(12) STANDARD PATENT (11) Application No. **AU 2017359915 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Access control system having automatic status update

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

(21) Application No: **2017359915** (22) Date of Filing: **2017.11.09**

(87) WIPO No: **WO18/091354**

(30) Priority Data

(31) Number	(32) Date	(33) Country
16198977.7	**2016.11.15**	**EP**

(43) Publication Date: **2018.05.24**
(44) Accepted Journal Date: **2021.02.25**

(71) Applicant(s)
Inventio AG

(72) Inventor(s)
Friedli, Paul

(74) Agent / Attorney
Griffith Hack, Level 10 161 Collins St, MELBOURNE, VIC, 3000, AU

(56) Related Art
WO 2016/139528 A1
US 2014/0292481 A1
US 20140051407 A1

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
24. Mai 2018 (24.05.2018)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2018/091354 A1

(51) Internationale Patentklassifikation:
G07C 9/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/078790

(22) Internationales Anmeldedatum:
09. November 2017 (09.11.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
16198977.7 15. November 2016 (15.11.2016) EP

(71) Anmelder: **INVENTIO AG** [CH/CH]; Seestrasse 55, 6052 Hergiswil (CH).

(72) Erfinder: **FRIEDLI, Paul**; Lindenweg 2, 5453 Remetschwil (CH).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: 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) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT,

(54) **Title:** ACCESS CONTROL SYSTEM HAVING AUTOMATIC STATUS UPDATE

(54) **Bezeichnung:** ZUGANGSKONTROLLSYSTEM MIT AUTOMATISCHER STATUSAKTUALISIERUNG

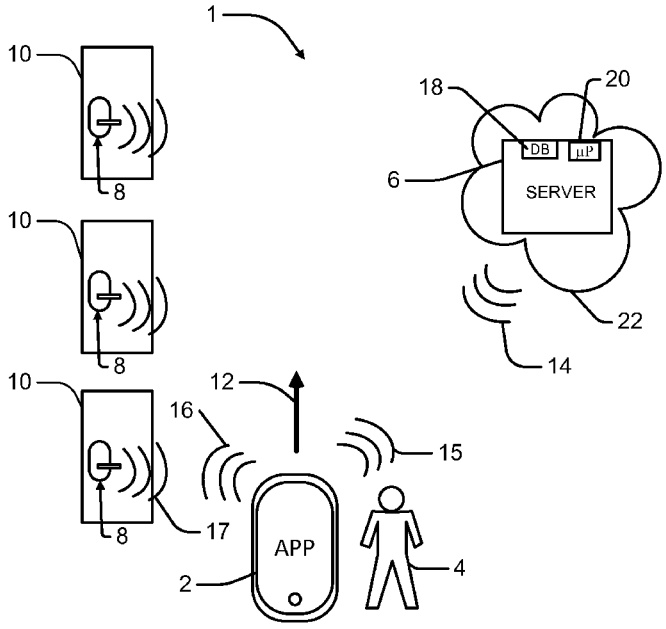

Fig. 1

(57) **Abstract:** In an access control system, a mobile electronic device (2) receives a data signal comprising a lock ID and a lock status identifier when the mobile electronic device (2) is within radio range of an electronic lock (8). The mobile device (2) generates a server message which comprises the lock ID, the lock status identifier and a device ID of the mobile electronic device (2). The mobile electronic device (2) transmits the server message to a data processing device (6) which stores a status of the electronic lock (8) based on an evaluation of the lock status identifier. The data processing device (6) generates a confirmation message containing an electronic code for activating the electronic lock (8) if the electronic lock (8) is inactive and the device ID in the user data file is assigned to the lock ID, and containing a user message if the electronic lock (8) is active or the user (4) has no access authorisation to enter the

WO 2018/091354 A1

[Fortsetzung auf der nächsten Seite]

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).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

restricted access zone assigned to the electronic lock (8).

(57) Zusammenfassung: In einem Zugangskontrollsystem empfängt ein mobileselektronisches Gerät (2) ein Datensignal mit einer Schloss-Kennung und einem Schloss-Zustandsbezeichner, wenn es in Funkreichweite zum elektronischen Schloss (8) ist. Das mobile Gerät (2) erzeugt eine Server-Nachricht, die die Schloss-Kennung, den Schloss-Zustandsbezeichner und eine Geräte-Kennung des mobilen elektronischen Geräts (2) umfasst. Das mobile elektronische Gerät (2) sendet die Server-Nachricht zur Datenverarbeitungseinrichtung (6), die einen Zustand des elektronischen Schlosses (8) basierend auf einer Auswertung des Schloss-Zustandsbezeichners speichert. Die Datenverarbeitungseinrichtung (6) erzeugt eine Bestätigungsnachricht, die einen elektronischen Code zum Aktivieren des elektronischen Schlosses (8) enthält, wenn das elektronische Schloss (8) in einem inaktiven Zustand ist und die Geräte-Kennung in der Nutzerdatei der Schloss-Kennung zugeordnet ist, und die eine Nutzernachricht enthält, wenn das elektronische Schloss (8) im aktiven Zustand ist oder der Nutzer (4) keine Zugangsberechtigung zur dem elektronischen Schloss (8) zugeordneten zugangsbeschränkten Zone hat.

2017359915 21 Jan 2021

Access control system having automatic status update

1. FIELD OF THE INVENTION

The technology described here relates generally to an access control system for a building. Exemplary embodiments of the technology relate in particular to an access control system with an electronic lock which can be actuated by a mobile device and a method for operating such an access control system.

2. BACKGROUND OF THE INVENTION

In known access control systems, doors are fitted with electronic door locks. US patent 9,077,716 for example describes an access control system in which a mobile device communicates with an electronic door lock by means of a Bluetooth or WLAN radio connection and with a web server by means of a WAN (wide area network) radio connection (e.g. GSM) in order to open the electronic lock. To this end, the mobile device sends its device identifier and the identifier of the electronic lock to the web server which checks the access authorization and sends a coded response consisting of a lock command, the lock identifier and a code pattern to the mobile device. The mobile device checks whether the lock identifier is known and if this is the case, activates an opening button to be pressed by the user. If this is pressed within a specified time, the mobile device sends the lock command and the code pattern to the electronic lock. If the lock identifies the lock command and the code pattern as valid, it is opened and the web server receives a confirmation via the mobile device. If the lock is already open however, the web server contains an error message.

This access control system offers a certain user friendliness since the user need not carry a conventional key with him and note any access code. Instead, the mobile device which many users already carry with them for communication purposes in any case affords the function of a key. In order to enable this user friendliness, the access control system requires a complex communication process including the sending of a confirmation or error message to the web server depending on whether the door was closed or open. There is therefore a need for a different, less complex technology.

3. SUMMARY OF THE INVENTION

One aspect of present invention makes available an access control system comprising an

2017359915 21 Jan 2021

electronic lock and a data processing device. The electronic lock is arranged on an access-restricted zone, has an active and an inactive state and comprises a radio transceiver. The radio transceiver is configured to automatically emit a data signal which can be picked-up / received by a mobile electronic device when in radio transmission range and to receive an electronic code from such mobile electronic device, wherein the data signal comprises a lock identifier and a lock state designator. The data processing device contains a database which stores the state of the electronic lock and comprises a user file in which a user is assigned at least one access authorization to an access-restricted zone. The mobile electronic device is provided for communication with the electronic lock and the data processing device, wherein the mobile electronic device is assigned to the user and during operation generates a server message which comprises the lock identifier, the lock state designator and a device identifier of the mobile electronic device. The data processing device is configured to generate a confirmation message, which contains an electronic code for activating the electronic lock when the electronic lock is in the inactive state and the device identifier in the user file is assigned to the lock identifier, and which contains a user message when the electronic lock is in the active state or the user has no access authorization to the access-restricted zone assigned to the electronic lock.

In a further aspect, the present invention provides a method for operating an access control system as noted above. In this access control system, a mobile electronic device receives a data signal with a lock identifier and lock state designator when it is within radio range of the electronic lock. The electronic lock is configured to broadcast such signal automatically (ie without having to receive a request made through or by the mobile electronic device). The mobile device generates a server message which comprises the lock identifier, the lock state designator and a device identifier of the mobile electronic device. The mobile electronic device sends the server message to the data processing device which stores a state of the electronic lock based on an evaluation of the lock state designator. The data processing device thereafter generates a confirmation message which contains an electronic code for activating the electronic lock when the electronic lock is in an inactive state and the device identifier in the user file is assigned to the lock identifier and which contains a user message when the electronic lock is in the active state or the user has no access authorization to the access-restricted zone assigned to the electronic lock.

The technology described here creates an access control system with an improved

2017359915 21 Jan 2021

monitoring and updating of the state of an electronic lock. As soon as the mobile electronic device and the electronic lock come into radio contact, the mobile electronic device picks-up and relays the lock state designator of and broadcast by the electronic lock to the data processing device. The data processing device then updates the state of this electronic lock in its database. In other words, therefore, each electronic lock itself ensures that the database stores its current state through interaction with the mobile device. This process takes place automatically without the user having to be active.

In order to be able to store the current state in the data processing device, the lock state designator is evaluated, for example, by a processor in the data processing device. The evaluation is thus made centrally in the data processing device so that the mobile electronic device can relay the state designator without evaluation.

The automatic state updating is advantageous if several persons are located in the building and for example are located on a floor near a door with an electronic lock or are passing by. If their mobile electronic devices come within the radio range of the electronic lock, each mobile electronic device generates a server message and sends it to the data processing device. After receiving each server message and evaluating the lock state designator contained therein, the data processing device stores the state of the electronic lock. Each mobile electronic device therefore contributes to the stored state of the electronic lock being up-to-date and specifically independently of whether its user wishes access to a door or not.

In one embodiment the mobile electronic device sends the confirmation message to the electronic lock when the electronic lock is in the inactive state and the device identifier in the user file is assigned to the lock identifier. The electronic lock is then activated when the electronic code of the confirmation message agrees with a reference code stored in the electronic lock. This is also accomplished in one embodiment without assistance of the user. As long as the mobile electronic device is located in the radio range of the electronic lock, it is not necessary for the user to make use of the mobile electronic device or move towards the electronic lock.

In a modification to the previous embodiment it can be provided in one embodiment that the user has to bring the mobile electronic device into the vicinity of the electronic lock

2017359915 21 Jan 2021

when this lock is to be activated. In this embodiment the mobile electronic device sends the confirmation message to the electronic lock when the mobile electronic device is at a distance from the electronic lock which is shorter than a specified maximum distance . The electronic lock is activated when the electronic code of the confirmation message agrees with a reference code stored in the electronic lock. These alternatives regarding what the user has to do when access to a zone is desired, allow the access control system to adapt flexibly to the requirements in a building.

The technology described also allows flexibility with regard to the manner whether and how the user is to be informed. In one embodiment the information is accomplished by means of the mobile electronic device which the user carries with him. The mobile electronic device generates the notification based on the confirmation message. The notification can be presented visually and/or audibly, e.g. by means of at least one notification type, wherein the notification type is selected from a group comprising text, symbols, pictograms, speech, tones and sounds.

In one embodiment, the confirmation message contains, in addition to the electronic code, a further electronic code which is stored in the electronic lock and is valid for a future activation of the electronic lock. The further electronic code constitutes the reference code for the future activation. This enables a flexible choice of a desired security level. If a high security level is desired, the electronic code can only be used once on the electronic lock. If the electronic lock is to be activated again thereafter, the electronic code sent with the confirmation message must then correspond to the further electronic code (reference code). If a lower security level is desired, the reference code can be replaced, for example, after a certain usage time or after a certain number of activations of the electronic lock by the further electronic code.

In one embodiment the radio communication between the mobile electronic device and the electronic lock is based on a Bluetooth standard. In particular smartphones are fitted with this radio technology so commercially available devices can be used for the technology described here.

Various aspects of the improved technology in accordance with the various aspects of the invention are explained in detail hereinafter with reference to embodiment in conjunction

2017359915 21 Jan 2021

with the figures. In the figures the same elements have the same reference numbers.

4. BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 shows a schematic diagram of an exemplary access control system combined with several building doors;

Fig. 2 shows a schematic diagram of an embodiment of an electronic lock; and

Fig. 3 shows a flow diagram of an embodiment of a method for operating the access control system.

5. DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Figure 1 shows a schematic diagram of an exemplary access control system 1 combined with a building of which only doors 10 are shown for diagrammatic reasons. The access control system 1 shown in Fig. 1 comprises electronic locks 8, a mobile electronic device 2 (hereinafter also designated as mobile device 2) which a user 4 carries with him and a computer system 6, hereinafter designated as server 6, which has a data memory 18 and a processor 20. Each electronic lock 8 has an individual identifier which uniquely characterizes the lock 9 and is stored in an internal memory 34 and two states (an open/unlocked state and a closed/locked state). These states are represented by a lock state designator (hereinafter also called "state designator"). In the situation shown the user moves towards the doors 10 which is indicated by an arrow 12. Figure 1 additionally shows symbols for radio connections 14, 15, 16, 17 which are used for wireless communication in the access control system 1.

The doors 10 delimit zones or spaces to which only authorized persons have access from regions which are subjected to no or a different access restriction. The doors 10 can be building outer doors or building inner doors. Depending on the use of the building, for example as a residential and/or commercial building, the doors 10 in the building interior can be apartment doors, floor doors or office doors. The situation shown in Fig. 1 can, for example, exist on a hallway of a building floor from which individual apartments or offices can be entered. The person skilled in the art identifies that examples of application instead of a door 10, a barrier, a gate, a turnstile or another type of barrier can be used to either block or release access. In the embodiment shown each door 10 has an electronic lock 8 for locking the door 10.

2017359915 21 Jan 2021

In the situation shown in Fig. 1 the technology described here can advantageously be used to operate the access control system 1 with the lowest possible complexity and to grant the user 4 convenient access to the desired zone. Summarized briefly and as an example, the operation of the access control system takes place as follows: when the user 4 moves in the building, his mobile device 2 receives from each door 10 which he approaches or which he passes-by its lock identifier and the relevant lock state designator. The mobile device 2 sends the received information together with its device identifier to the server 6 which then stores the state of the door 10 or its electronic lock 8 and checks whether the user 4 is access-authorized to the door 10. If this is the case, the server 6 sends an electronic code for further use to the mobile device 2. In one embodiment the mobile device 2 sends the code automatically to the electronic lock 8 in order to activate or open this. If the user 4 desires access to this now unlocked door 10, he can pass through it into the access-restricted zone. In another embodiment, the electronic lock 8 is only activated, for example, when the user 4 holds the mobile device 2 relatively close (e.g. at a distance of several centimetres) to the electronic lock 8.

Since each lock 8 automatically sends, in addition to its lock identifier, also its lock state designator and specifically regardless of whether the user 4 desires access to a door 10 or not, the states of the doors 10 are automatically updated in the server 6. Particularly when several users 4 are located on the building floor and are going past the doors 10, the crowd of users 4 communicates with the server 6. The server 6 uses the plurality of received lock state designators to continuously update the states of the doors 10 and specifically without the users 4 needing to be active.

For its function in the access control system 1 the mobile device 8 is fitted with corresponding hardware (e.g. one or more radio modules) and corresponding software (e.g. one or more application programs or application-specific software (also designated as "App")). Depending on the configuration of the mobile device 2, for example, each radio module and each App can be selectively activated and deactivated via a graphical user interface (also designated as graphical user interface, GUI) of the mobile device 2. The mobile device 2 can, for example, be a mobile telephone, a smartphone, a tablet PC, a smartwatch, glasses with a miniature computer or another computer-assisted device worn on the body (also designated as "wearable device").

2017359915 21 Jan 2021

As mentioned, communication in the access control system 1 takes place by means of the radio connections 14, 15, 16, 17 wherein the radio connections 16, 17 are used for communication between the electronic lock 8 and the mobile device 2 and the radio connections 14, 15 are used for communication between the mobile device 2 and the server 6. The radio connections 16, 17 can, for example, be based on a known radio technology for short distances, e.g. Bluetooth, NFC (near field communication), WiFi/WLAN or RFID technology. The radio connections 14, 15 can, for example, be based on a known radio technology for mobile telephone/data communication, e.g. according to a mobile radio standard for GSM (global system for mobile communications), UMTS (universal mobile telecommunications system) or LTE (long term evolution).

In one embodiment, the electronic lock 8 comprises a radio module which is based on Bluetooth technology. Accordingly, the mobile device 2 is configured for a communication based on Bluetooth technology. If the mobile device 2 is, for example, a Smartphone, the user 4 can selectively activate and deactivate the Bluetooth function via the graphical user interface of the Smartphone. In the activated state the radio module continuously sends the individual lock identifier (e.g. "ID: 12345") together with the lock state designator (e.g. "status: closed") for example in the form of a digital data signal. The mobile device 2 receives the digital data signal when it is in radio range; i.e. the data signal sent by the electronic lock 8 has a signal strength (expressed by an RSSI value (received signal strength indicator) at the location of the mobile device 2 (receiving location) which is greater than a threshold value specified for a secure receipt.

The mobile device 2 (e.g. one or more installed software applications) generates from the received lock identifier, the received lock state designator and its device identifier a digital data signal (server message) and sends it by means of the radio connection 15 to the server 6. The processor 20 of the server 6 processes this data signal (server message) and controls the storage of the lock state designator in the data memory 18. In one embodiment the server 6 is a computer system which provides computer functionalities such as service programs, data or other resources (e.g. access to a file system or a database) so that other computers (e.g. the mobile device 2) or programs ("clients") can access them via a network 22. Standardized transfer protocols (e.g. HTTP, HTTPS) and network protocols such as, for example, IP and TCP are used as transfer methods. The general function of a server is known to the person skilled in the art so that only the aspects which

2017359915 21 Jan 2021

seem helpful for an understanding of the technology described here are discussed.

The data memory 18 stores in a database a user file in which it is specified for each user 4 of the building at which door 10 the user 4 is access-authorized. A user 4 can also be access-authorized to several doors 10. In one embodiment each mobile device 2 and therefore each device identifier is allocated to a user 4. For this a first group of datasets is placed in the user files wherein in one dataset at least one door 10 at which the user 4 is access-authorized is assigned to a device identifier. In one embodiment a second group of datasets is placed in the user file wherein for each door 10 there exists a dataset which stores the state (e.g. open/closed or unlocked/locked) of the door 10 in the form of the lock state designator. With the aid of the user file it can thus be checked inter alia whether the user 4 of the mobile device 2 is access-authorized for the door 10. Alternatively to such an organisation of the datasets into two groups, the datasets can also be organized in a single group in another embodiment.

In one embodiment, the server 6 is arranged in the building in order to process and store data locally. Communication with the mobile device 2 can then be made, for example, via a WiFi/WLAN radio connection or a mobile radio network connection. The access control system 1 can thus be considered as a central/local access control system 1 intended for a building. The functions of the server 5 can, for example, be integrated in a building server which executes further building-specific functions.

In another embodiment, the server 6 is arranged outside the building, for example in a remote service centre which, along with other services also executes access control for the building. The service centre can execute these services for one or more buildings. Communication with the mobile device 2 can then be accomplished, for example, via a radio connection by means of a mobile radio network or by means of a combination of WiFi/WLAN and WAN, including the internet. The access control system 1 can thus be viewed as a decentralized access control system 1.

The server 6 stores the state of the electronic key 8 and its processor 20 generates a confirmation message which the server 6 sends to the mobile device 2. The content of the confirmation message depends on the state of the electronic key 8 and on the access authorization of the user 4. The confirmation message contains, for example, an electronic

2017359915 21 Jan 2021

code for activating the electronic lock 8 when the electronic lock 8 is in the inactive/closed state and the device identifier in a user file is assigned to the lock identifier; this also means that the user 4 is access-authorized. If, on the other hand the electronic lock 8 is in the active/open state and the user 4 has no access authorization to the access-restricted zone assigned to the electronic lock 2, the confirmation message contains a user message which informs the user 4 of this.

Figure 2 shows an embodiment of the electronic lock 8 with a latchkey 24 such as can be used on the door 10. A door leaf 10a and a door frame 10b are shown of the door 10. The person skilled in the art identifies that instead of the latchkey 24, another possible handle, for example, a doorknob or a handle recess can be provided to open the door 10. If the door 10, in another embodiment, is fitted with a drive motor, a possible handle on the door 10 can possibly be dispensed with. For diagrammatic reasons a possibly provided strike plate, a door handle and a possibly provided bolt are not shown. When the door 10 is closed in one embodiment the door handle and/or the bolt engage in the strike plate of the door frame 10b. The electronic lock 8 can also be arranged completely or partially in the door frame 10b.

On the door leaf side, Fig. 2 additionally shows a radio module 30 (shown as transceiver TX/RX) and an unlocking device 26 which is coupled to the radio module 30 via a connection 28. The radio module 30 (e.g. as Bluetooth radio module) is provided for communication with the mobile device 2 by means of the radio connections 16, 17. The part of the door frame 10b shown in Fig. 2 is, for example, integrated in a building wall and comprises an unlocking device 32. The unlocking device 32 is optional since depending on the configuration of the electronic lock 8, either the door frame 10b or the door leaf 10a can contain an unlocking device (26, 32). If the unlocking device 32 is present on the frame side, the radio module 30 can also be arranged on the door frame 10b.

The unlocking devices 26, 32 have an electromechanical mechanism which in one embodiment contains an electromagnetically activatable barrier or an electromagnetically activatable bolt or pin. In another embodiment, the electromechanical mechanism can comprise an electric motor which drives a bolt or pin. The electric motor can, for example, push the bolt into the strike plate of the door frame 10b and withdraw it from this. The electromechanical mechanism can be activated by a control signal (hereinafter also

2017359915 21 Jan 2021

designated as activation signal). The control signal can, for example, be generated by the unlocking device 26 itself or received by the mobile device 2.

For diagrammatic reasons the doors 10 shown in Fig. 1 and Fig. 2 are shown with latch-keys 24 as possible handles so that the user 4 can open the desired door 10. The person skilled in the art identifies that a door 10 can, for example, be fitted with an electric (motor) drive which automatically opens and closes the door 10 without assistance of the user 4 as soon as the electronic lock 8 is unlocked. Depending on the configuration, a possible handle can possibly be omitted. The door 10 can, for example, be configured as a sliding door which can be slid laterally by a sliding mechanism after unlocking.

The electronic lock 8 contains a processing device 36 and an internal memory 34 which in one embodiment is arranged in the unlocking device 26, 32 or are connected to said device. The internal memory 34 stores the lock identifier, the lock state designator and an electronic reference code. The processing device 36 checks whether an electronic activation code received by the mobile device 2 agrees with the stored electronic reference code. If this is the case, the electronic lock 8 is activated.

With the understanding of the above-described fundamental system components and their functionalities, a description of an exemplary method for operating the access control system 1 is made in the following. The description is made with reference to a user 4 who wishes to enter at a door 10, for example to his office. This access authorization and possible others are stored in the user file for this user 4. The user 4 carries the mobile device 2 with him and has activated the software application and the radio modules (e.g. for Bluetooth communication and mobile radio communication). The method begins in a step S1 and ends in a step S10.

When the user 4 with his mobile device 2 moves towards a door 10, in a step S2 the mobile device 2 receives a data signal emitted by the electronic lock 8 with its lock identifier and lock state designator. The lock state designator specifies whether the lock 8 has a status/state “open”/“active” or a status/state “closed”/”inactive”. In this embodiment the electronic lock 8 and the mobile device 2 communication via a Bluetooth radio connection.

2017359915 21 Jan 2021

In a step S3 the mobile device 2 generates from this and its own device identifier a server message and sends this to the server 6 in a step S4. The mobile device 2 sends the server message according to a specified protocol for mobile radio communication to a radio network access node which relays the server message to the server 6. The person skilled in the art is familiar with the fundamental operating mode of the communication between the mobile device 2 and the server 6 from the field of mobile radio communication so that extensive explanations do not seem necessary.

When the server 6 receives the server message from the mobile device 2, it analyzes the server message to obtain from this the device identifier, the lock identifier and the state designator. The server message therefore specifies from which mobile device 2 is was sent (device identifier), which electronic lock 8 is involved (lock identifier) and in which state the electronic lock 8 is located (state designator). It is therefore also known that the user 4 of the mobile device 2 is located in the vicinity of the electronic lock 8 with this lock identifier. Since the mobile device 2 is assigned to the user 4, the server 6 determines the identity of the user 4 with the aid of the user file.

In a step S5 the server 6 stores the state of the electronic lock 8 in the database 18. As a result of this storage a possibly stored state for this electronic lock 8 is overwritten. Accordingly, the current state of the electronic lock 8 is stored in the database 18.

In a step S6 the server 6 checks using the stored state of the electronic lock 8 whether the electronic lock 8 is active, i.e. open/unlocked or inactive, i.e. closed/locked. In addition, in step S6 the server 6 checks using the device identifier and/or the determined identity of the user 4 whether the user 4 is access-authorized at the door 10 to which the electronic lock 8 is assigned. An access authorization exists, for example, when the device identifier or the identity of the user 4 in the user file are assigned to the lock identifier. If both conditions are satisfied, the method proceeds along the yes branch to a step S7. If on the other hand they are not satisfied, the method proceeds along the no branch to a step S9.

Depending on the result of the examination in step S6, the server 6 generates a confirmation message. If the electronic lock 8 is in the inactive/closed stat and if the user 4 is access-authorized, the server generates an electronic activation code in step S7. In one embodiment the activation code is only valid at this electronic lock 8. The validity can be

2017359915 21 Jan 2021

subject to time restrictions, for example, it can be valid only at specific times (e.g. during business hours) or only for a specified time duration. The confirmation message generated by the server 6 comprises the activation code, including possible time restrictions, the lock identifier and possibly the device identifier of the mobile device 2 to which the server 6 sends the confirmation message.

In one embodiment the confirmation message comprises a further electronic code in addition to the electronic activation code. This further electronic code is transmitted together with the activation code to the electronic lock 8 and stored in the internal memory of the electronic lock 8. The further electronic code is valid for a future activation of the electronic lock 8, for example, the activation following the instantaneous activation. For this following activation the further electronic code forms the reference code.

If the electronic lock 8 is in the active/open state or the user 4 is not access-authorized, in step S9 the server 6 generates a user message. An activation code is not necessary in these situations. Depending on the configuration of the system, the user message can have different contents. The user message can inform the user 4, for example that the door 10 is open or that he has no access authorization for it. When the mobile device 2 receives the user message, it can generate a visual and/or audible notification from this. The notification can be formed by at least one type of notification which is selected from a group comprising text, symbols, pictograms, speech, tones and sounds. Alternatively to this or additionally, the electronic lock 8 can have a device for such a type of notification (e.g. an LED display for different colours (e.g. red, green) or an LCD display in each case with or without loudspeaker or buzzer).

In a step S8 the mobile device 2 receives the confirmation message which either comprises the activation code generated in step S7 or the user message generated in step S9. The communication between the server 6 and the mobile device 2 is made by means of the above-described mobile radio communication.

If the confirmation message contains the activation code for the door 10 near which the user 4 is located, if the activation code agrees with the reference code, the electronic lock 8 can thus be unlocked and the door 10 thereby opened. The state of the electronic lock 8 is now active or unlocked; the lock state designator follows this change of state. The state

2017359915 21 Jan 2021

designator remains in this state until the door 10 is closed again and the electronic lock 8 is locked.

As already mentioned above, in one embodiment the mobile device 2 can automatically and without further assistance of the user 4, send the activation code to the electronic lock 8 in order to activate or open this. In this embodiment the mobile device 2 transmits with a transmission power so that the electronic lock 8 can receive the confirmation message. The transmission power is selected so that a radio transmission is possible over a distance of about 50 cm to a few metres. A distance of about 50 cm to about 1 meter can exist, for example, if the user 4 approaches a door 10 on a floor hallway or goes past this.

In another embodiment the mobile device 2 sends the activation code with a transmission power which is provided for a radio connection over a short distance. In this case, the user 4 must hold the mobile device 2 relatively close to the electronic lock 8 if he wishes to access at this door 10. For this purpose, a maximum distance can be specified in one embodiment. A radio connection comes about when a distance between the electronic lock 8 and the mobile device 2 is shorter than the specified maximum distance. Depending on the configuration, the maximum distance can be between about 0 cm and about 10 cm, wherein a distance of 0 cm means that the mobile device 2 is touching the electronic lock 8. The transmission power is adapted to this maximum distance.

When the door 10 is unlocked, the user 4 can open the door 10 and enter the access-restricted zone through it. In this state or during this process the electronic lock 8 sends its lock identifier and the lock state designator (accordingly: “open”/”unlocked”). As soon as the mobile device 2 of the user 4 has sent the activation code, it can again receive the lock identifier and the lock state designator of the electronic lock 8 since it is still in radio range. The mobile device 2 sends this information to the server 6 which then updates the status for this electronic lock 8 in the database as described above. If, for example, the user 4 has entered the access-restricted zone and then closes the door 10 after him, The state designator characterizes the closed/locked state of the door 10. The server message sent by the mobile device 2 then causes the server 6 to update the status in the database (e.g. set to “closed/locked”).

If further mobile devices 2 are located in radio range of the electronic lock 8, each mobile

2017359915 21 Jan 2021

device 2 receives the lock identifier and the lock state designator of this electronic lock 8 and communicates it to the server 6. Each of these mobile devices 2 thus contributes to the server 6 storing the current state of the electronic lock 8 and specifically regardless of whether the user thereof wishes access to the door 10. This can be helpful, for example, when the mobile device 2 of the user 4 who is going through the door 10 cannot receive the lock identifier and the lock state designator sent by the electronic lock 8. The user 4 can, for example, go too quickly through the door 10 so that at the transmission time of the electronic lock 8 the mobile device 2 is outside the radio range. In this case, the mobile device 2 sends no server message and there is no updating of the status in the server 6. The database can, for example, still display the status “open” although the door 10 is already closed again and the electronic lock 8 is locked.

2017359915 21 Jan 2021

Patent claims

1. A method for operating an access control system which comprises an electronic lock having an active and an inactive state at an access-restricted zone, the electronic lock having a radio transceiver configured for automatically emitting data signals containing a lock state designator and a lock identifier, a data processing device with a database configured to store the state of the electronic lock and a user file in which a user is assigned at least one access authorization to an access-restricted zone, and a mobile electronic device to be carried by the user and which has a device identifier and is configured for communication with the electronic lock and the data processing device, wherein the method comprises the following steps:

- receiving, by the mobile electronic device, the data signal emitted by the electronic lock radio transceiver, when the mobile electronic device is within radio range of the electronic lock;
- generating a server message by the mobile electronic device, the server message comprising the lock identifier, the lock state designator and the device identifier of the mobile electronic device;
- sending the server message by the mobile electronic device to the data processing device in a first radio transmission;
- storing the state of the electronic lock in the data processing device based on an evaluation of the lock state designator contained in the server message;
- generating a confirmation message by the data processing device, wherein the confirmation message:

  contains an electronic code for activating the electronic lock when the electronic lock is in the inactive state and the device identifier in the user file is assigned to the lock identifier and

  contains a user message when the electronic lock is in the active state or the user has no access authorization to the access-restricted zone assigned to the electronic lock; and
- receiving, by the mobile device, a second radio transmission containing the confirmation message.

2. The method according to claim 1, further comprising:

- sending the confirmation message by the mobile electronic device to the electronic lock

2017359915 21 Jan 2021

radio transceiver when the electronic lock is in the inactive state and the device identifier in the user file is assigned to the lock identifier; and
- activating the electronic lock when the electronic code contained in the confirmation message agrees with a reference code stored in the electronic lock.

3. The method according to claim 1, further comprising:
- sending the confirmation message by the mobile electronic device to the electronic lock radio transceiver when the mobile electronic device is at a distance from the electronic lock which is shorter than a specified maximum distance; and
- activating the electronic lock when the electronic code contained in the confirmation message agrees with a reference code stored in the electronic lock.

4. The method according to any one of claims 1 to 3, further comprising the data processing device evaluating the lock state designator in order to store the state of the electronic lock in the data processing device.

5. The method according to any one of the preceding claims, further comprising generating a user information notification by the mobile electronic device, wherein the generation of the notification is based on a content of the confirmation message.

6. The method according to claim 5, further comprising presenting the user information notification by at least one notification type, wherein the notification type is selected from a group comprising text, symbols, pictograms, speech, tones and sounds.

7. The method according to any one of the preceding claims, wherein several mobile electronic devices are in the radio range of the electronic lock, wherein each of the several mobile electronic devices is configured to generate a server message in accordance with claim 1 and sends it to the data processing device, and wherein the data processing device, after receiving each such server message and evaluating the lock state designator contained therein stores the state of the electronic lock.

8. The method according to any one of the preceding claims, wherein the confirmation message contains, in addition to the electronic code, a further electronic code which is stored in the electronic lock and is valid for a future activation of the electronic lock.

2017359915 21 Jan 2021

9. An access control system, comprising:

- an electronic lock which is located at an access-restricted zone, has an active and an inactive state and comprises a radio transceiver configured to emit a data signal and receive an electronic code, wherein the data signal comprises a lock identifier and a lock state designator;

- a mobile electronic device assigned to a user configured for (i) receiving data signals emitted by the electronic lock transceiver when within radio range of the electronic lock transceiver, (ii) during operation generating and wirelessly transmitting a server message which comprises the lock identifier, the lock state designator and a device identifier of the mobile electronic device, (iii) wirelessly receiving signals containing a confirmation message and (iv) wirelessly transmitting signals to the electronic lock transceiver containing the electronic code; and

- a data processing device with a database which stores the state of the electronic lock received via the mobile electronic device and comprises a user file in which the user is assigned at least one access authorization to an access-restricted zone, wherein the data processing device is configured for receiving and analysing the server message to obtain from this the device identifier, the lock identifier and the state designator, and wherein the data processing device is arranged for wireless communication with the mobile electronic device and for generating the confirmation message, wherein the confirmation message:

contains the electronic code for activating the electronic lock when the electronic lock is in the inactive state and the device identifier in the user file is assigned to the lock identifier; and

contains a user message when the electronic lock is in the active state or the user has no access authorization to the access-restricted zone assigned to the electronic lock.

10. The access control system according to claim 9, wherein the electronic lock has a storage device which stores the lock identifier and an electronic reference code, and a processing device configured to activate the electronic lock when the electronic code of the confirmation message agrees with the electronic reference code.

11. The access control system according to claim 9 or 10, wherein the electronic lock has an unlocking device configured to unlock a door in the active state and locks the door

2017359915 21 Jan 2021

in the inactive state.

12. The access control system according to any one of claims 9 to 11, wherein the radio transceiver of the electronic lock is configured to receive the electronic code when the mobile electronic device is at a distance from the electronic lock which is shorter than a specified maximum distance.

13. The access control system according to any one of claims 9 to 12, wherein the radio transceiver of the electronic lock comprises a radio module for communication according to a Bluetooth standard.

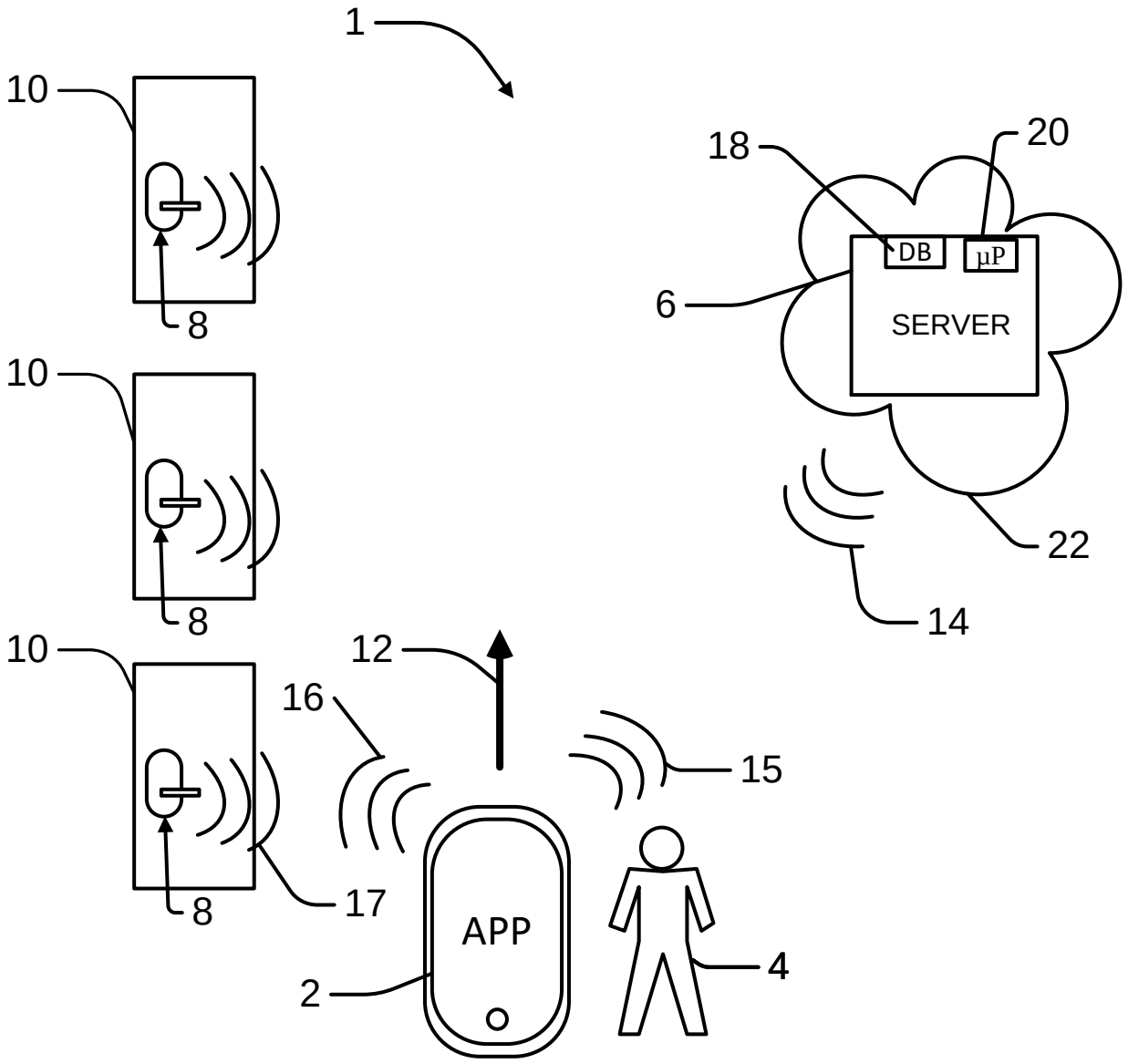

Fig. 1

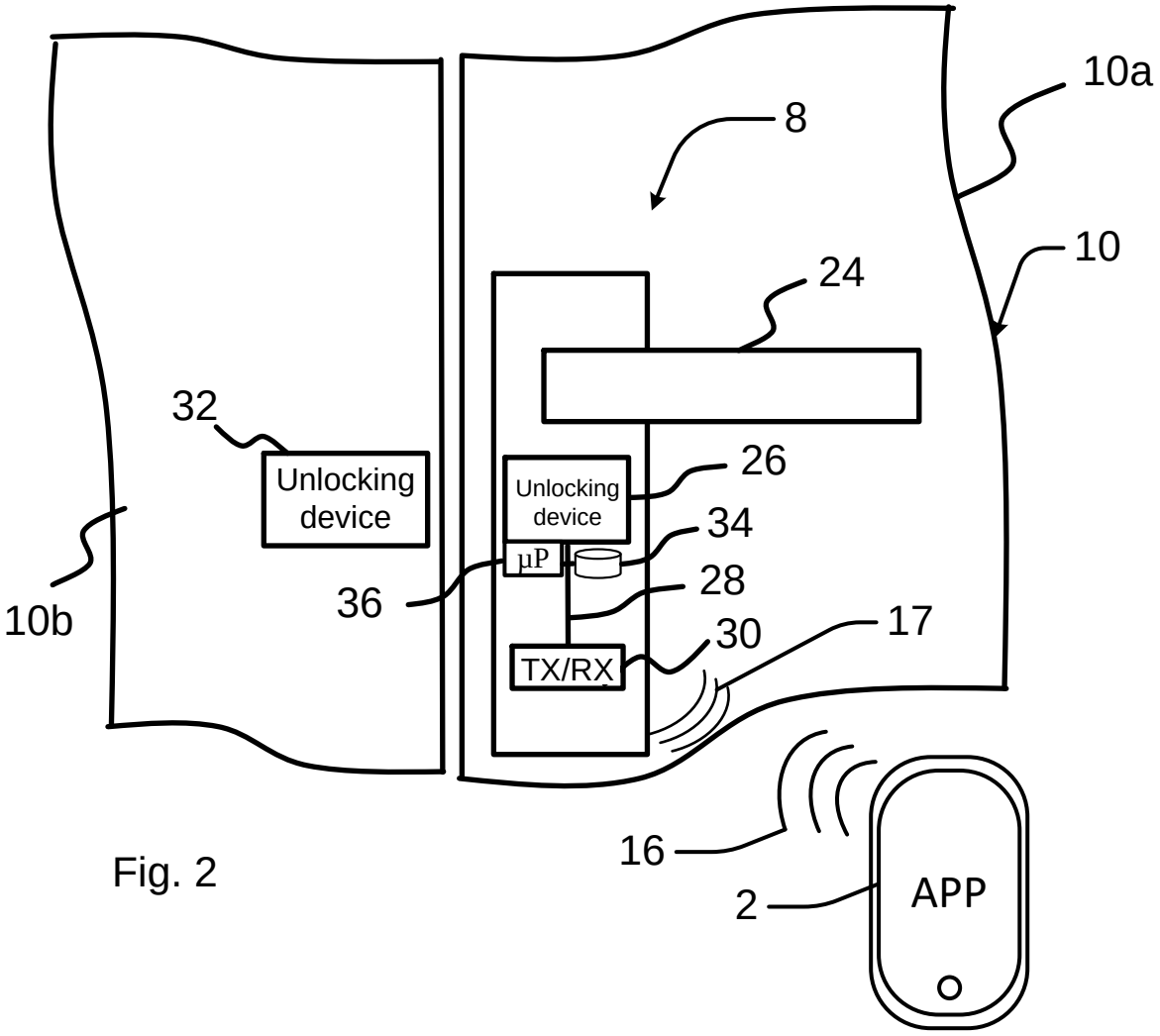
10a
8
10
24
32
Unlocking device
26
Unlocking device
34
µP
36
28
10b
30
17
TX/RX
16
2
APP

Fig. 2

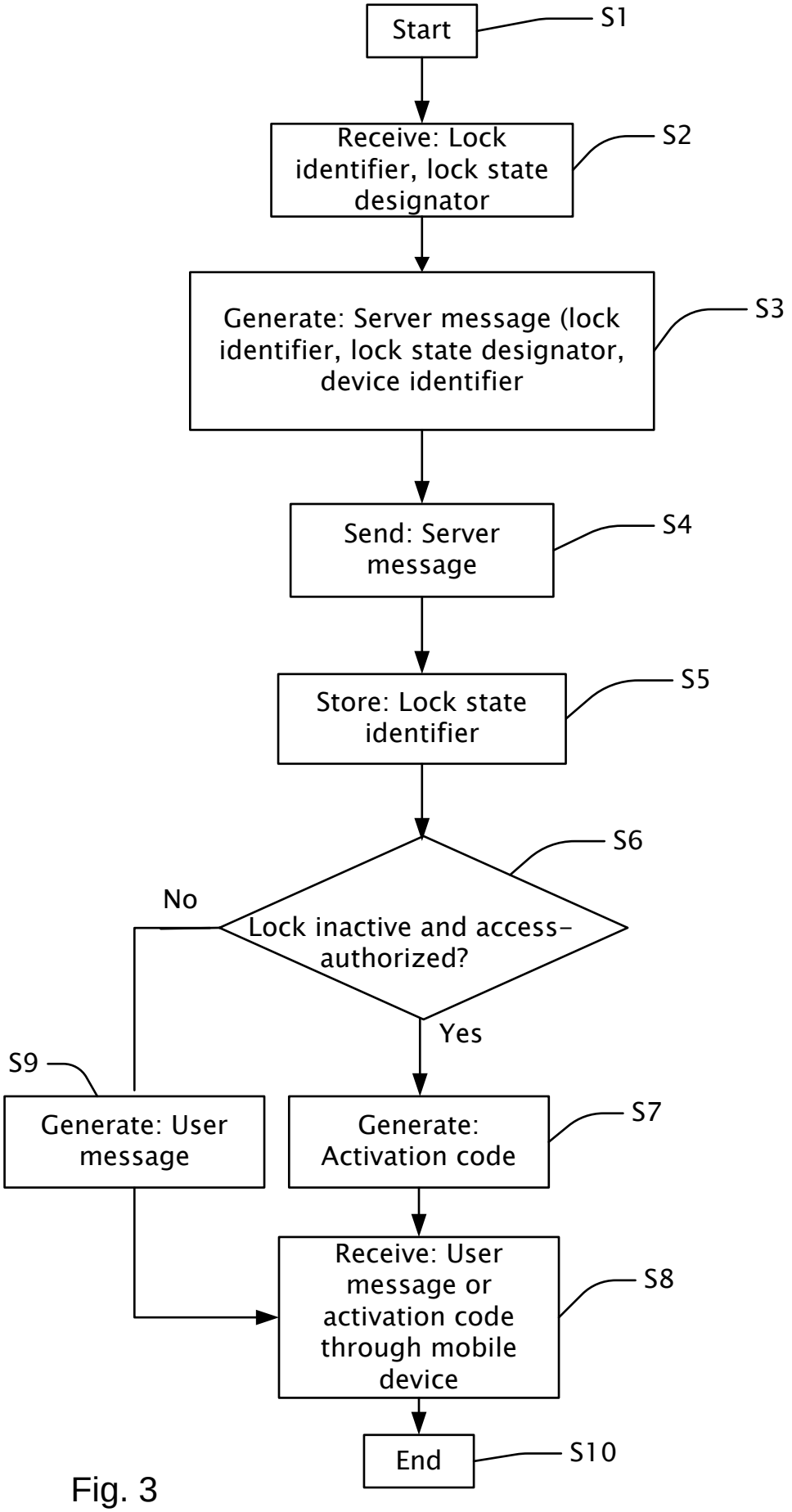
Start
S1
Receive: Lock identifier, lock state designator
S2
Generate: Server message (lock identifier, lock state designator, device identifier
S3
Send: Server message
S4
Store: Lock state identifier
S5
Lock inactive and access-authorized?
S6
No
Yes
Generate: User message
S9
Generate: Activation code
S7
Receive: User message or activation code through mobile device
S8
End
S10

Fig. 3