



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

(21) International Application Number:
PCT/US2019/043343

(22) International Filing Date:
25 July 2019 (25.07.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201811035985 25 September 2018 (25.09.2018) IN

(71) Applicant: **CARRIER CORPORATION** [US/US];
13995 Pasteur Blvd., Palm Beach Gardens, Florida 33418
(US).

(72) Inventors: **EATHAKOTA, Hrishi**; Floor #10, Building
#12C, Raheja Mindspace, Cyberabad, Hitech City, Mad-
hapur, 500081 Hyderabad, Telangana (IN). **BETHALAM,**
Suresh Raju; Floor #10, Building #12C, Raheja Mind-

space, Cyberabad, Hitech City, Madhapur, 500081 Hyder-
abad, Telangana (IN).

(74) Agent: **GASKEY, David J.**; Carlson, Gaskey & Olds, 400
W. Maple Road, Suite 350, Birmingham, Michigan 48009
(US).

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

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

(54) Title: SMART KEY AND ACCESS MANAGEMENT

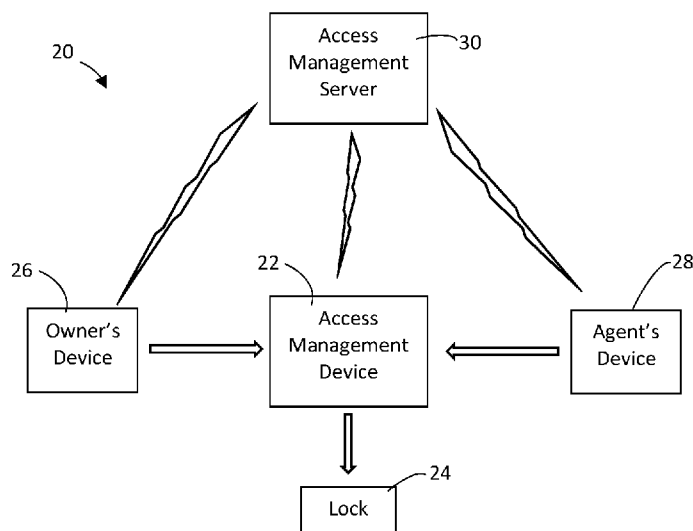


FIG. 1

(57) Abstract: An illustrative example access management device includes a processor, memory associated with the processor, a receiver configured to receive wireless communications, and a transmitter configured to wirelessly communicate with other devices. The memory contains an application. The receiver receives an access request from a user device and the transmitter wirelessly communicate payload to a lock for unlocking the lock when the processor invokes the application in the memory and thereby determines that the received access request is an authorized request.

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))*

SMART KEY AND ACCESS MANAGEMENT

BACKGROUND

[0001] There are various situations in which access to a locked building is needed by someone other than the building owner. For example, when a home is offered for sale potential buyers and real estate agents require access to the home to view its interior. For many years lock boxes have been available to hold a physical key that allows such individuals to unlock a door to the home. Traditional lock boxes require manually entering a code, which is usually a sequence of numbers, on a keypad to open the lock box to retrieve the key. Before leaving, the individual who used the key replaces it in the lock box.

[0002] With advances in electronics it has become possible to eliminate the need to manually enter a code on a keypad of a lock box. Instead, it is now possible to open a lock box using a mobile device, such as a cell phone, to provide an authorization code to open the lock box. The eKey products and services offered by United Technologies allow individuals to open lock boxes through a cell phone or another mobile device.

[0003] With either approach mentioned above, a physical key may be retrieved from a lock box. There are situations, however, in which the lock to be opened does not require or accept a physical key.

SUMMARY

[0004] An illustrative example access management device includes a processor, memory associated with the processor, a receiver configured to receive wireless communications, and a transmitter configured to wirelessly communicate with other devices. The memory contains an application. The receiver receives an access request from a user device and the transmitter wirelessly communicate payload to a lock for unlocking the lock when the processor invokes the application in the memory and thereby determines that the received access request is an authorized request.

[0005] In an example embodiment having one or more features of the device of the previous paragraph, the transmitter transmits a communication to the user device indicating that the access request was denied when the processor determines that the access request was not an authorized request.

[0006] In an example embodiment having one or more features of the device of any of the previous paragraphs, the memory includes a plurality of authorized access request

codes and the processor is configured to determine whether the received access request is an authorized request by comparing a code of the received access request with the stored authorized access request codes.

[0007] In an example embodiment having one or more features of the device of any of the previous paragraphs, the receiver receives the plurality of authorized access request codes from a first user device or a remote server.

[0008] In an example embodiment having one or more features of the device of any of the previous paragraphs, the wireless communications include a close range communication protocol.

[0009] An example embodiment having one or more features of the device of any of the previous paragraphs includes a housing configured to be mounted to a portion of a building near the lock.

[00010] An example embodiment having one or more features of the device of any of the previous paragraphs includes a housing configured to be secured to a portion of a vehicle that includes the lock.

[00011] An illustrative example access management system includes the access management device of any of the previous paragraphs and a server that communicates with other devices to provide the other devices with information regarding authorized access requests.

[00012] In an example embodiment having one or more features of the system of the previous paragraph, the server communicates with the access management device to install the application in the memory.

[00013] An illustrative example method of managing access to an area secured by a lock includes storing an application in memory of an access management device based on a communication from a first user device, receiving an access request from a second user device, using the application in the memory for determining whether the received access request is an authorized request, and using the application in the memory for transmitting payload to the lock for unlocking the lock when the received access request is an authorized request.

[00014] An example embodiment having one or more features of the method of the previous paragraph includes transmitting a communication to the second user device when the access request was determined to be an unauthorized request.

[00015] An example embodiment having one or more features of the method of any of the previous paragraphs includes obtaining a plurality of authorized access request codes and

determining whether the received access request is an authorized request by comparing a code of the received access request with the obtained authorized access request codes.

[00016] In an example embodiment having one or more features of the method of any of the previous paragraphs, obtaining the plurality of authorized access request codes comprises communicating with a server that provides the codes.

[00017] An example embodiment having one or more features of the method of any of the previous paragraphs includes providing the second user device with at least one authorized access request code from a server remote from the access management device.

[00018] An example embodiment having one or more features of the method of any of the previous paragraphs includes unlocking the lock to provide access to one of a vehicle or a building.

[00019] The various features and advantages of at least one disclosed example embodiment will become apparent to those skilled in the art from the following detailed description. The drawings that accompany the detailed description can be briefly described as follows.

BRIEF DESCRIPTION OF THE DRAWINGS

[00020] Figure 1 schematically illustrates an access management system designed according to an embodiment of this invention.

[00021] Figure 2 schematically illustrates an access management device designed according to an embodiment of this invention.

[00022] Figure 3 is a flow chart diagram summarizing an example access management method.

DETAILED DESCRIPTION

[00023] Figure 1 schematically illustrates an access management system 20 that allows individuals to gain access to a locked space, such as the interior of a building or vehicle. An access management device 22 is configured to communicate with other devices including a lock 24, a first user device 26, and a second user device 28. The system 20 also includes an access management server 30.

[00024] When the access management device 22 is used to unlock a door to a building the first user device 26 will usually be an owner's or custodian's device such as a mobile phone and the second user device 28 will usually be owned or used by a real estate agent. When the access management device 22 is used to unlock a door to a vehicle the first user device 26 will usually be used by a dealer representative or custodian of vehicles in inventory

and the second user device 28 will usually be a sales person's or customer's device. In some embodiments the first user device 26 is a mobile station, such as a cell phone. In other embodiments, the first user device 26 is a computing device that communicates with the access management device over a Wi-Fi or wireless local area network connection. In most implementations the second user device 28 will be a mobile station such as a smartphone. These examples are not intended to be limiting.

[00025] Figure 2 schematically illustrates selected portions of an example embodiment of an access management device 22. A processor 32 is associated with memory 34. The processor 32 is configured or programmed to invoke an application in the memory 34 to perform certain functions to allow for access to a space protected by the lock 24 when appropriate criteria are satisfied.

[00026] A receiver 36 is configured to receive wireless communications from other devices, including the first user device 26 and the second user device 28. In some embodiments, the receiver 36 is also configured to communicate directly with the access management server 30.

[00027] A transmitter 38 is configured to wirelessly communicate with other devices including the lock 24 (from Figure 1). In some embodiments, the transmitter 38 also communicates with the owner's device 26, the agent's device 28, and the access management server 30.

[00028] The processor 32, memory 34, receiver 36 and transmitter 38 are illustrated as individual components for discussion purposes. In some embodiments a microprocessor device may include the receiver and transmitter capabilities of the example access management device. Similarly, the memory 34 and the processor 32 may be part of a single device or be separate components.

[00029] The access management device 22 includes a housing 40 that is configured to be situated upon or mounted on a portion of a building that includes an entrance locked by the lock 24. For example, the housing 40 may include a hook or bracket for hanging the access management device 22 on a door handle. In other embodiments, the housing 40 includes adhesive or suction-based mounting features to secure the housing 40 to a flat surface, for example. In some instances, the access management device 22 is supported on a portion of a vehicle and the lock 24 is incorporated into a door of the vehicle.

[00030] Figure 3 is a flowchart diagram 50 that summarizes an example method of managing access to the space protected by the lock 24. At 52, the owner of the access management device 22 or an authorized individual activates that device. In the illustrated

example embodiment, the owner uses the first user device 26 to communicate wirelessly with the access management device 22 for purposes of activating the latter.

[00031] At 54, the owner provides an application to the access management device 22 from or through the first user device 26. For example, the first user device 26 may be capable of sharing an application from the first user device 26 with the access management device 22. This approach allows the access management device 22 to clone the application previously stored on the first user device 26. In some embodiments the communication from the first user device 26 to the access management device 22 instructs the access management device 22 to download the application from the remote server 30.

[00032] The receiver 36 of the access management device receives the application and the processor 32 stores the received application in the memory 34. That application configures the devices 26 and 22, respectively, to communicate an appropriate payload to the lock 24 to unlock the lock 24 to provide access to the associated space, such as the interior of a building or a vehicle. In most cases, the application will be installed on the first user device 26 before being installed on the access management device 22. As part of the initiation or activation at 52 or part of the application provision at 54 the owner or user of the first user device 26 identifies the lock 24 so that the application saved in the memory 34 configures the access management device 22 to communicate with the lock 24. For example, the brand, model number or serial number of the lock 24 will identify the lock 24 sufficiently so that the access management device 22 will be able to provide the appropriate payload when the lock 24 should be unlocked. In many cases, the application will be specific to the lock 24 and initially obtained by the owner or user through the lock manufacturer.

[00033] At 56, the access management device 22 is configured to recognize an authorized access request. In some embodiments, the access management server 30 communicates directly with the access management device 22 over a cellular network connection, for example. In other embodiments, the access management server 30 communicates with the first user device 26 over a wireless cellular communication link, for example, to provide information for identifying authorized access requests to the first user device 26, which in turn provides that information to the access management device 22. In such embodiments, the first user device 26 communicates the authorized access request information to the access management device 22 over a close proximity communication link and the information is then stored in the memory 34.

[00034] Example embodiments include cookies installed in the memory 34 in association with or as part of the installed application. The cookies identify whether a

particular access request is authorized. The cookies may be programmed into the access management device 22 or obtained from the server 30. In some embodiments the information pertaining to an authorized access request includes at least one authorized access code. Given this description those skilled in the art will realize how to configure the access management device 22 to be able to recognize appropriate requests for access that requires unlocking the lock 24.

[00035] Once the access management device 22 has been activated and provided with the application installed in the memory 34 that configures the access management device 22 to communicate the payload for unlocking the lock 24 and at least information for recognizing an authorized access request, it is possible for an individual other than the owner of the building or vehicle protected by the lock 24 to gain access to that building or vehicle by unlocking the lock 24 through communications with the access management device 22. For example, a real estate agent who desires to gain access to a home to show the home to a prospective buyer uses the second user device 28, such as smartphone, to communicate with the access management server 30. The second user device 28 has already stored an application received from the access management server 30 that configures the second user device 28 to communicate an authorized access request to the access management device 22. For example, the application on the second user device 28 may generate a communication including an access request code that corresponds to at least one authorized access request code stored in the memory 34 of the access management device 22. When the second user device 28 is brought in close enough proximity to the access management device 22, the second user device 28 transmits the access request to the access management device 22. The receiver 36 receives the access request at 58.

[00036] At 60, the processor 32 determines if the received access request is an authorized request. In embodiments using access request codes, the processor 32 compares the code of the received access request with authorized access codes in the memory 36. If the access request is authorized, at 62 the processor 32 causes the transmitter 38 to transmit the payload for unlocking the lock 24. The lock 24 responds to the received payload by unlocking, which allows access to the building.

[00037] The system 20 and the technique of unlocking the lock 24 provides security over the payload used for unlocking the lock 24. The agent using the second user device 28 never has access to the payload required by the lock 24 so it cannot be misused or shared with anyone else.

[00038] In some embodiments, an authorized access request code or identifier has a time limit and expires after an appropriate amount of time. In some embodiments, an authorized access request code can only be used from a particular agent's device 28 a predetermined number of times. In such embodiments, the processor 32 is able to determine an identity of the agent's device 28 based on information received by the receiver 36 when the agent's device 28 transmits the access request. The processor 32 determines whether the access code of that request has been transmitted by the agent's device 28 more than an authorized number of times. If so, the processor 32 determines that the access request should be denied as an unauthorized request even though the access code, itself, matches with an access code in the memory 34.

[00039] In some instances, the agent's device 28 will not transmit an authorized access request and when the processor 32 determines that there is no correspondence between a received access request code and any authorized codes within the memory 34, the processor 32 causes the transmitter 38 to provide an indication that the access request is unauthorized and denied at 64. Such an indication may be provided to the agent's device 28, the owner's device 26, the access management server 30, or all of them.

[00040] The illustrated example includes wireless communications between the devices 22, 26, and 28 that occur over a relatively close range using Wi-Fi, Bluetooth or a similar communication protocol. Communications between the access management device 22 and the lock 24 are wireless in this example and utilize a Bluetooth communication link, for example. Communications with the access management server 30 occur over a longer range and may utilize cellular network wireless communication links.

[00041] Embodiments of this invention, such as the disclosed example, provide security over a lock code used for a smart lock that can be unlocked without a physical key. The lock code is maintained secure because only the owner of the lock 24 knows the lock code. The individual using the agent's device 28 never gains access to the actual lock code. Additionally, the host of the server 30 need not obtain the lock code.

[00042] Another feature of embodiments of this invention is that an individual, such as a real estate agent, only needs to install a single application on the agent's device 28 to facilitate communications with the access management server 30 that allows that individual to communicate with a large number of access management devices to be able to unlock a large variety of different types of smart locks that operate without a physical key. It is not necessary for an individual agent to obtain a large number of lock codes nor is it necessary

for an individual to download a large number of applications to be able to communicate with locks of various manufacturers.

[00043] The preceding description is exemplary rather than limiting in nature. Variations and modifications to the disclosed examples may become apparent to those skilled in the art that do not necessarily depart from the essence of this invention. The scope of legal protection given to this invention can only be determined by studying the following claims.

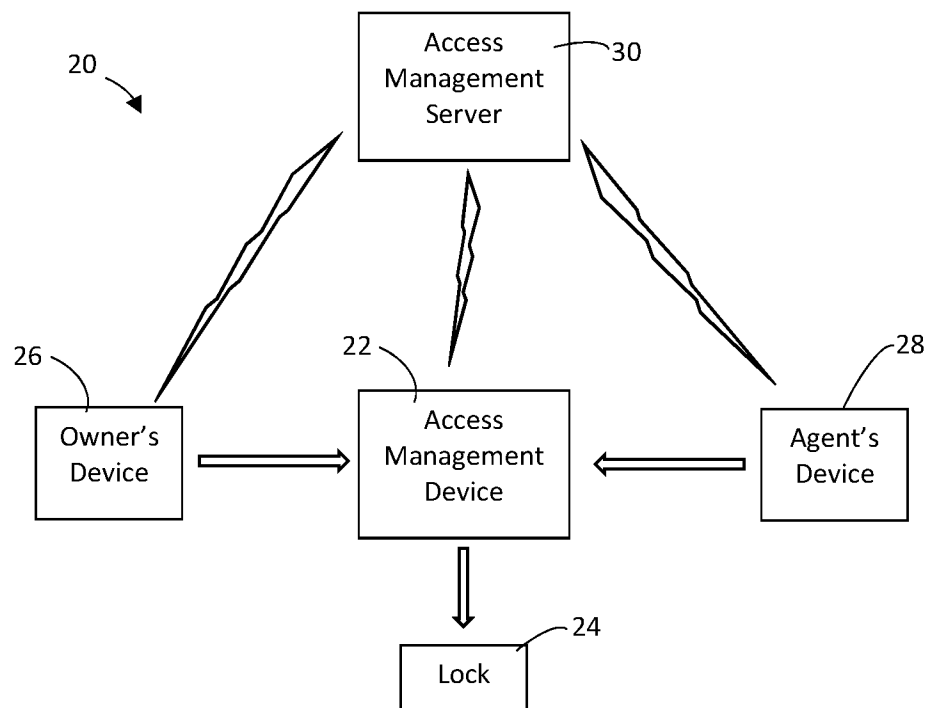
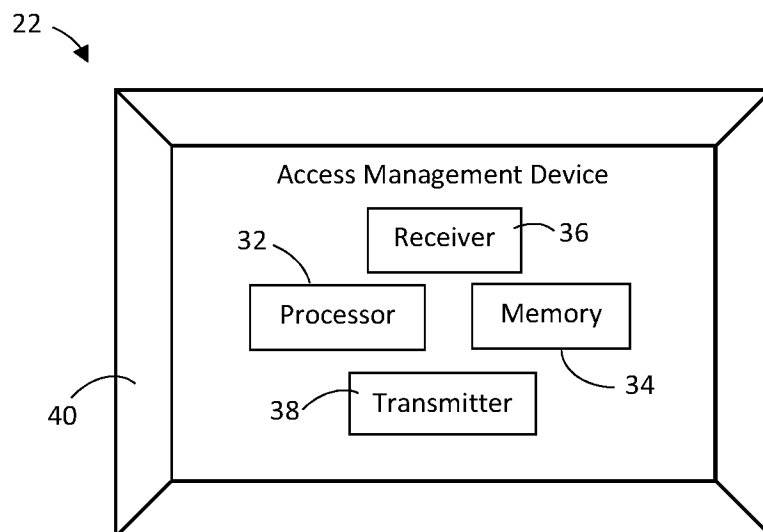
CLAIMS

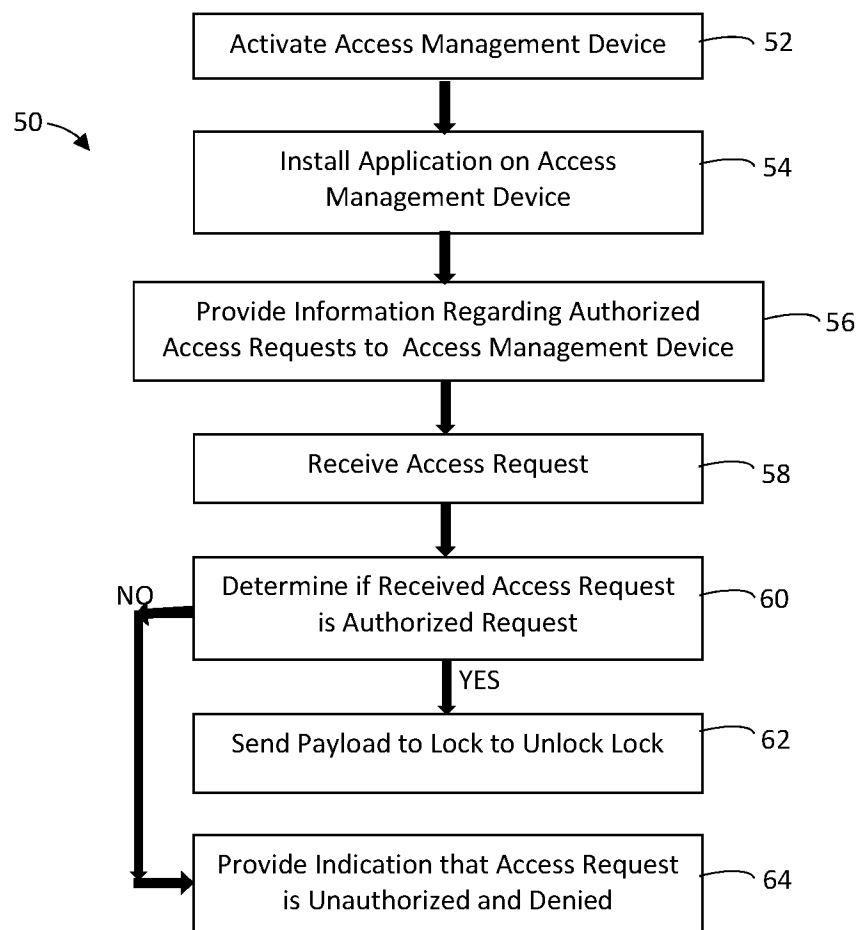
We claim:

1. An access management device, comprising:
a processor;
memory associated with the processor, the memory containing an application;
a receiver configured to receive wireless communications including an access request from a user device; and
a transmitter configured to wirelessly communicate payload to a lock for unlocking the lock when the processor invokes the application in the memory and thereby determines that the received access request is an authorized request.
2. The access management device of claim 1, wherein the transmitter transmits a communication to the user device indicating that the access request was denied when the processor determines that the access request was not an authorized request.
3. The access management device of claim 1, wherein
the memory includes a plurality of authorized access request codes; and
the processor is configured to determine whether the received access request is an authorized request by comparing a code of the received access request with the stored authorized access request codes.
4. The access management device of claim 3, wherein the receiver receives the plurality of authorized access request codes from a first user device or a remote server.
5. The access management device of claim 1, wherein the wireless communications include a close range communication protocol.
6. The access management device of claim 1, comprising a housing configured to be mounted to a portion of a building near the lock.
7. The access management device of claim 1, comprising a housing configured to be secured to a portion of a vehicle that includes the lock.

8. An access management system, comprising:
the access management device of claim 1; and
a server that communicates with other devices to provide the other devices with information regarding authorized access requests.
9. The access management system of claim 8, wherein the server communicates with the access management device to install the application in the memory.
10. A method of managing access to an area secured by a lock, the method comprising:
storing an application in memory of an access management device based on a communication from a first user device;
receiving an access request from a second user device;
using the application in the memory for determining whether the received access request is an authorized request; and
using the application in the memory for transmitting a payload to the lock for unlocking the lock when the received access request is an authorized request.
11. The method of claim 10, comprising transmitting a communication to the second user device when the access request was determined to be an unauthorized request.
12. The method of claim 10, comprising
obtaining a plurality of authorized access request codes; and
determining whether the received access request is an authorized request by comparing a code of the received access request with the obtained authorized access request codes.
13. The method of claim 12, wherein obtaining the plurality of authorized access request codes comprises communicating with a server that provides the codes.
14. The method of claim 10, comprising providing the second user device with at least one authorized access request code from a server remote from the access management device.

15. The method of claim 10, comprising unlocking the lock to provide access to one of a vehicle or a building.

**FIG. 1****FIG. 2**

**FIG. 3**

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/043343

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

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C

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

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

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2018/128754 A1 (CARRIER CORP [US]) 12 July 2018 (2018-07-12) abstract; figure 2 paragraphs [0031] - [0058] -----	1-15
X	EP 2 320 388 A1 (ERICSSON INC [US]) 11 May 2011 (2011-05-11) abstract; figures 1,2,3 paragraphs [0011] - [0029] -----	1-15
X	US 2016/371910 A1 (BAUMGARTE JOSEPH WAYNE [US] ET AL) 22 December 2016 (2016-12-22) abstract; figures 1a,1b,2 paragraphs [0014] - [0033] -----	1-15



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

27 September 2019

Date of mailing of the international search report

07/10/2019

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Pfyffer, Gregor

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2019/043343

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2018128754 A1	12-07-2018	CN 110169031 A WO 2018128754 A1	23-08-2019 12-07-2018
EP 2320388 A1	11-05-2011	AU 2002308549 A1 DK 1423826 T3 EP 1423826 A1 EP 2320388 A1 ES 2507548 T3 KR 20040033285 A PT 1423826 E US 2002178385 A1 WO 02095689 A1	03-12-2002 08-09-2014 02-06-2004 11-05-2011 15-10-2014 21-04-2004 26-09-2014 28-11-2002 28-11-2002
US 2016371910 A1	22-12-2016	US 2016371910 A1 US 2018040184 A1 US 2019043296 A1	22-12-2016 08-02-2018 07-02-2019