(12) STANDARD PATENT (11) Application No. **AU 2006343377 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
System and method for remotely assigning and revoking access credentials using a near field communication equipped mobile phone

(51) International Patent Classification(s)
H04W 24/00 (2009.01)

(21) Application No: **2006343377** (22) Date of Filing: **2006.04.20**

(87) WIPO No: **WO07/130006**

(30) Priority Data

(31) Number	(32) Date	(33) Country
11/397,542	**2006.04.03**	**US**

(43) Publication Date: **2007.11.15**
(44) Accepted Journal Date: **2011.02.24**

(71) Applicant(s)
Assa Abloy AB

(72) Inventor(s)
Lowe, Peter R.

(74) Agent / Attorney
Allens Arthur Robinson Patent & Trade Marks Attorneys, Level 27 530 Collins Street, Melbourne, VIC, 3000

(56) Related Art
US 2003/0023874
US 6895234
US 2004/0180646
US 5903845

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/130006 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/015304

(22) International Filing Date: 20 April 2006 (20.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/397,542 3 April 2006 (03.04.2006) US

(71) Applicant *(for all designated States except US)*: **ASSA ABLOY IDENTIFICATION TECHNOLOGY GROUP AB** [SE/SE]; Box 70340, S-107 23 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LOWE, Peter, R.** [US/US]; 16380 Falcon Highway, Peyton, Colorado 80831-7993 (US).

(74) Agents: **BLAKELY, Todd, P.** et al.; SHERIDAN ROSS P.C., 1560 Broadway, Suite 1200, Denver, Colorado 80202-5141 (US).

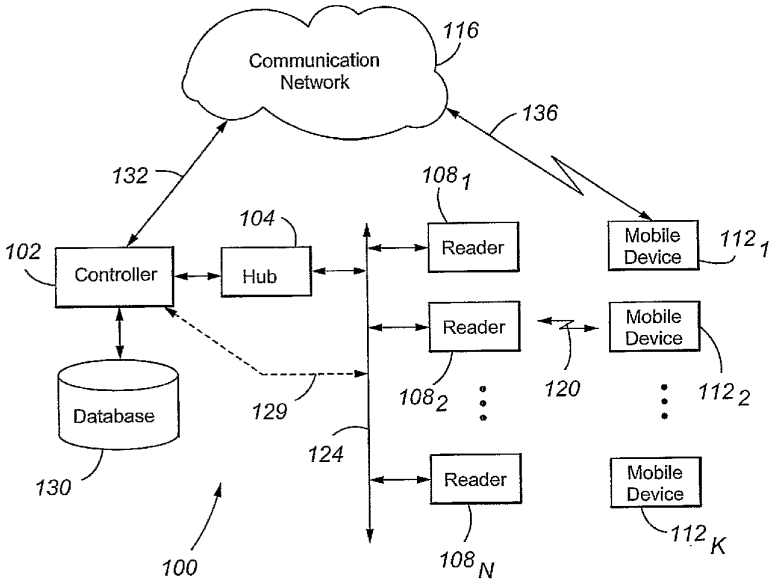
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEM AND METHOD FOR REMOTELY ASSIGNING AND REVOKING ACCESS CREDENTIALS USING A NEAR FIELD COMMUNICATION EQUIPPED MOBILE PHONE



(57) **Abstract:** The present invention is generally directed toward a mobile device that can be used in a secure access system. More specifically, the mobile device can have credential data loaded thereon remotely updated, enabled, disabled, revoked, or otherwise altered with a message sent from, for example, a control panel and/or controller in the system.

WO 2007/130006 A2

SYSTEM AND METHOD FOR REMOTELY ASSIGNING AND REVOKING ACCESS CREDENTIALS USING A NEAR FIELD COMMUNICATION EQUIPPED MOBILE PHONE

FIELD OF THE INVENTION

The invention is directed generally to using mobile devices in an access control system. Specifically, a mobile device utilizing near field communications protocol (NFC) may be used for controlling access to assets, places, or things by having access credentials remotely assigned and revoked.

BACKGROUND OF THE INVENTION

The following discussion of documents, acts, materials, devices, articles and the like is included in the specification solely for the purpose of providing a context for the present invention. It is not suggested or represented that any or all of these matters formed part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed in Australia before the priority date of each claim of this application.

Radio frequency IDs (RFIDs), like contactless smart cards, store credential information that can be used later 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 the credential information on the smart card is valid then the reader/interrogator sends the initiates any number of actions allowing the holder of the smart card access to a particular asset.

NFC is a communication method that is showing great promise for communication between devices at short range. NFC may be regarded as the same protocol that is used by contactless smart cards working at 13.56MHz. Several companies are in the process of announcing mobile phones that incorporate an NFC chip. The communication protocol of a typical NFC chip can be seen for instance in *Short Form Specification of the PN511-Transmission module, February 2004* from Philips Semiconductors, which is herein incorporated by reference in its entirety.

The protocol used in NFC can vary depending on the mode that the chip and reader/ interrogator are in. For example, if an active NFC mode is used, both a reader/ interrogator and target are using their own radio frequency (RF) field to enable

communication between each other. A reader/interrogator is powered to generate an RF filed of a particular frequency, for instance at 13.56MHz. The target has its own power supply for digital processing and communications. When the target receives a communication from a reader/interrogator, the target uses its own power supply to generate another RF field to answer the reader/interrogator. Communications can occur back and

forth between the reader/interrogator and target. Alternatively, if a passive NFC mode is implemented, the target answers to a reader/interrogator command in a load modulation scheme. The target is not powered to generate its own RF field. Rather, the target uses energy from the RF created by the reader/interrogator to create its RF field and reply to be sent back to the reader/interrogator.

If the NFC chip is coupled with a micro-processor, the chip may act like smart cards or the like where communication between a reader and card are performed to gain access to an asset. Typically a mobile phone includes a battery and the NFC chip can be powered by that battery. If the chip derives power from the mobile phone battery, the NFC chip may communicate with an reader/interrogator according to the active protocol described above. Alternatively, the NFC chip can communicate with a reader/ interrogator in a passive mode. This will eliminate the need for the chip to be powered by the battery of a mobile phone, which may increase the life of the battery.

In most global system for mobile communication (GSM) devices, *e.g.*, mobile phones, there is a Subscriber Identification Module (SIM) that is a secure memory containing all of the owner's account information, as well as space available for additional applications such as an electronic purse for e-commerce. This memory is accessible from outside of the mobile device, i.e., remotely. Mobile devices carry a secure memory much like smart cards or the like and the new applications in NFC protocols enable the mobile device to perform functions like smart cards. The ability to have a mobile device also operate as a smart card creates a variety of new applications for the device.

Typical smart cards are a small, usually credit card shaped, device that contains at least a memory device for storing information and a transceiver to communicate with a reader/interrogator. The reader/interrogator communicates through the transceiver on the smart card to access the stored information. The reader/interrogator may simply read the information, load the information into the memory device or modify existing data in the memory device. For example, if the owner of a smart card uses a smart card containing financial information to make a purchase, the reader/interrogator can read the information including the owner's identity and the availability of funds. The reader/interrogator can also deduct the purchase amount from the available funds if it has writing capabilities. Further, the reader/interrogator can store transaction data on the smart card including the time and location of the transaction in addition to the identity of the reader/interrogator.

Smart cards have a variety of uses and can be utilized in any transaction that involves the exchange of data or information between individuals and an institution. For

example, smart cards can be used to store information including medical records, financial information, vehicle maintenance information, pet information, and a virtually limitless variety of other information traditionally printed on paper or plastic or stored on cards having a magnetic stripe or an optical bar code. Smart card technology has been particularly useful in banking systems and other financial transaction systems. Furthermore, smart cards have been widely used in access control systems. For example, an reader/interrogator may control doors that provide access to particular assets. The reader/interrogator only allows qualified individuals carrying smart cards, with proper credentials loaded thereon, access through control doors.

In a conventional access control system, the door reader/interrogators positioned at ingress/egress points are connected to a control panel. This control panel is kept up to date with the authorized codes corresponding to persons with authorized access to the location. When activity occurs, the control panel is updated with the activity information. For example, if the activity related to access gained through a particular door, the door and potentially the person who gained access are stored in the control panel log. Also, if the activity related to a financial transaction, the information relating to the transaction including amount and who performed the transaction are sent and stored at the control panel. There are, however, circumstances in which control panels associated with remote locations that are not regularly updated. If a person's status changes from authorized to unauthorized, it might take a relatively long time for the control panel associated with a remote door to get the message and bar the credential associated with this person from access. Furthermore, typical access control systems are limited in that control panels, either localized or central, are the only source that tracks, logs, and monitors the activity associated with a given access point. When entries take place in these conventional access control systems, the information is sent to the control panel where it stays. If someone would like to be aware of activity associated with the access control system they are usually required to physically go to the control panel itself.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention there is provided a method of remotely maintaining a secure access system, comprising:

receiving, at a secure access system controller, a credential update for at least one user of the secure access system; and

in response to receiving the credential update, said controller automatically initiating a system update process, the system update process comprising:

generating a message comprising information representing the credential update;

determining at least one target for said message, wherein said at least one target comprises at least one mobile device associated with the at least one user; and

transmitting said message to said at least one target.

According to a second aspect of the present invention there is provided a secure access system, comprising:

at least one mobile device comprising memory, wherein said memory comprises credential information;

a controller that is operable to receive a credential update for at least one user of the secure access system and in response to receiving the credential update automatically initiate a system update process, wherein during the system update process the controller is operable to automatically cause a message to be generated that comprises said updated credential, and cause said message to be transmitted to said at least one mobile device associated with said at least one user.

According to a third aspect of the present invention there is provided a mobile device for use by a user in a secure access system, comprising:

a memory, wherein said memory comprises credential information; and

an interface operable to communicate with a reader and further operable to receive messages relating to updated credential information, wherein, upon receipt of a first message, said credential information for the user is automatically changed from a first state to a second state and wherein said messages relating to updated-credential information are received without said at least one user transmitting a request for said messages.

The present invention provides a system and method that automatically updates credentials on a mobile device immediately after authorization changes have been made. In one embodiment, the system and method provides a controller (e.g., a control panel, number of control panels, host computer, number of host computers, server, and the like), a plurality of readers, and a plurality of mobile devices. Each of the

plurality of mobile devices has a memory associated with them that stores credential information. The readers are typically associated with a particular asset (e.g., a door permitting access to a secure room, a computer permitting access to secure information, a lock permitting access to a safe, etc.). The readers communicate with the mobile devices to determine if the credential information stored on the memory of the mobile device permits the person using the mobile device to access a particular asset. Credential information is verified at the reader then transmitted to the controller in order to notify security personnel or the like about the activity that has just taken place at the reader. When credential information is changed at the controller (e.g., access rights for a particular user of a mobile device have been partially or fully revoked, updated, enabled, augmented, added, etc.), that changed information is relayed to the mobile device via a communication network. The memory of the mobile device is then updated to reflect the change that was logged at the controller.

As used herein, a "credential" or "credential information" is any data, set of data, encryption scheme, key, and/or transmission protocol used by a particular mobile device to verify its authenticity with a reader/interrogator.

In another embodiment of the present invention, a system and method for periodically updating and/or enabling the credentials of a mobile device and/or reader is provided. Specifically, the controller updates the credential information of a mobile device on a predetermined periodic basis. Every predetermined period (e.g., every second, minute, hour, day, etc.) the credentials associated with one or a population of mobile devices is updated. At the same time, in one embodiment of the invention, the information relating to the updated credentials is relayed to the readers so that when a valid mobile device is presented to a reader, the reader is aware of the updated credentials and can assess the validity of the mobile device appropriately. Alternatively, or in addition to updating the mobile device credentials, the mobile devices may require a periodic enablement of their credentials in order to maintain their validity. For example, the credential information associated with a particular mobile device may not change, but the information will be erased, expire, or the mobile device may not be allowed to transmit its credential information if it does not receive the periodic enablement messages from the controller. Therefore, when a user is no longer permitted access to a particular asset, the automatic enablement messages are not sent to his/her mobile device. If a user has had their credentials revoked or changed for whatever reason, they may attempt to shield their mobile device from receiving any authorization disabling messages. By changing the logic of the

mobile device such that the credentials periodically time out unless an enabling message is received from the control panel, attempts to maintain or prolong authorized credentials by shielding mobile devices from a disabling message are thwarted.

In yet another embodiment of the present invention, a system and method for relaying information associated with activities detected at a reader or set of readers to a mobile device is provided. Rather than keeping a log of the activity information only at the controller, selected mobile devices can receive the activity information from the controller. In a residential lock situation, the system can send a Short Message Service (SMS) message/signalor the like to the mobile device of the homeowner. A homeowner at work may want to know when a child, housekeeper, or other person enters and exits their house. The selected mobile device could retrieve the message employing a number of other methods. For example, records of activities at a particular reader can be logged at that reader. A mobile device authorized to recover the activity log could be presented to the reader and the log file could be transferred to and displayed on the mobile device. Likewise, the reader (or the mobile device) could send the log file to a computer via email using various types of text messaging protocols.

These and other advantages will be apparent from the disclosure of the invention(s) contained herein. The above-described embodiments and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible using, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram depicting an exemplary system for authenticating mobile devices and remotely updating credentials associated with the mobile devices in accordance with embodiments of the present invention;

Fig. 2 is a block diagram depicting a mobile device in accordance with embodiments of the present invention;

Fig. 3 is a flow chart depicting a method of remotely updating credentials associated with a mobile device in accordance with embodiments of the present invention;

Fig. 4 is a flow chart depicting a method of periodically updating credentials associated with a mobile device in accordance with embodiments of the present invention; and

Fig. 5 is a flow chart depicting a method of relaying access activity in an exemplary system to a mobile device in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

The present invention is generally directed toward a system and method for using mobile communication devices as personal credential verification devices. Specifically, the present invention utilizes communication techniques and protocols to automatically and remotely update credential information associated with one or a set of mobile devices.

Fig. 1 depicts an access network 100 used to verify the identity of at least one mobile device. In one embodiment of the present invention, the system 100 comprises a controller 102, a hub 104, a plurality of readers 108_{1-n}, and a plurality of mobile devices 112_{1-k} such that n and k are integers wherein n and k are greater than or equal to one, and typically k is greater than n. The plurality of readers 108_{1-n} may include readers 108 of the same type, as well as readers of different types. For example, a subset of the plurality of readers 108_{1-n} may be legacy readers (e.g. readers using older transmission protocols). Whereas another subset of the plurality of readers 108_{1-n} may be newer readers utilizing improved and/or more secure protocols.

In the depicted embodiment, the readers 108 are coupled to the controller 102 via the interconnecting hub 104 through interfaces 124 and 128. In an alternate embodiment, the readers 108 may be directly coupled to the respective inputs/outputs of the controller 102 via interface 129. Interfaces 124 and 128 between the readers 108, the hub 104, and the controller 102 and interface 129 are generally bi-directional interfaces, which may selectively be implemented in a form of wired, wireless, fiber-optic communication links, or combinations thereof. Even though the interfaces 124, 128, and 129 are depicted as bi-directional interfaces, one of skill in art can appreciate that the interfaces 124, 128, and 129 may be implemented as unidirectional interfaces that use a unidirectional communication protocol, for example, the Wiegand protocol.

As can be appreciated by one of skill in the art, the interfaces 124, 128, and 129 may be implemented utilizing buses or other types of connections. For example, the I/O ports may be one or more of a USB port, parallel port, serial port, Small Computer Systems Interface (SCSI) port, modem, Ethernet, and/or an RF interface. The protocols used to communicate between the controller 102 and the readers 108 may include one or more of the TCP/IP protocol, RS 232, RS 485, Current Loop, Power of Ethernet (POE), Bluetooth, ZigBee, GSM, WiFi, and other communication methods and protocols known in the art.

Bi-directional RF interfaces 120 between a reader 108 and a mobile device 112 are automatically established when the mobile device 112 is placed within an active zone (not shown) of the interrogating reader 108. The active zone of the reader 108 is defined as a

three dimensional space where the intensity of RF signals emitted by the reader exceeds a threshold of sensitivity of the mobile device 112 and the intensity of RF signals emitted by the mobile device 112 exceeds a threshold of sensitivity of the reader 108. The interface 120 shown can be between one or a number of readers 108 and one or a number of mobile devices 11. Furthermore, the interface120 may utilize known methods and protocols including NFC protocol, Infra Red communication methods, Bluetooth, ZigBee, GSM, WiFi, and/or other protocols known to those of skill in the art.

The controller 102 may be a general-purpose computer adapted for multi-task data processing and suitable for use in various settings including, but not being limited to, business, commercial, residential, and industrial settings. Examples of suitable types of controllers 102 include, but are not limited to, a control panel, a number of control panels, a host computer, a processor, a server, combinations thereof, and other controllers known to those of skill in the art. A memory of the controller 102 comprises software program(s) containing a database of records for the access system 100. Alternatively, a database 130 may be separated from the controller 102 as depicted in Fig. 1. The database 130, whether integral to the controller 102, separate from the controller 102, or both, maintains records associated with the readers 108, mobile devices 112 and their respective holders or users, algorithm(s) for acquiring, decoding, verifying, and modifying data contained in the mobile device, algorithm(s) for testing authenticity and validity of the mobile devices 112, and algorithm(s) for implementing the results of these tests. Specific configurations of the controller 102 are determined based on and compliant with computing and interfacing capabilities of the readers 108 and/or the hub 104. As used herein, in reference to an individual or an object associated with a mobile device 112, the terms a "holder" and a "user" are used interchangeably.

Each reader 108 is adapted for exchanging information with the controller 102 and for requesting data from the mobile device 112 to verify the authenticity of the mobile device. Typically, a reader 108 is associated with a particular asset (e.g., a door protecting access to a secure room, a computer lock protecting sensitive information or computer files, a lock on a safe, and the like). In one embodiment, upon verification of credential information stored on the mobile device 112, the reader 108 generates signals facilitating execution of the results of interrogating the mobile device (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, provides access to a computer system, provides access to a particular document, and the like). Alternatively, the controller 102 may generate such

signals.

In addition to being proximity readers (e.g. readers that verify authenticity of smart cards, mobile devices and the like) the readers 108 may also have additional functionality. The readers 108 may include a keypad or other user input devices for receipt of additional user known passwords, contact card identification devices, and biometric authentication devices including voice recognition, retina scanners, finger print analyzers, facial feature analyzers, and the like.

In accordance with embodiments of the present invention, a stand-alone reader 108 may be utilized to perform the functionality of both the reader 108 and the controller 102. This stand-alone reader 108 may include, or have access to, the database 130 that contains data used to determine the authenticity of a mobile device 112 and/or algorithm(s) used to make the determination of authenticity of the mobile device 112. A determination of authenticity for a mobile device 112 is made at the receiving point rather than having to transmit data across a network from the reader 108 to a controller 102 in order to make a determination of authenticity. The stand-alone reader is further operable to execute instructions based upon the analysis of the mobile device 112.

A user typically carries the mobile devices 112 in order to verify his/her identity to a reader 108. Acceptable mobile devices 112 include, mobile cellular phones, personal digital assistants (PDAs), Blackberrys™, or any other mobile communication device that can be enabled for use in the access system 100 described. Essentially, the mobile device 112 can perform functions associated with typical mobile devices and can also act like a smart card, RFID, or other type of identification device. Typical identification devices utilize various protocols to communicate their credential information to a reader in order to gain access to a particular asset. The mobile devices 112, in accordance with embodiments of the present invention, are enabled to communicate with readers 108 in a similar fashion to that of smart cards and the like.

In accordance with embodiments of the present invention, the controller 102 is able to communicate with at least one of the plurality of the mobile devices 112 using a communication network 116. The communication network 116 utilized may be a conventional mobile radio network, for example, a GSM network, a Digital Cellular System (DCS), or Personal Communications Systems (PCS). The interface 132 may be a wired or wireless interface allowing the controller 102 to communicate with various other entities connected to the communication network 116. The mobile device 112 communicates with the communication network 116 via interface 136. The communication network 116

provides a way for the controller 102 to automatically notify and/or update information to the mobile devices 112 related to the access system 100. Additionally, the communication network 116 allows mobile devices 112 to communicate with each other.

Referring now to Fig. 2, an exemplary mobile device 112 will be described in accordance with embodiments of the present invention. In the depicted embodiment, the mobile device 112 comprises a memory 200, a processor 204, an RF receiver/transmitter 208 including an RF modulation/demodulation unit 212 and an RF antenna 216 for communication with a reader 108, an RF receiver/transmitter 230 including an antenna 226 and an RF modulation/demodulation unit 230 for communication with the communication network 116, an optional RF rectifier 220, and a power source 224. The processor 204 (e.g., an application specific integrated circuit (ASIC), microprocessor, programmable controller, or the like) uses bi-directional interfaces to communicate with various other parts of the mobile device 112.

One or more of the above-noted parts of the mobile device may be located on a subscriber identification module (SIM) card, which identifies the user in the communication network 116. SIM cards are already utilized now in GSM, DCS, or PCS mobile apparatus, among other things. Also, the SIM card may be either a full-sized card or a plug-in card; it is connected to the mobile device through a contact region (not shown) on the surface of the card. Other card formats, as well as contact lists SIM cards, may, however, likewise be used within the scope of this invention. U.S. Patent No. 6,859,650 to Ritter, which is herein incorporated by this reference in its entirety, describes using a SIM card located in a mobile device and an interface to communicate with external devices, without use of a mobile radio network.

As can be seen in Fig. 2, the mobile device 112, in one embodiment, communicates with external devices via two bi-directional interfaces 120 and 136. For example, the interface 120 where the RF antenna 216 transmits RF signals through free-space to be received by the reader 108. The reader 108 has a transceiver mounted thereon to receive the RF signals transmitted by the mobile device 112. The RF antenna 216 used by the mobile device 112 to create interface 120 may be a coil made by winding of a wire, by printing or etching of a conductor film, or with strip lines. Depending on the application, a transmission frequency, for instance, of 125 kHz, 13.56 MHz, 400 MHz or 5.2 GHz is used, the applied frequency also being dependent on the data transmission where needed. A frequency of about 13.56 MHz is preferred. However, in order to ensure compatibility with the readers 108, various other frequencies may be used. Through interface 120, the mobile

device 112 and the reader 108 can exchange data and programs with each other without contact and without making use of the communications network 116. As noted above, the interface 120 is created when the mobile device 112 enters an active region of a reader 108.

The memory 200 of the mobile device 112 generally comprises at least one array of non-volatile memory cells, e.g., static random access memory (SRAM) cells or Flash Memory Cells, among other types of non-volatile memory cells. The memory 200 may also comprise at least one array of dynamic random access memory (DRAM) cells. Therefore a content of at least a portion of the memory 200 may be pre-programmed and write protected thereafter, whereas the content of other portions of the memory 200 may be selectively modified and/or erased by the controller 102 and/or the reader 108.

The mobile device 112, according to embodiments of the present invention, is used as an identification device. Identification information is preferably loaded into a secure area of the memory 200 where it can be accessed by the processor 204 to communicate to readers 208 via interface 120. Information loaded on the memory 200 may include credential information of the user of the mobile device 112, for instance, unique IDs, manufacture IDs, passwords, keys, encryption schemes, transmission protocols, and the like. Additionally, the memory 200 may contain executable functions that are used by the processor 204 to run other components of the mobile device 112. When presented to a reader 108, the RF antenna 216 typically receives interrogating signals via interface 120. The interrogating signals are in the form of RF signals produced by the reader 108.

In accordance with embodiments of the present invention, the memory 200 may further comprise self-authenticating data and/or functions. Examples of self-authenticating data include, but are not limited to, assets the mobile device 112 has access to, times of allowed access to each asset, and other data that can assist the mobile device in determining if it is eligible to gain access to a particular asset. The self-authenticating functions use the self-authenticating data to enable the mobile device 112 to make a determination of its own access rights with respect to an asset.

A mobile device 112 that determines its own access rights and permissions is typically referred to as a smart mobile device. In operation, a "smart" mobile device 112 is presented to a reader 108. The reader 108 is associated with one or more assets and the reader 108 is the gatekeeper of those assets. The reader 108 contains information about its associated assets and usually time of day information. Upon presentation of the mobile device 112 to the reader 108, the reader 108 supplies the asset information and time of day

information to the mobile device 112. The mobile device 112 then analyzes the asset information and time of day information using its self-authenticating data. The mobile device 112 then makes a determination whether it is allowed to access the given asset (*e.g.*, whether the holder of the mobile device 112 can have access to a room behind a door, a bank account, computer files, *etc.*) If the mobile device 112 determines that it is allowed access to the particular asset, then it sends a signal back to the reader 108 indicating that validation of the mobile device 112 has been confirmed and access should be granted. Upon confirmation of validation of the mobile device 112, the reader 108 will unlock the door, access the bank account, permit access to the computer files, or perform the requisite steps to grant access to the holder of the mobile device 112. If the mobile device 112 determines that it is not allowed access to the particular asset, then it can either do nothing or send a signal back to the reader 108 indicating that validation of the mobile device 112 was not confirmed and access should not be granted. Upon the receipt of this signal, the reader 108 may perform no action, generate a message indicating that access was not granted, sound an alarm, or perform some other sort of action in accordance with denying the holder of the mobile device 112 access to the asset.

In operation, the reader 108 and the mobile device 112 use pre-programmed communication protocols. To increase the probability of error-free reception, the same messages may redundantly be repeated a pre-determined number of times or during a pre-determined timed interval. The interrogating reader 108 generates an interrogating RF signal. The interrogating RF signal of the interrogating reader 108 (or, if the protocol used by the mobile device 112 is an active protocol, RF signals produced by the mobile device 112) is received by the RFID antenna 216 and is forwarded to the modulation/ demodulation unit 212 that in turn demodulates the RF signal and provides the demodulated signal for processing to the processor 204. Upon receipt of the RF signal by the processor 204, the memory 200 is accessed and relevant credential information is retrieved from the memory 200 by the processor 204. The retrieved credential information is then passed on to the modulation/demodulation unit 212 where it is modulated and sent to the RF antenna 216. The RF antenna 216 provides the modulated signal back to the reader 108 via interface 120. At the reader 108 or controller 102 the credential information is processed to determine the validity of the mobile device 112.

The RF signals generated by the reader 108 inherently contain electromagnetic energy. The signals can be sent to the optional RF rectifier 220 and the energy from those signals can be converted into energy to run various components of the mobile device 112.

A power source 224 is also available to supply power to any other component of the mobile device 112 depicted or not depicted.

In accordance with embodiments of the present invention, the RF receiver/transmitter 234 for communication with the communication network 116 receives update signals (or other communication signals) from the communication network 116. In the event that the signal received by the antenna 226 is an update signal from the controller 102, the update signal is sent from the antenna 226 to the RF modulation/demodulation unit 230 where the signal is demodulated. The demodulated signal is sent to the processor 204, which then updates the memory 200 based on the update signal. The RF receiver/transmitter 230 also allows the mobile device 112 to communicate with other devices connected to the communications network 116.

Referring now to Fig. 3, a method of automatically and remotely updating credential information on a mobile device 112 will be described in accordance with embodiments of the present invention. The method begins at step 300 then proceeds to step 304 where credential information is changed at the controller 102. As noted above, credential information can include any data, set of data, encryption schemes, keys, transmission protocol, and the like, used by a particular mobile device 112 to verify its authenticity to a reader 108. Altering, modifying, enabling, disabling, revoking, adding, and updating any portion of the credential information may effect a change in the credential information. The credential information changed at the controller 102 is then updated at the database 130 in step 308. Thereafter, in step 312, information is retrieved from the database 130 by the controller 102 relating to what mobile device the changed information was associated with. The mobile device corresponding to the changed information is then identified as the target device. For example, if the access rights of one user have been modified, then the mobile device 112 associated with that user is the only mobile device 112 that needs to have its respective memory 200 updated, and thus the single mobile device 112 is the targeted mobile device 112. Alternatively, a change may relate to a number of mobile devices 112 and each device will need to receive the updated information on its respective memory 200. Thus each mobile device 112 will become a targeted device.

Once a targeted device is determined in step 312, a message is sent from the controller 102 to the determined (targeted) mobile device 112 via the communication network 116 in step 316. That information is received at the mobile device 112 through interface 136 by the antenna 226 that forwards this information to the RF modulation/demodulation unit 230 where the signal is demodulated. The RF

modulation/demodulation unit 230 then sends the demodulated update signal to processor 204. The processor updates the memory 200 to reflect the change that was made at the controller 102 in step 320.

Referring now to Fig. 4, another method of updating, enabling, and/or revoking the credentials of a mobile device 112 will be described in accordance with embodiments of the present invention. The method starts at step 400 and proceeds to step 404 where a time interval between credential updates is determined. The time period may vary depending upon the requirements and security needs of the system 100. For example, the interval may be set to update credentials every second, minute, hour, day or a variation thereof. In step 408, new credential information is determined. As noted above, the new credential information may relate to one or a number of mobile devices 112. In step 412, the new credential information is sent to the readers 108. Specifically, the readers 108 need to be made aware of changes of credential information if the changes are related to transmission protocols, keys, password changes, and the like. In step 416, the new credential information is sent to the respective mobile devices 112. This process is performed to ensure, for example, only mobile devices that are in communication with the communication network 116 have their credentials updated. Typically, when a user is de-enrolled from an access list, a message will be sent via a communication from the controller 102 to the mobile device 112 to revoke the associated credential information from the memory 200. A message is sent to the mobile device 112 immediately when that user is de-enrolled and therefore any attempts to gain access to the system 100 will be denied.

If the user who is no longer authorized to gain access to the system 100 intends to create problems, he/she might try to prevent the memory 200 in his/her phone from being de-authorized thereby keeping his/her access credentials on the mobile device 112. One way a person might do this would be by switching his/her phone off or otherwise shield it from the incoming messages by disabling the antenna 226 or tampering with interface 136. Thereafter he/she may only turn on and expose the mobile device 112 immediately prior to trying to gain access to an asset through reader 108. In one embodiment of the present invention, a signal (*i.e.*, an SMS signal) periodically transmitted to the mobile device 112 is required to keep the respective credentials active. Changing the system 100 logic so that the mobile device's 112 credentials time out periodically thwarts these attempts to stop a mobile device 112 from receiving a disable message. If the mobile device 112 does not receive an enabling message, then the credential information stored thereon will become obsolete.

In embodiments employing a smart mobile device 112, the periodically transmitted message may be required to keep the self-authenticating data and/or functions active and up to date. Essentially, a database of self-authenticating data may have a time out function such that after a predetermined amount of time, the self-authenticating data expires and erases itself. This way when a smart mobile device 112 is presented to a reader 108, it will not be able to validate its own access rights and thus will not be able to grant itself access to the asset associated with the given reader 108. The self-authenticating data may also be dynamically changing, thus if the mobile device 112 does not receive the updated version of the authenticating data, it will not be able to validate its own access rights.

Other functions of a mobile device 112 may also require periodic update/enabling signals in order to allow the smart mobile device 112 to validate its own access rights. For example, communications protocols or communication frequencies between a reader 108 and a mobile device 112 may also periodically change. If the mobile device 112 does not receive the updated communications directions, it will not be able to communicate properly with the reader 108, thus it will not be able to gain access to a particular asset.

An alternative embodiment would be to change protocols related to the communication interface 120. The changes could be sent via a message across the communications network 116 to the mobile device 112 such that the mobile device 112 is aware of the rolling or constantly changing credential information. For example, rolling access codes and keys may be applied to the readers 108 and the mobile devices 112. Any mobile device that is not in communication with the communication network 116 will not be updated with these rolling codes and will therefore not be able to be properly validated by reader 108.

In step 420, the amount of elapsed time since the last credential update is determined and if this time is determined to be greater than or equal to the determined update interval in step 424, the method goes to step 408 and new credential information is determined. However, if the time elapsed is not greater than the update interval, the process repeats step 420 until the periodic threshold is reached.

Referring now to Fig. 5, a method of relaying information relating to activities in an access system will be described in accordance with at least some embodiments of the present invention. The process starts at step 500 and then proceeds to step 504 where activity is detected at a reader 108. Information related to that activity is determined in step 508 and potentially logged. The information may be stored at reader 108 and/or sent to controller 102 to be stored in database 130. Thereafter, it is determined if a mobile device

112 is enabled to receive information about the activity that has just occurred in step 512. If there is a mobile device 112 enabled to receive information, the identity of that mobile device 112 is determined in step 516 by the controller 102, using a comparison of access rights and mobile device identities in the database. Otherwise, the logged information is not sent to any mobile device and the method ends at step 524. Once the enabled mobile device(s) 112 is determined in step 516, information relating to the activity is sent to the enabled mobile device(s) 112 in step 520.

As noted above, the information relating to the activity may be stored at the reader 108 and logged there. An enabled mobile device 112 may be presented to reader 108 and the log file of activities that have occurred at that particular reader 108 may be relayed to the enabled mobile device 112 in step 520. The information may also be sent to the mobile device via communications network 116 from the controller 102. Messages may be sent using an SMS message or other types of text messages known in the art. Additionally, the message may be sent via a voice recording to the mobile device 112 where the user of the mobile device can listen to an audio message rather than viewing a digital message.

The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments 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.

The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. In the foregoing Detailed Description for example, various features of the invention are grouped together in one or more embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed invention requires 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 embodiment. 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 invention.

Moreover, though the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, 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 embodiments 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.

It is to be understood that, throughout the description and claims of the specification the word "comprise" and variations of the word, such as "comprising" and "comprises", is not intended to exclude other additives, components, integers or steps.

The claims defining the invention are as follows:

1. A method of remotely maintaining a secure access system, comprising:

receiving, at a secure access system controller, a credential update for at least one user of the secure access system; and

in response to receiving the credential update, said controller automatically initiating a system update process, the system update process comprising:

generating a message comprising information representing the credential update;;

determining at least one target for said message, wherein said at least one target comprises at least one mobile device associated with the at least one user; and

transmitting said message to said at least one target.

2. The method of claim 1, wherein said credential update is pushed toward said at least one mobile device without any solicitation by said at least one mobile device or a user of said at least one mobile device, wherein the system update process further comprises transmitting said message to at least one of a reader and a database, wherein said at least one mobile device has a first set of credential data stored thereon, and wherein upon receiving said message from said controller, said first set of credential data is changed to a second different set of credential data and wherein said message is transmitted to said at least one mobile device without receiving a request for said message from said at least one user, wherein said at least one mobile device is a smart mobile device, wherein said first set of credential data comprises self-authenticating data, wherein said second set of credential data comprises different self-authenticating data, and wherein said self-authenticating data enables said at least one mobile device to make a determination of its own access rights with respect to an asset.

3. The method of claim 2, wherein said first set of credential data has at least one of a key, password, unique ID, encryption scheme, and transmission protocol that is different in said second set of credential data.

4. The method of any one of claims 1 to 3, further comprising, in the event that said at least one mobile device does not receive said message and is subsequently presented to a reader, determining, by said reader, that said at least one mobile device is invalid.

5. The method of any one of claims 1 to 4, wherein said credential updates are received at the controller on a periodic basis.

6. The method of any one of claims 1 to 5, further comprising:

receiving said message at said at least one mobile device; and

modifying at least a portion of memory of said at least one mobile device according to said updated credential information, wherein said modifying comprises at least one of disabling and revoking at least a portion of said memory..

7. The method of any one of claims 1 to 6, further comprising de–enrolling a user of at least one mobile device from an access list, wherein said credential update is generated in response to de–enrolling said user from said access list.

8. The method of any one of claims 1 to 7, wherein said message is transmitted over a cellular communication network.

9. The method of any one of claims 1 to 8, wherein said message is transmitted by at least one of a radio frequency signal and a near field communication signal.

10. The method of any one of claims 1 to 9, further comprising:

presenting said at least one mobile device to a reader;

generating a second message comprising information related to said at least one mobile device being presented to said reader; and

sending said second message to at least one of a database, controller, and another mobile device.

11. The method of claim 10, wherein said second message is sent via a short message service (SMS) message.

12. A secure access system, comprising:

at least one mobile device comprising memory, wherein said memory comprises credential information; and

a controller that is operable to receive a credential update for at least one user of the secure access system and in response to receiving the credential update automatically initiate a system update process, wherein during the system update process the controller is operable to automatically cause a message to be generated that comprises said updated credential, and cause said message to be transmitted to said at least one mobile device associated with said at least one user.

13. The system of claim 12, further comprising:

at least one reader for determining an authenticity of said at least one mobile device; and

a database for maintaining information related to said system, wherein said controller is further operable to cause a second message to be generated that comprises said updated credential and cause said second message to be transmitted to at least one of said reader and said database.

14. The system of claim 13, wherein, in the event that said at least one mobile device does not receive said message, credentials of for said at least one mobile device become obsolete.

15. The system of claim 14, wherein, upon presentation of said at least one mobile device to said at least one reader, the authenticity of said at least one mobile device is determined to be invalid.

16. The system of any one of claims 12 to 15, wherein credential information on said memory is altered in response to receiving said message, wherein said credential update is initiated by an entity other than said at least one user, wherein said at least one mobile device is a smart mobile device, wherein said credential information comprises self-authenticating data, wherein said self-authenticating data is altered, and wherein said self-authenticating data enables said at least one mobile device to make a determination of its own access rights with respect to an asset.

17. The system of any one of claims 12 to 16, wherein credential updates are received at said controller on a periodic basis.

18. The system of any one of claims 12 to 17, wherein credential information on said memory is at least one of disabled and revoked in response to receiving said message.

19. The system of any one of claims 12 to 18, wherein said mobile device comprises a timing–out mechanism, wherein said timing–out mechanism is operable to disable said memory unless an enabling message is received from said controller.

20. The system of any one of claims 12 to 19, wherein said controller causes said message to be transmitted to said mobile device via at least one of a global system for mobile communications, a digital cellular system, and a personal communications system.

21. The system of any one of claims 12 to 20, wherein said at least one mobile device is at least one of a cellular phone, and personal digital assistant.

22. The system of any one of claims 12 to 21, wherein said credential update is initiated in response to de–enrolling at least one user from a list of authorized users.

23. The system of any one of claims 12 to 22, wherein said at least one mobile device comprises a plurality of mobile devices, and wherein credential information in each one of the plurality of mobile devices is altered.

24. The system of any one of claims 12 to 23, wherein said at least one mobile device comprises a plurality of mobile devices, and wherein credential information in less than all of the plurality of mobile devices is altered.

25. The system of any one of claims 12 to 24, wherein said message is transmitted via at least one of a radio frequency and near field communication signal.

26. The system of any one of claims 12 to 25, wherein said message is transmitted via a cellular communications network.

27. A mobile device for use by a user in a secure access system, comprising:

a memory, wherein said memory comprises credential information; and

an interface operable to communicate with a reader and further operable to receive messages relating to updated credential information, wherein, upon receipt of a first message, said credential information for the user is automatically changed from a first state to a second state and wherein said messages relating to updated-credential information are received without said at least one user transmitting a request for said messages.

28. The device of claim 27, wherein, in the event that said first message is not received, said credential information is maintained in said first state and as a result becomes obsolete, wherein said reader is operable to determine an authenticity of said mobile device based at least in part upon said credential information, and upon presentation of said mobile device to said reader, the authenticity of said mobile device is determined to be invalid.

29. The device of claim 27 or 28, wherein said reader is associated with a controller and the controller is operable to determine an authenticity of said mobile device based at least in part upon said credential information, wherein said reader is operable to determine an authenticity of said mobile device based at least in part upon said credential information.

30. The device of any one of claims 27 to 29, wherein said credential information comprises at least one of a key, password, unique ID, encryption scheme, and transmission protocol.

31. The device of any one of claims 27 to 30, wherein said at least one of a key, password, unique ID, encryption scheme, and transmission protocol is different in said first state than in said second state.

32. The device of any one of claims 27 to 31, wherein said credential information comprises self–authenticating data, wherein said self–authenticating data is different between said first state and said second state, and wherein said self-authenticating data enables said mobile device to make a determination of its own access rights with respect to an asset.

33. The device of any one of claims 27 to 32, further comprising a timing–out mechanism, wherein said timing–out mechanism is operable to disable said memory unless an enabling message is received.

34. The device of any one of claims 27 to 33, wherein a near field communications protocol is used by said first interface to communicate with said reader.

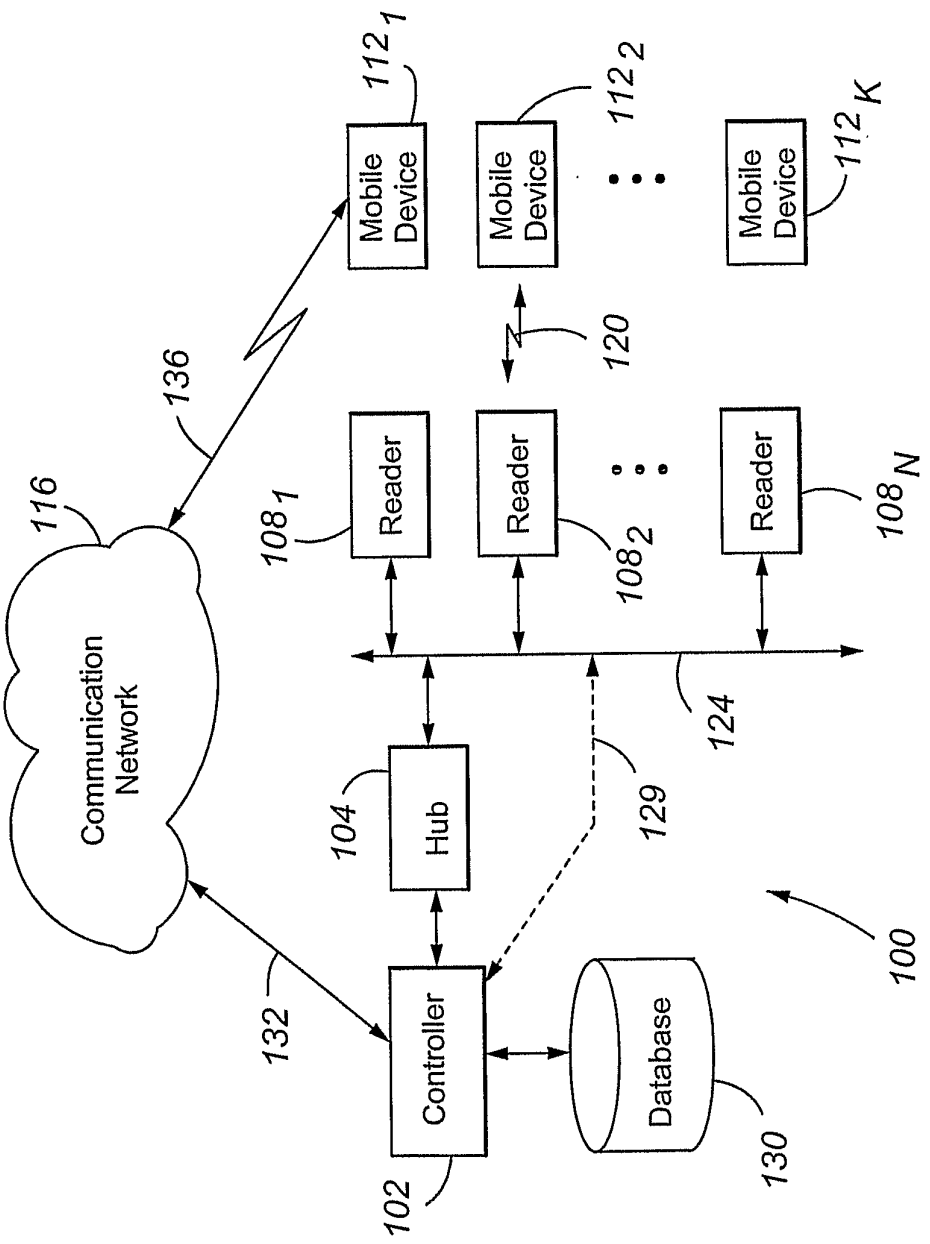

Mobile Device
Mobile Device
Mobile Device
Reader
Reader
Reader
Communication Network
Hub
Controller
Database
116
136
120
124
129
132
100
102
104
130
112_1
112_2
112_K
108_1
108_2
108_N

Fig. 1

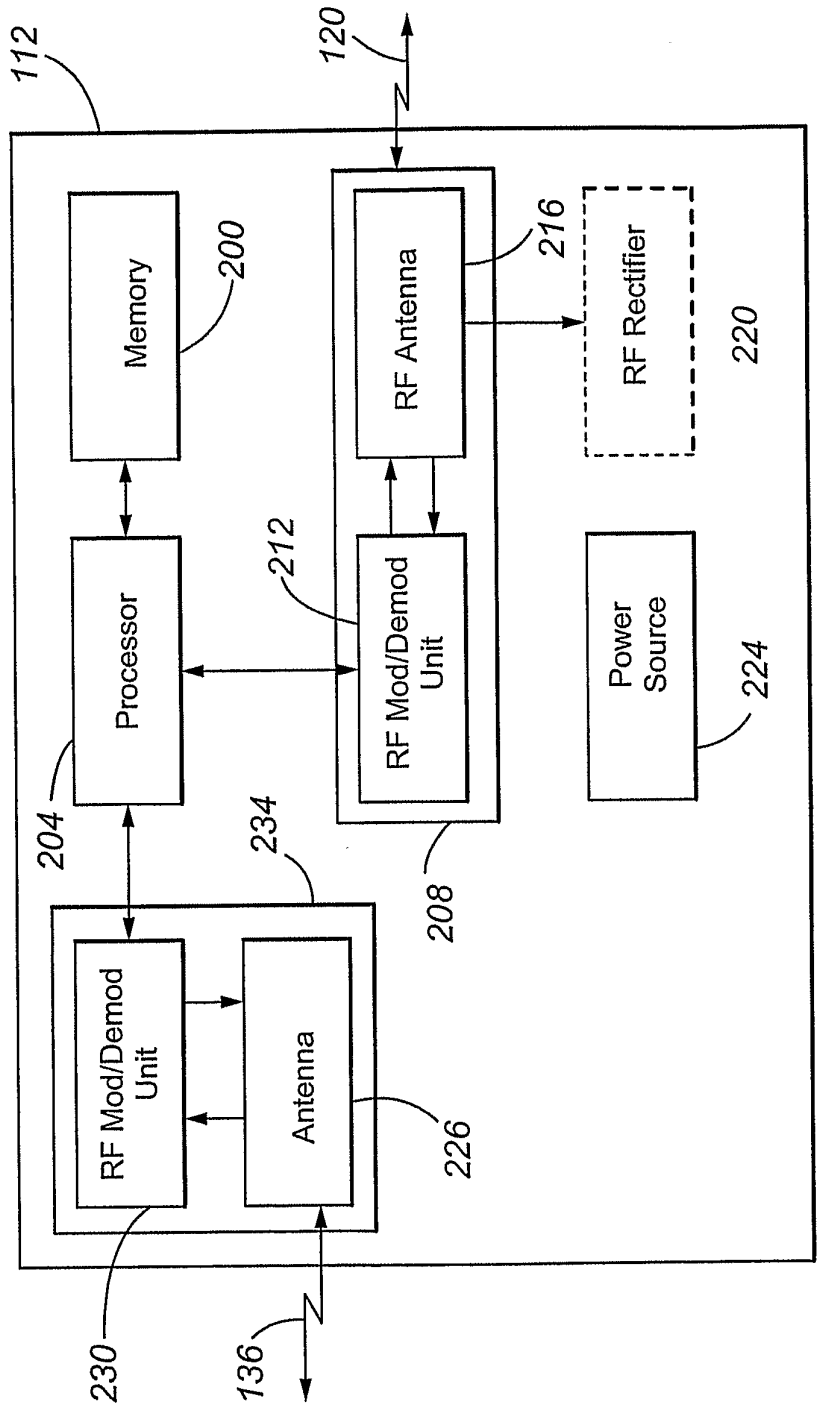

112
120
Memory
200
RF Antenna
216
RF Rectifier
220
Processor
212
RF Mod/Demod Unit
Power Source
224
204
234
208
RF Mod/Demod Unit
Antenna
226
230
136

Fig. 2

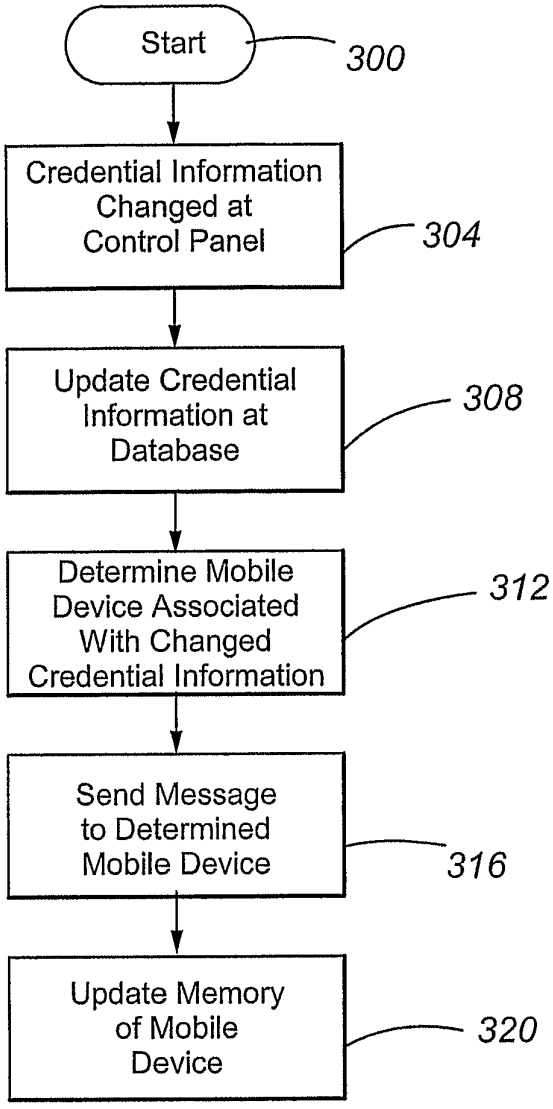

Start
300
Credential Information Changed at Control Panel
304
Update Credential Information at Database
308
Determine Mobile Device Associated With Changed Credential Information
312
Send Message to Determined Mobile Device
316
Update Memory of Mobile Device
320

Fig. 3

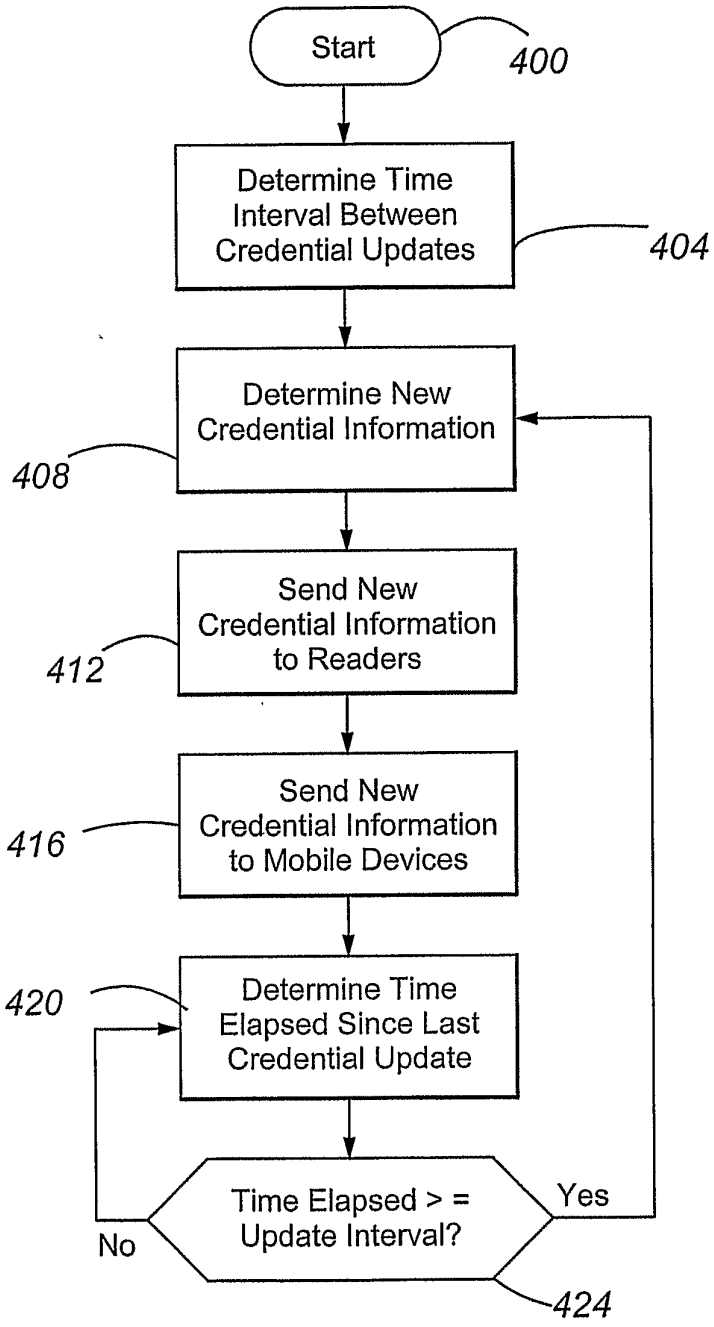

Start
400
Determine Time Interval Between Credential Updates
404
Determine New Credential Information
408
Send New Credential Information to Readers
412
Send New Credential Information to Mobile Devices
416
Determine Time Elapsed Since Last Credential Update
420
Time Elapsed > = Update Interval?
Yes
No
424

Fig. 4

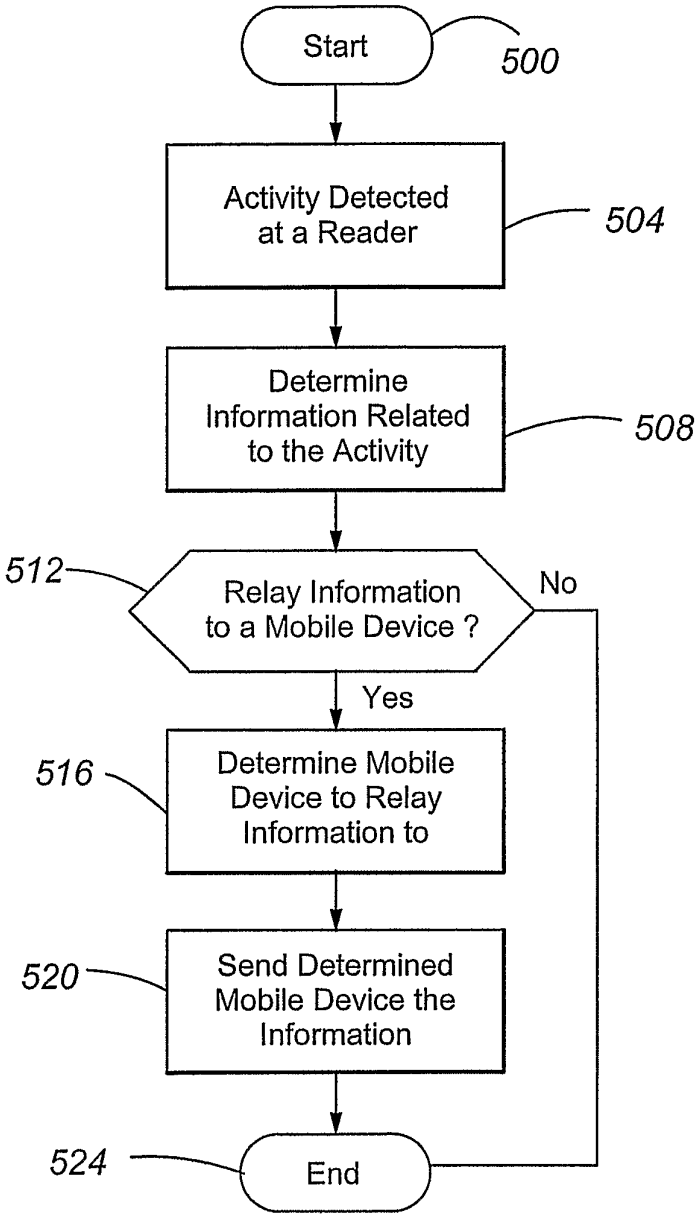

Start
500
Activity Detected at a Reader
504
Determine Information Related to the Activity
508
512
Relay Information to a Mobile Device ?
No
Yes
516
Determine Mobile Device to Relay Information to
520
Send Determined Mobile Device the Information
524
End

Fig. 5