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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 December 2016 (08.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/196475 A1

(51) International Patent Classification:
E05B 47/02 (2006.01) *G06F 21/31* (2013.01)
E05B 49/00 (2006.01) *G06F 21/34* (2013.01)
E05B 19/00 (2006.01)

(21) International Application Number:
PCT/US2016/035036

(22) International Filing Date:
31 May 2016 (31.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/168,715 29 May 2015 (29.05.2015) US
15/136,198 22 April 2016 (22.04.2016) US

(71) Applicant: **SCHLAGE LOCK COMPANY LLC** [US/US]; 2720 Tobey Drive, Indianapolis, IN 46219 (US).

(72) Inventors: **BAUMGARTE, Joseph, W.**; 12536 Charing Cross Road, Carmel, IN 46033 (US). **HOPKINS, Benjamin, J.**; 2805 W. High Grove Circle, Zionsville, IN 46077 (US). **STUDT, David, G.**; 21180 Carrigan Crossing, Noblesville, IN 46062 (US).

(74) Agents: **SCHEPERS, Brad A.** et al.; Taft Stettinius & Hollister LLP, One Indiana Square, Suite 3500, Indianapolis, IN 46204 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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

(54) Title: CREDENTIAL DRIVING AND AUTOMATIC LOCK UPDATE

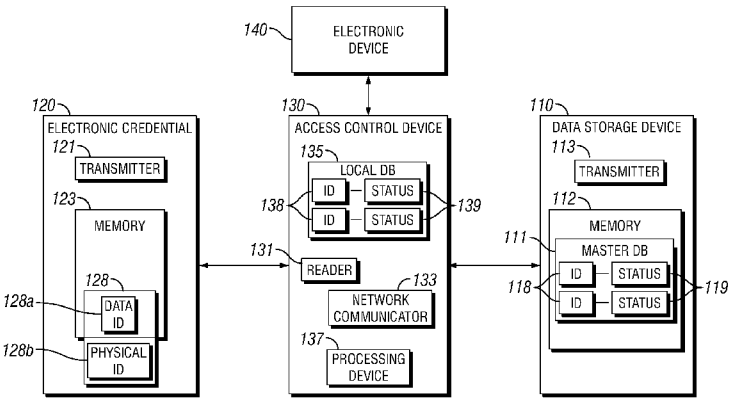


FIG. 1

(57) Abstract: An access control system including a data storage device configured to store a master credential database having a plurality of master identifiers and master status codes, an access control device having a local credential database including a plurality of local identifiers, and an electronic credential including a credential identifier. The access control device is configured to receive the credential identifier from the electronic credential, to determine whether to perform an update based upon the local status code associated with the local identifier of the credential identifier, and to update data in the local credential database with data in the master credential database by way of communication with the data storage device in response to the determining.

WO 2016/196475 A1

CREDENTIAL DRIVING AN AUTOMATIC LOCK UPDATE

TECHNICAL FIELD

[0001] The present application generally relates to an access control device, and more particularly but not exclusively relates to an access control device which automatically updates when a user presents a new authorized electronic credential to the device.

BACKGROUND

[0002] Present access control devices suffer from a variety of drawbacks, limitations, disadvantages and problems including high power consumption and system update logistical requirements. For example, certain battery powered access control devices query a central server each time an unrecognized credential is presented. Each query requires activation of a network communicator which consumes power. In another example, certain access control systems require an administrator to visit the access control devices in an access control system to update the authorized credential data associated with each device being accessed, including a lock. Therefore, a need exists for further technological developments in the area of access control devices.

SUMMARY

[0003] One exemplary embodiment is an access control system including a data storage device configured to store a master credential database including a plurality of master identifiers and master status codes, an access control device having a local credential database including a plurality of local identifiers, and an electronic credential including a credential identifier. The access control device is configured to receive the credential identifier from the electronic credential, to determine whether to perform an update based upon the local status code associated with the local identifier of the credential identifier, and to update data in the local credential database with data in the master credential database by way of communication with the data storage device in response to the determining. Further embodiments, forms, features, and aspects of the present application will become apparent from the description and figures provided herewith.

BRIEF DESCRIPTION OF THE FIGURES

[0004] FIG. 1 is a schematic block diagram of an access control system according to an embodiment of the invention.

[0005] FIG. 2 is a schematic flow diagram of a process of operating an access control system.

[0006] FIG. 3 is a schematic flow diagram of a process of operating an access control system.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0007] For the purposes of promoting an understanding of the principles of the invention, reference will now be made to the embodiments illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended. Any alterations and further modifications in the described embodiments, and any further applications of the principles of the invention as described herein are contemplated as would normally occur to one skilled in the art to which the invention relates.

[0008] Referring to FIG. 1, there is illustrated a block diagram depicting an exemplary access control system 100 configured to grant or deny access to a secured area such as an event ground, a building, or a portion of a building. The system 100 includes a data storage device 110, an electronic credential 120, and an access control device 130.

[0009] The storage device 110 includes a memory device 112, a master database 111, and a transceiver 113. The memory device holds the master database 111 having a plurality of master identifiers 118 and a plurality of master status codes 119. Each master status code 119 is associated with one identifier 118. The master database 111, in different embodiments, includes additional information related to each master identifier 118. The master identifier118 includes one or more a unique identifiers having a numeric, alphanumeric, or alphabetic character string associated with an electronic credential 120, as will be discussed in further detail below. The master status code 119 associated with each master identifier 118 indicates to an access control device 130 whether to grant access, deny access, perform a database update, and/or carry out another command. In one embodiment, the storage device 110 is a server. In other embodiments, the storage device 110 is a part of a network such as, for example, a cloud computing network. In other embodiments, the system 100 may include more than one storage device 110.

[0010] In the illustrated form, the transceiver 113 is a bidirectional communication device operable to send data from the master database 111 to the access control device 130, and to receive data from the access control device 130. The transceiver 113 is also capable of transferring data to other devices and receiving data from other devices such as, for example, a computer. In one embodiment, the transceiver 113 communicates with other devices via a wireless connection such as WiFi, Bluetooth, BLE, Zigbee, or Z-Wave. In one embodiment, the

transceiver 113 communicates with another device via a wired connection. In other embodiments, the transceiver 113 may be configured as a transceiver, a network adapter, a network card, an interface, or a port (e.g., a USB port, serial port, parallel port, and analog port, digital port, VGA, DVI, HDMI, FireWire, CAT 5, or any other suitable type of port or interface). The transceiver 113 includes hardware, software, and/or firmware which enables the transfer of data between the data storage device 110 and other devices such as, for example, the access control device 130. It is contemplated that the transceiver 113 may include more than one of the adapters, cards, or ports.

[0011] The storage device 110 is operable to store the master database 111 in the memory device 112. The storage device 110 responds to a request for a database update transmitted by the access control device 130 to the storage device 110. In response, data is transmitted from the master database 111 to the access control device 130. The storage device 110 is operable to receive data from the transceiver 113, and to modify the master database 111 using the received data. From time to time, a site administrator 102 (FIG. 2) modifies the master database 111 by transmitting data to the transceiver 113 so as to change permissions of an existing user 104 (FIG. 2) or to add or remove an identifier 118.

[0012] The electronic credential 120 includes a transceiver 121, a memory device 123 and a credential identifier 123. The electronic credential 120 is associated with a unique credential identifier 128, and is operable to transmit the credential identifier 128 to the access control device 130. In one or more embodiments, the credential identifier 128 is displayed on the electronic credential 120 and/or is stored in the memory device 123 within the electronic credential 120. In one embodiment, the electronic credential 120 is a contactless smartcard. In another embodiment, the electronic credential 120 is a mobile device. In one embodiment, the credential identifier 128 and the transceiver 121 are provided as a barcode printed on the electronic credential 120. In another embodiment, the access control system 100 includes a plurality of electronic credentials.

[0013] The transceiver 121 is operable to transmit the credential identifier 128. In one embodiment, the transceiver 121 is self-powered. For example, the transceiver 121 is powered by a battery located within the electronic credential 120. In another embodiment, the access control device 130 powers the transceiver 121 before the transceiver 121 provides an identifier to the access control device 130. For example, the access control device 130 may inductively

transfer power to the transceiver 121. In other embodiments, the electronic credential 120 does not necessarily need to be powered.

[0014] The access control device 130 includes a reader device 131, a network communicator 133, a local database 135, and a processing device 137. In one embodiment, the access control system 100 includes more than one access control device 130. In another embodiment, the access control device 130 is affixed to a permanent structure near a point of ingress to the secured area. In a further embodiment, the access control device 130 is a handheld electronic device. In other embodiments, the access control device 130 may be powered by a battery or other means of providing power, as is known in the art.

[0015] The reader device 131 is operable to detect the electronic credential 120, and to receive the credential identifier 128 from the electronic credential 120. The reader device 131, in different embodiments includes, for example, a barcode scanner, a QR (quick response) code scanner, a magnetic strip reader, or any other device configured to read a code physically imprinted on the electronic credential 120. In one embodiment, the reader 131 receives the credential identifier 128 from the electronic credential 120 via a wireless connection, such as RFID, WiFi, Bluetooth, BLE, Zigbee, or Z-Wave.

[0016] The network communicator 133 is operable to send a database update request to the data storage device 110, and to receive data from the data storage device 110. In other embodiments, the network communicator 133 is configured as a gateway or a router. The network communicator 133 may be configured as a transceiver, a network adapter, a network card, am interface, or a port (e.g., a USB port, serial port, parallel port, and analog port, digital port, VGA, DVI, HDMI, FireWire, CAT 5, or any other suitable type of port or interface). The network communicator 133 includes hardware, software, and/or firmware which allows data to be transferred between the access control device 130 and other devices such as, for example, the data storage device 110. It is contemplated that the network communicator 133 may include more than one of the adapters, cards, or ports. It is further contemplated that the network communicator 133 includes other features and functionalities not previously discussed.

[0017] The circuitry of the electronic credential 120, the data storage device 110, and/or the network communicator 133 is configured to provide appropriate signal conditioning to transmit and receive data, and correspondingly may include filters, amplifiers, limiters, modulators,

demodulators, CODECs, digital signal processing, and/or different circuity or functional components as would occur to those skilled in the art to perform the desired communications.

[0018] The local database 135, similar to the master database 111, includes a plurality of local identifiers 138 and local status codes 139. Each local status code 139 is associated with one identifier. The local database 135 may be a prior or current version of the master database 111.

[0019] The access control device 130 also includes a processing device 137 operable to receive data from and transmit data to the reader device 131, the network communicator 133, and/or the local database 135. When the electronic credential 120 is presented to the reader device 131 for the first time, the processing device 137 receives the credential identifier 128 by way of the reader device 131, reviews the local status code 139 associated with the matching local identifier 138, and replaces data in the local database 135 with data in the master database 111. In one embodiment, the entire local database 135 may be replaced by the current version of the master database 111. In another embodiment, the local status codes 139 of the local database 135 may be replaced by data in the current version of the master database 111. In still another embodiment, only the local status code 139 which is associated with the local identifier 138 and which matches the credential identifier 128 presented to the access control device 130 is replaced by data from the master database 111.

[0020] In one embodiment, the processing device is a microcontroller which includes one or more individual controllers or microprocessors, each of which includes at least one processor coupled to a memory such as, for example, memory used to store the local database 135. The memory may include random access memory (RAM) devices comprising the main memory storage of the microcontroller, as well as any supplemental levels of memory (e.g., cache memories), non-volatile or backup memories (e.g., programmable or flash memories), or read-only memories (ROM). The processing device is configured to execute stored program instructions and store, transmit, receive and manipulate the data. The program instructions may be embodied as program code in software and/or as firmware resident in the processing device or in memory.

[0021] The processing device 137 makes a determination of whether to grant or deny access to the secured area as a function of a comparison of the credential identifier 128 with one of the status codes 139. If the comparison indicates that access should be granted, the access control device generates an output signal to an electronic device 140. The electronic device 140 may be

any type of input component or output component that allows data to be inputted to or outputted from the access control device 130. In one embodiment, the electronic device 140 is a locking mechanism having an unlocked state and a locked state. When the locking mechanism (the electronic device 140) receives an output signal to grant access, the locking mechanism 140 transitions to or remains in the unlocked state. When the locking mechanism receives an output signal configured to deny access, the locking mechanism 140 transitions to or remains in the locked state.

[0022] In another embodiment, the electronic device 140 is one or more of a switch, a router, a firewall, a server, a database, a mobile device, a networking device, a controller, a computer, a processing system, a printer, a display, an alarm, an illuminated indicate such as a status indicator, a keyboard, a mouse, and a touch screen display. In another form, the electronic device 140 is incorporated into the access control device 130 to provide a single unit having the functions of both the access control device 130 and the electronic device 140. It is further contemplated that in other embodiments, more than one electronic device is in communication with the access control device 130.

[0023] A schematic flow diagram and related description provides an illustrative embodiment of performing procedures of controlling an access control system, such as the system 100 illustrated in FIG. 1 and described above. The described operations and functions are understood to be exemplary only, and in different embodiments, the operations and functions are combined in whole or in part, divided, added or removed, as well as re-ordered in whole or in part. It is contemplated that the various aspects, features, processing devices, processes, and operations from the various embodiments may be used in association with any of the other embodiments. It should be understood that certain operations may be implemented by a computer executing a computer program product on a non-transient computer readable storage medium, where the computer program product includes instructions causing the computer to execute one or more of the operations, or to issue commands to other devices to execute one or more operations.

[0024] While the embodiments described hereinafter may not specifically describe features analogous to those described above, such features may nonetheless be utilized in connection with the described systems.

[0025] Referring to FIG. 2, shown therein is a flow diagram illustrating one embodiment of a process 200 for controlling an access control system, such as the system 100 illustrated in FIG. 1.

The process 200 begins with an operation 201 which includes uploading master identifiers 118 and associated status codes 119 to the master database 111. The operation 201 is, for example, performed by a site administrator 102 or other authorized personnel. The master identifiers 118 correspond to each authorized electronic credential 120 intended to be used with the access control system 100, even if they are not initially assigned to a user 104. A status code 119 indicating that access should be granted is associated with the credential 120 given to existing users 104. Once the association of the status code 119 to the credential has been completed, the electronic credential 120 of the authorized existing user 104, if presented to the reader 131, grants immediate access to the secure area. The status code 119 associated with electronic credentials 120 which are not associated with existing users 104 initially indicate that a database update should be initiated.

[0026] After the identifiers and status codes have been uploaded to the master database 111, the process 200 proceeds to a load database operation 203 in which the master database 111 is transferred to the local database 135 of the access control device 130. The process 200 proceeds to an assign new card operation 205 in which the site administrator 102 assigns the electronic credential 120 to a new user 104. The site administrator 102 updates the master database 111 such that the status code 119, associated with the credential identifier 128 of the electronic credential 120 assigned to the new user 104, indicates access should be granted to the new user 104. The process 200 proceeds to a provide new card to user operation 207 in which the new user 104 receives a new electronic credential 120 from the site administrator 102.

[0027] After the master database 111 has been updated with the identifier 118 associated with the electronic credential 120 and the new user 104 has received the credential 120, the process 200 proceeds to a user presents the credential 120 operation 209. This operation begins when the new user 104 presents the electronic credential 120 to the access control device 130 for the first time. In the operation 209, the access control device 130 accesses the local database 135 and reads the local status code 139 associated with electronic credential 120. The process 200 then proceeds to a card requests update operation 211. In this operation 211, the local status code 139 provides an instruction indicating that a database update is required. Upon receipt of the instruction, the access control device 130 requests data from master database 111. The process 200 proceeds to a receive new door file operation 213 in which the data storage device 110 transmits data from master database 111 to the access control device 130. The transmitted data

includes the local status code associated with the electronic credential 120 which is assigned to a particular user. The local database 135 of the access control device 130 is updated by the newly received data from the storage device 110. After the local database 135 is updated with the newly received data, the process 200 proceeds to a user re-presents card operation 215 in which the new user 104 presents the electronic credential 120 to the access control device 130 a subsequent time. The access control device 130 reads the local status code 139 associated with the electronic credential 120 and generates a signal to grant access to the user 104.

[0028] Referring to FIG. 3, shown therein is a flowchart illustrating one embodiment of a process 300 for controlling an access control system, such as the system 100 illustrated in FIG. 1. The exemplary process 300 begins with a load all cards operation 301 in which a site administrator 102 loads the master database 111 into the data storage device 110. Each master status code 119 associated with electronic credentials 120 not given to existing users 104 initially indicates a database update should be initiated and access should be granted. The process 300 proceeds to a database loaded operation 303 in which the master database 111 is transferred to the local database 135 of the access control device 130.

[0029] The process 300 proceeds to an assigns card to new user operation 305 in which the site administrator 102 assigns an electronic credential 120 to a new user 104, and updates the master database 111 in the data storage device 110. The assignment of the master status code 119 associates the new user 104 with the credential identifier 128 of the electronic credential 120 which indicates that access should be granted to the new user 104. The process 300 proceeds to a gives new card to user operation 307 in which the new user 104 receives the electronic credential 120. The process 300 then proceeds to a user presents card operation 309 in which the new user 104 presents the electronic credential 120 to the access control device 130 for the first time. The access control device 130 accesses the local database 135 and reads the local status code 139 associated with the credential identifier 128. Process 300 then proceeds to a lock allows user entry operation 311 where the access control device 130 grants access to the new user 104. Process 300 proceeds to a card requests update operation 313 where the access control device 130 requests a new door file from the master database 111, and then proceeds to a receive new door file operation 315 where the data storage device 110 transmits the current version of the master database 111 to the access control device 130, and the local database 135 of the access

control device is replaced by the newly received version of the master database 111. In one embodiment, only the local status code 139 of the one local identifier 138 in question is updated.

[0030] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only the preferred embodiments have been shown and described and that all changes and modifications that come within the spirit of the inventions are desired to be protected.

[0031] It should be understood that while the use of words such as preferable, preferably, preferred or more preferred utilized in the description above indicate that the feature so described may be more desirable, it nonetheless may not be necessary and embodiments lacking the same may be contemplated as within the scope of the invention, the scope being defined by the claims that follow. In reading the claims, it is intended that when words such as "a," "an," "at least one," or "at least one portion" are used there is no intention to limit the claim to only one item unless specifically stated to the contrary in the claim. When the language "at least a portion" and/or "a portion" is used the item can include a portion and/or the entire item unless specifically stated to the contrary.

WHAT IS CLAIMED IS:

1. An access control system, comprising:

a data storage device configured to store a master credential database including a plurality of master identifiers and master status codes, wherein each of the master identifiers is associated with one of a plurality of local status codes;

an access control device having a local credential database including a plurality of local identifiers, wherein each of the plurality of local identifiers is associated with one of the plurality of local status codes, and each of the plurality of local identifiers is associated with one of plurality of the master identifiers; and

an electronic credential including a credential identifier, wherein the credential identifier is associated with one of the plurality of the master identifiers and one of the plurality of the local identifiers,

wherein the access control device is configured to receive the credential identifier from the electronic credential, to determine whether to perform an update based upon the local status code associated with the local identifier of the credential identifier, and to update data in the local credential database with data in the master credential database by way of communication with the data storage device in response to the determining.

2. The system of claim 1, wherein the data storage device comprises a server.

3. The system of claim 1, further comprising a plurality of the electronic credentials, wherein each of the electronic credentials includes a unique credential identifier.

4. The system of claim 1, wherein the electronic credential is configured to receive power from the access control device.

5. The system of claim 1, wherein the electronic credential is a contactless smartcard.

6. The system of claim 1, wherein the electronic credential is a mobile device.

7. The system of claim 1, further comprising a plurality of access control devices.

8. The system of claim 1, wherein the access control device and the data storage device are in communication via a wireless connection.

9. The system of claim 8, wherein the wireless connection comprises a WiFi connection.

10. An access control device, comprising:

a reader device configured to receive a credential identifier from an electronic credential;

a network communicator configured to transmit and receive data over a network;

a memory device configured to store a credential database including a list of local identifiers, wherein each of the local identifiers has an associated status code; and

a processing device configured to receive the credential identifier from the reader device, determine the credential identifier corresponds to a matching one of the local identifiers, transmit a credential database update request to the network by way of the network communicator in response to the status code associated with the matching the local identifier indicating a credential database update is needed, replace data of the credential database with data received from the network, and output a control signal to an electronic device.

11. The device of claim 10, wherein the electronic device comprises a locking mechanism having a locked state and an unlocked state, and wherein the locking mechanism is configured to transition between the locked and unlocked states based on the control signal.

12. The device of claim 10, wherein the electronic device comprises an output component configured to display access request results.

13. The device of claim 10, wherein the electronic device is configured to selectively grant and deny access to a secured area in response to the control signal.

14. The device of claim 13, wherein the access control device is further configured to

deny access to the secured area if the credential identifier does not correspond to any of the local identifiers.

15. The device of claim 13, wherein the access control device is further configured to selectively grant access to the secured area in response to receiving a local identifier with a status code indicating a database update is required.

16. The device of claim 15, wherein the access control device is further configured to selectively grant access to the secured area in response to the local credential database including the matching local identifier after the credential database update is complete.

17. A method for updating a credential database associated with an access control device, the method comprising:

receiving a presented identifier;

comparing the presented identifier to a first credential database including a plurality of potential identifiers, each with an associated status code;

identifying one of the plurality of potential identifiers that matches the received presented identifier; and

reviewing the status code associated with the matched one of the plurality of potential identifiers,

wherein in response to the status code associated with the matched one of the plurality of potential identifiers, updating the first credential database with data from a second credential database including identifiers, each with an associated status code.

18. The method of claim 17, further comprising receiving the presented identifier at the access control device a second time, and granting access to a secured area if the status code associated with the user identifier in an updated first credential database indicates access should be granted.

19. The method of claim 17, further comprising granting access to a secured area.

20. The method of claim 17, wherein updating the first credential database includes replacing at least the status code associated with the presented identifier with data from the second credential database.

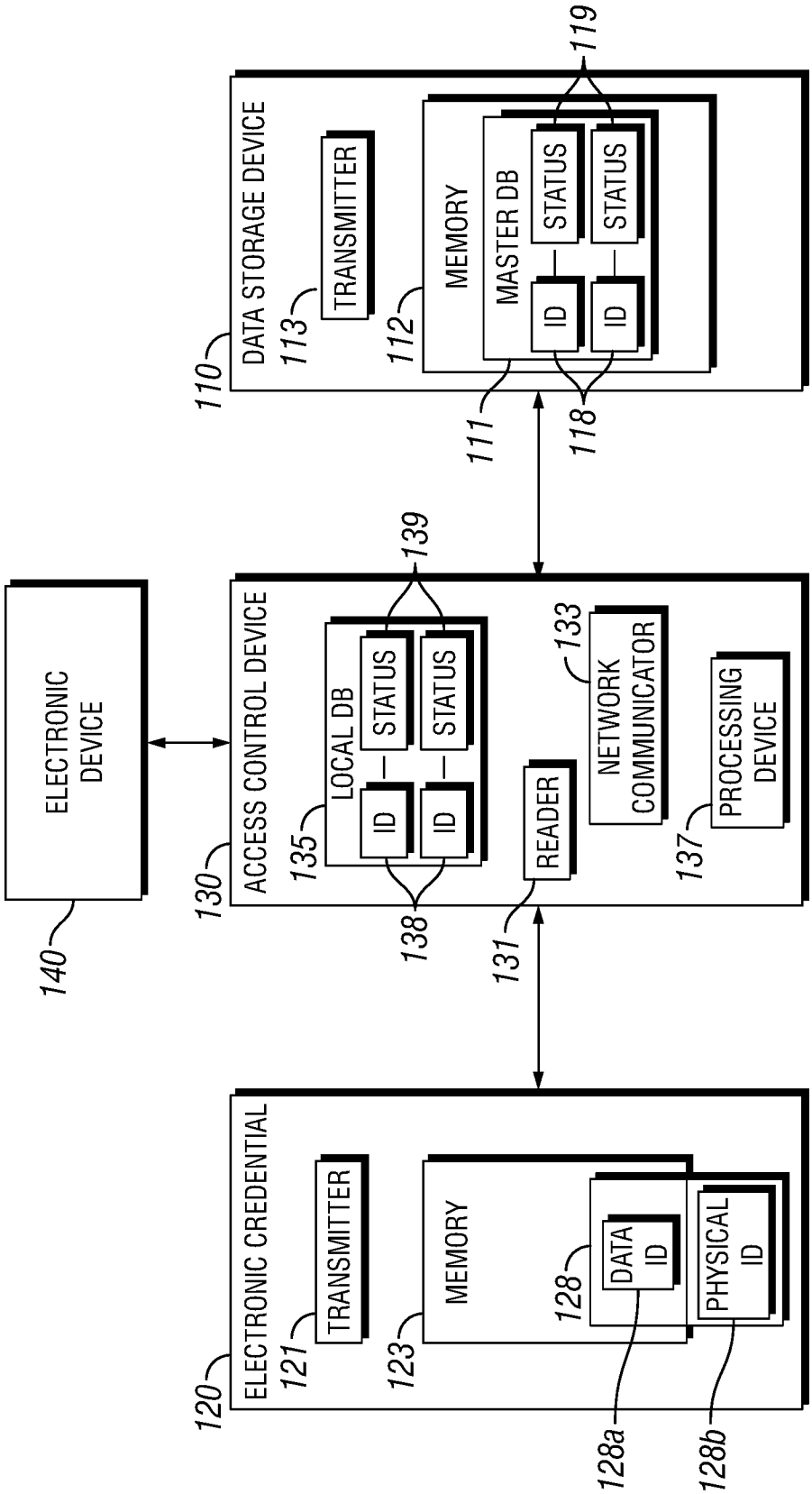

ELECTRONIC DEVICE
140
ACCESS CONTROL DEVICE
130
LOCAL DB
135
ID
STATUS
ID
STATUS
138
READER
131
NETWORK COMMUNICATOR
133
PROCESSING DEVICE
137
139
DATA STORAGE DEVICE
110
TRANSMITTER
113
MEMORY
112
MASTER DB
ID
STATUS
ID
STATUS
119
111
118
ELECTRONIC CREDENTIAL
120
TRANSMITTER
121
MEMORY
123
DATA ID
128
PHYSICAL ID
128a
128b

FIG. 1

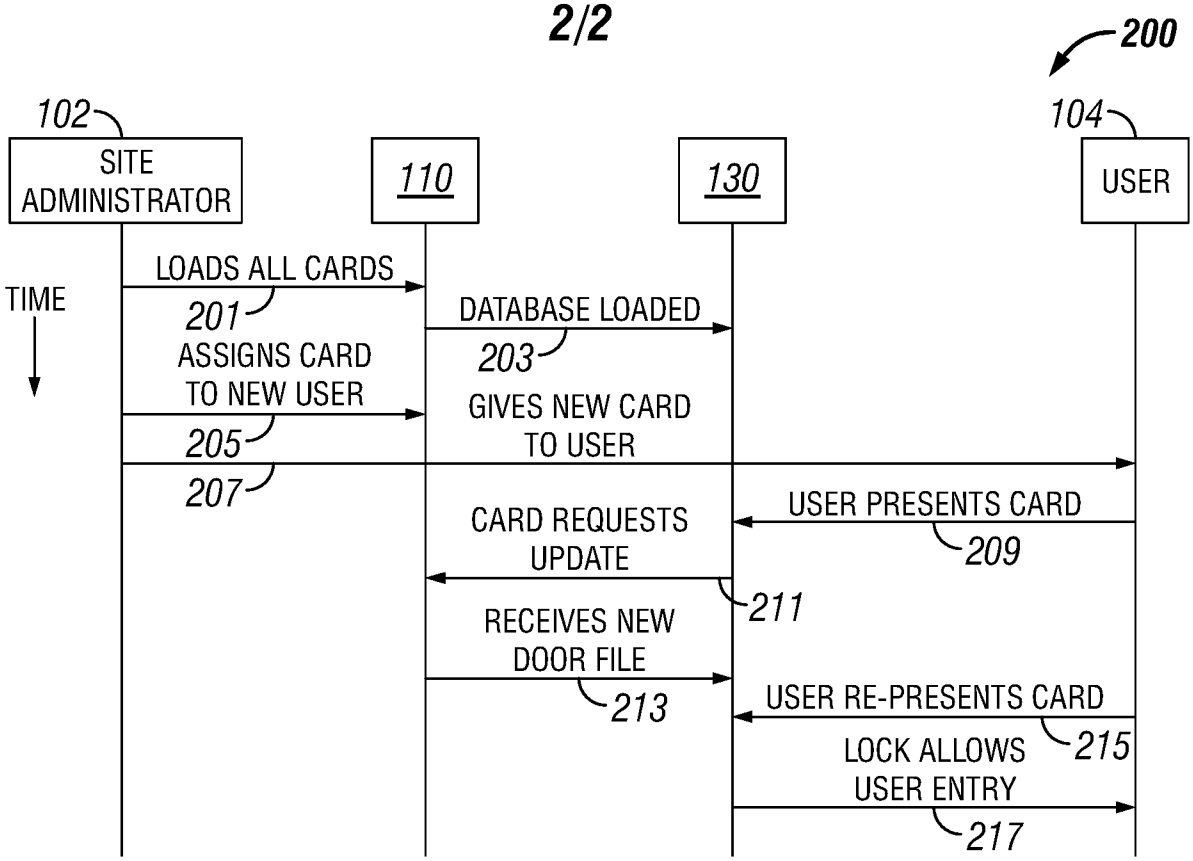

200
102
SITE ADMINISTRATOR
110
130
104
USER
TIME
LOADS ALL CARDS
201
DATABASE LOADED
203
ASSIGNS CARD TO NEW USER
205
GIVES NEW CARD TO USER
207
USER PRESENTS CARD
209
CARD REQUESTS UPDATE
211
RECEIVES NEW DOOR FILE
213
USER RE-PRESENTS CARD
215
LOCK ALLOWS USER ENTRY
217

FIG. 2

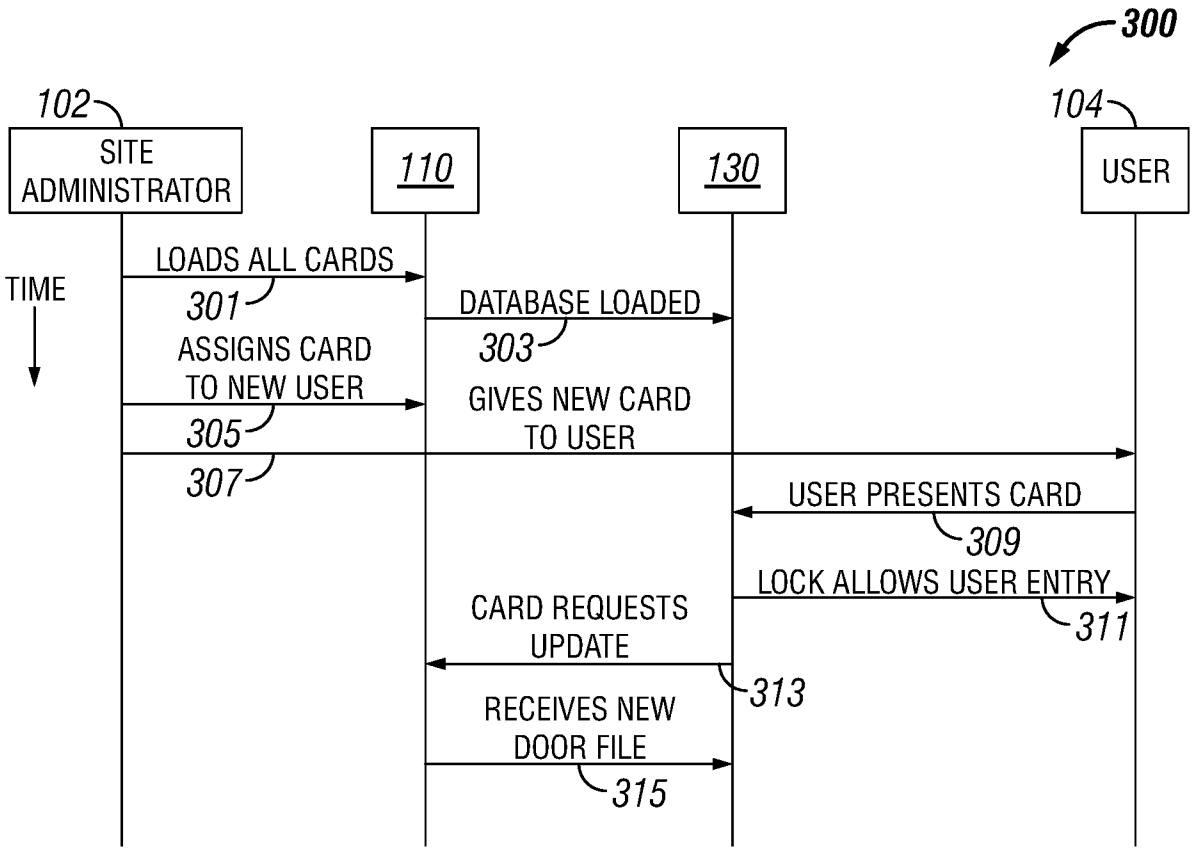

300
102
SITE ADMINISTRATOR
110
130
104
USER
TIME
LOADS ALL CARDS
301
DATABASE LOADED
303
ASSIGNS CARD TO NEW USER
305
GIVES NEW CARD TO USER
307
USER PRESENTS CARD
309
LOCK ALLOWS USER ENTRY
311
CARD REQUESTS UPDATE
313
RECEIVES NEW DOOR FILE
315

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/035036

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - E05B 47/02, E05B 49/00, G05B 19/00, G06F 21/31, G06F 21/34 (2016.01)
CPC - E05B 15/004, E05B 47/0001, E05B 47/0012, E05B 47/02, E05B 47/026, E05B 49/00 (2016.05)
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)
IPC - E05B 47/02, E05B 49/00, G05B 19/00, G06F 21/31, G06F 21/34
CPC - E05B 15/004, E05B 47/0001, E05B 47/0012, E05B 47/02, E05B 47/026, E05B 49/00, E05B 63/04, E05B 2047/002
E05B 2047/0027, E05B 2047/0058, E05B 2047/0067, E05B 2047/0086, E05B 2047/0097, G05B 19/0405, G06F 21/31

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 70/278.1, 70/279.1, 70/280, 340/5.7, 726/5, 726/9 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit, Google Patents, Google Scholar, Google
Search terms used: access control system, data storage, store master credential database

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0077474 A1 (YACOUB et al) 25 March 2010 (25.03.2010), entire document	1-20
Y	US 2008/0163361 A1 (DAVIS et al) 03 July 2008 (03.07.2008), entire document	1-20
Y	US 2011/0252843 A1 (SUMCAD et al) 20 October 2011 (20.10.2011), entire document	8, 9
Y	US 2011/0187505 A1 (FAITH et al) 04 August 2011 (04.08.2011), entire document	12
A	US 2010/0283579 A1 (KRAUS et al) 11 November 2010 (11.11.2010), entire document	1-20
A	US 2011/0311052 A1 (MYERS et al) 22 December 2011 (22.12.2011), entire document	1-20
A	US 2013/0192316 A1 (SCHLAGE LOCK COMPANY LLC) 01 August 2013 (01.08.2013), entire document	1-20
A	US 2013/0212248 A1 (XCEEDLD CORPORATION) 15 August 2013 (15.08.2013), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 July 2016	29 AUG 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)