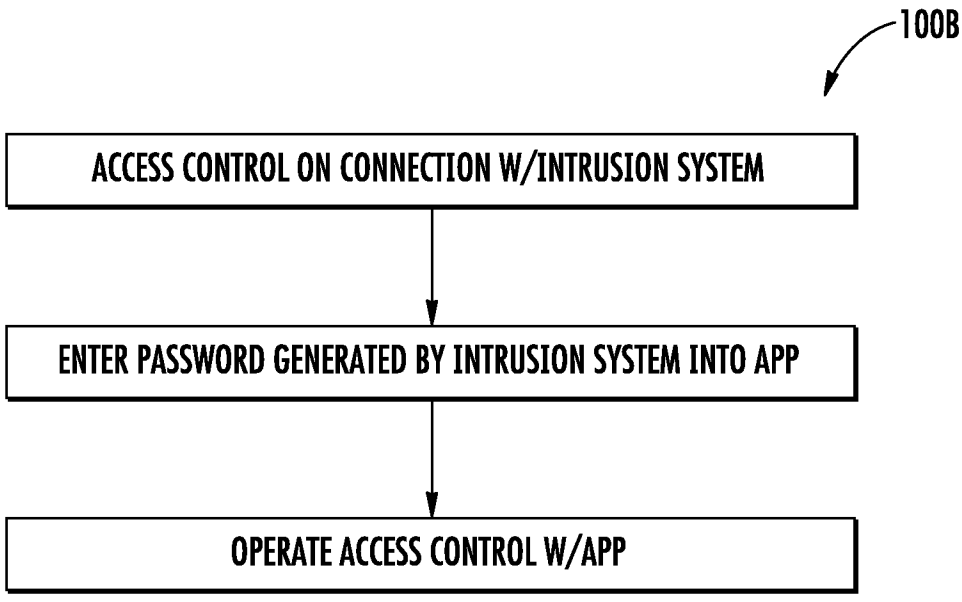

100B
ACCESS CONTROL ON CONNECTION W/INTRUSION SYSTEM
ENTER PASSWORD GENERATED BY INTRUSION SYSTEM INTO APP
OPERATE ACCESS CONTROL W/APP

FIG. 5

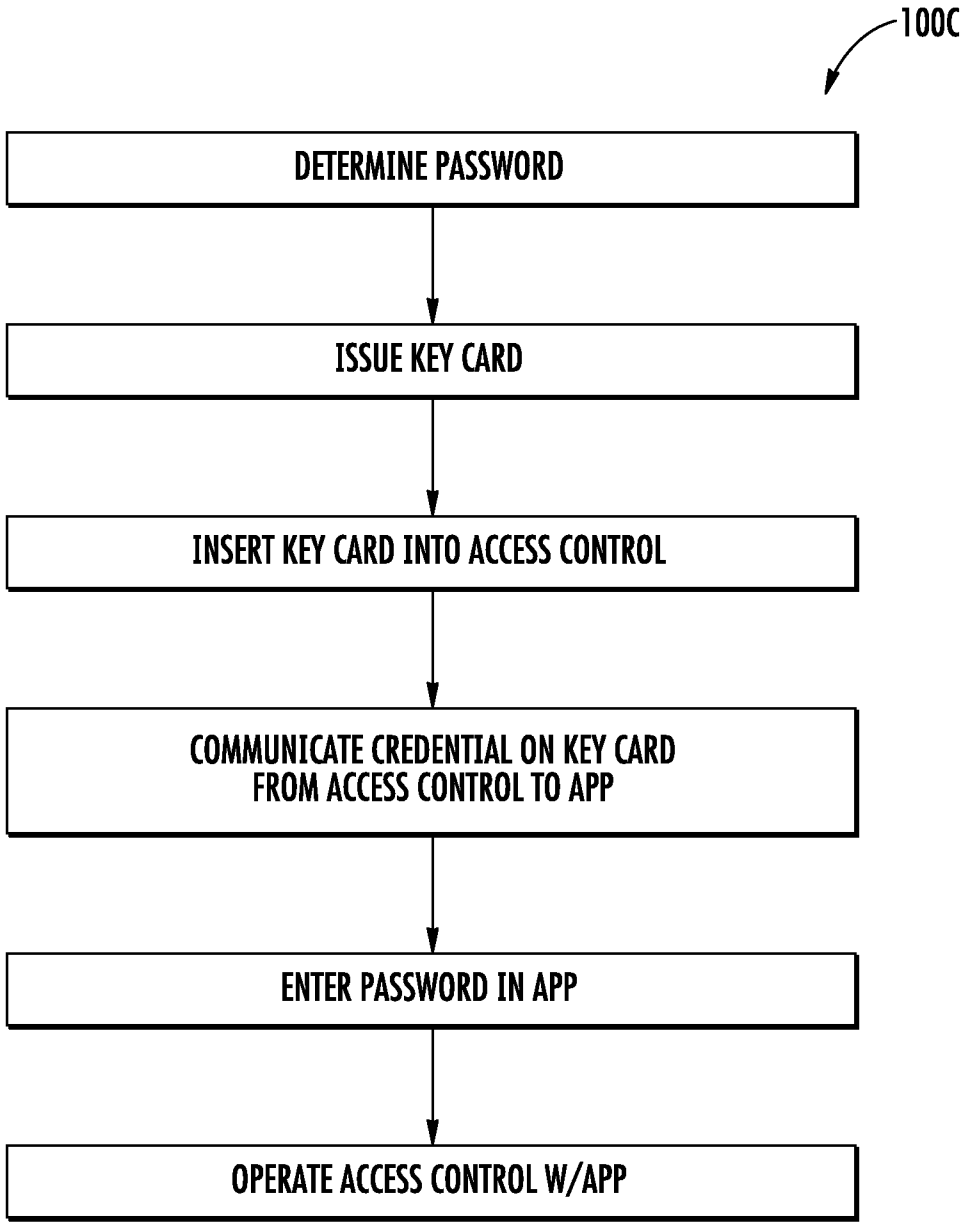

100C
DETERMINE PASSWORD
ISSUE KEY CARD
INSERT KEY CARD INTO ACCESS CONTROL
COMMUNICATE CREDENTIAL ON KEY CARD FROM ACCESS CONTROL TO APP
ENTER PASSWORD IN APP
OPERATE ACCESS CONTROL W/APP

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/065682

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06 H04W12/08 G07C9/00 H04W12/04
H04W4/02 H04L9/08 G06Q50/12
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 H04L H04W G06Q

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, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 3 062 295 A1 (ASSA ABLOY AB [SE]) 31 August 2016 (2016-08-31) paragraph [0006] paragraph [0021] - paragraph [0025] paragraph [0028] paragraph [0033] - paragraph [0035] paragraph [0039] paragraph [0044] - paragraph [0048] paragraph [0052] - paragraph [0053] figure 1 -----	1-21
X	US 2014/219453 A1 (NEAFSEY JEFFREY SCOTT [US] ET AL) 7 August 2014 (2014-08-07) paragraph [0011] paragraph [0031] - paragraph [0034] paragraph [0042] paragraph [0049] - paragraph [0051] paragraph [0059] - paragraph [0065] ----- -/--	1-21

[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
8 March 2018	16/03/2018

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	Cankaya, Sukru

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/065682

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012/046096 A1 (MORRISON JAMES [US] ET AL) 23 February 2012 (2012-02-23) paragraph [0072] paragraph [0089] -----	9
A	US 9 397 980 B1 (CHEN GANG [US]) 19 July 2016 (2016-07-19) column 3, line 64 - column 4, line 60 -----	1,2, 14-16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/065682

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3062295 A1	31-08-2016	EP 3062295 A1	31-08-2016
		US 2016249159 A1	25-08-2016
US 2014219453 A1	07-08-2014	CA 2926206 A1	14-08-2014
		US 2014219453 A1	07-08-2014
		US 2016227593 A1	04-08-2016
		WO 2014124300 A1	14-08-2014
US 2012046096 A1	23-02-2012	US 2012046096 A1	23-02-2012
		WO 2013036655 A2	14-03-2013
US 9397980 B1	19-07-2016	US 9397838 B1	19-07-2016
		US 9397980 B1	19-07-2016
		US 9730065 B1	08-08-2017