(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 620 919 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
05.01.2022 Bulletin 2022/01

(51) Int Cl.:
G07C 9/27 *(2020.01)*

(21) Application number: **12152711.3**

(22) Date of filing: **26.01.2012**

(54) **Locking system**

Schliesssystem

Système de verrouillage

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
31.07.2013 Bulletin 2013/31

(73) Proprietor: **SimonsVoss Technologies GmbH**
85774 Unterföhring (DE)

(72) Inventors:
- **Götz, Ivan**
  80997 Munich (DE)
- **Voss, Ludger**
  81676 Munich (DE)

(74) Representative: **Vossius & Partner**
Patentanwälte Rechtsanwälte mbB
Siebertstrasse 3
81675 München (DE)

(56) References cited:
WO-A1-2007/126375
WO-A2-2005/091182
WO-A2-2009/147548
US-A1- 2010 306 549
US-A1- 2011 035 604

- **Ray Walters: "NFC-enabled SIM cards to become a worldwide standard | ExtremeTech", , 18 November 2011 (2011-11-18), XP055686297, Retrieved from the Internet: URL:https://web.archive.org/web/20111118120340/https://www.extremetech.com/mobile/105683-nfc-enabled-sim-cards-to-become-a-worldwide-standard [retrieved on 2020-04-16]**
- **Claire Swedberg: "MicroSD Card Brings NFC to Phones for Credit Card Companies, Banks | RFID JOURNAL", RFID Journal, 25 November 2009 (2009-11-25), XP055686830, Retrieved from the Internet: URL:https://www.rfidjournal.com/microsd-card-brings-nfc-to-phones-for-credit-card-companies-banks [retrieved on 2020-04-17]**

EP 2 620 919 B1

Description

[0001] The present invention generally relates to an access control system and a method for using said system. In particular, the present invention relates to locking system and a corresponding method for controlling and customizing access of a mobile key to a lock. More particularly, the invention provides an easy, convenient and still safe system and method which allows an administrator to control and customize a mobile phone which comprises an NFC (Near Field Communication) device, as a mobile key for one a plurality of locks of a locking system. The method and system according to the present invention, however, is not limited on access control systems for locks but can be used for any kind of access control systems.

BACKGROUND OF THE INVENTION

[0002] Locking systems with a plurality of electronic locks and a plurality of electronic keys are known in the art. In particular, it is well known that transponders (active or passive) or RFID cards can be used as portable electronic keys (in the following also called credentials), which provide a plurality of advantages over pure mechanical locking systems with mechanical keys and mechanical locks. In these known electronic locking systems, the electronic keys and/or the electronic locks may be programmed individually, which allows to provide very flexible locking plans. For instance, each hotel guest or employee has its own electronic key, which can be individually programmed for unlocking a particular lock or a plurality of locks during a specific period of time.

[0003] In order to program the electronic key, e.g., the RFID card, locally coupling to a card reader/writer of an administrator is required. Furthermore, in order to provide a more flexible electronic locking system it is further preferred to interconnect the electronic locks of the locking system and/or to connect these electronic locks to a locking system management, e.g. a central computer with appropriate software which allows the administrator to program the electronic key(s) and/or the individual lock(s) individually. A drawback of such known locking systems is, however, that the electronic key has to be connected physically to the card reader of the administrator for programming or re-programming. Moreover, the electronic locks have to be connected to the locking system management to allow individual programming of the locks. Such an connection between the locking system management and the electronic locks typically requires complex wiring or sophisticated wireless networks.

[0004] Document US 2010/306549 A1 describes a system and a method for managing access to RFID locking units using mobile devices equipped with NFC modules. The mobile devices can function as keys to control the locking units by emulating RFID cards.

[0005] It is an object of the present invention to provide a locking system with a plurality of locks and a plurality of portable electronic keys, wherein at least some of the electronic keys are mobile phones. The present invention further relates to a corresponding method for administrating the locking system according to the present invention.

[0006] The object of the invention is achieved by the features of the independent claims. Further preferred embodiments of the invention are defined by the dependent claims.

SUMMARY OF THE INVENTION

[0007] A locking system according to the present invention comprises at least one electronic lock, preferably a plurality of electronic locks and at least one portable electronic key, preferably a plurality of electronic keys. The system further comprises a locking system management (also called Locking-System-Management; LSM in the following) which allows controlling and administrating access of individual or groups of electronic keys to individual or groups of electronic locks.

[0008] For instance a locking system according to the present invention a may be based on a digital locking and access control system (see e.g. System 3060 from SimonsVoss) which is an electronic version of a mechanical locking system which provides all the functions of a classical access control system. Electronic transponders (electronic keys) may be used instead of mechanical keys, along with electronic locks, such as digital locking cylinders. Radio communication between the electronic locks and the electronic keys takes the place of a key turning in a lock. Data is preferably transferred from the transponder to the locking cylinders or SmartRelays inductively at a frequency range of 25 kHz. The typical reading distance up to 40 cm for the locking cylinder and up to 120 cm for the SmartRelays may be provided. Using intelligent relays (SmartRelays), electronic switches can be activated depending on the transponder authorisation. For instance, the locking cylinders can be directly networked, e.g., on the basis of a 868 MHz frequency network. Furthermore, instead of using active transponder, MIFARE® Classic and MIFARE® DESFire RFID cards may be used as electronic keys. Using the Locking-System-Management (LSM) allows to define locking plans and allocate individual access rights. Access management and building automation are preferably managed by the Locking-System-Management-Software, which preferably works centrally from a single location. This basis system provides the advantage to organize one or even a plurality of locking systems and subsystems anywhere in the world.

[0009] The locking system according to the present invention is preferably a further advancement of the above discussed locking system. In particular, the present invention provides the further advantage that access management of electronic locks, which are not connected via a network to the LSM, can still be flexibly and individually managed by using mobile phones (also labeled cell

phones throughout the present application) as electronic keys, wherein said mobile phones are connectable to the LSM via the cellular network (mobile network; mobile communication network) of the mobile network operators (mobile phone providers). According to a further preferred embodiment, mobile phones with NFC (Near Field Communication) devices are used as mobile electronic keys.

[0010] In the following some essential technologies which are useful for the understanding of the present invention will be discussed in more detail.

[0011] Transponders, in particular passive transponders, are well known in the art to be used in electronic access control devices. For instance, RFID (Radio Frequency IDentification) is an automatic identification method relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is typically a small object that can be attached to or incorporated into a product. RFID tags contain silicon chips to enable them to receive and respond to queries from an RFID reader/writer. In an RFID system, the power supply to the transponder and the data exchange between the transponder and a reader is achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields. An RFID system is always made up of two components, the transponder/RFID tag and the reader.

[0012] NFC (Near Field Communication) is a short-range wireless connectivity technology standard designed for intuitive, simple, and safe communication between electronic devices (usually mobile phones communicating with RFID readers or RDID tags). NFC communication is enabled by bringing two NFC-compatible devices within a few centimeters of one another. This "context of proximity" is basis for many new NFC-based applications, e.g.: contactless transactions such as payment, transit ticketing, simple and fast data transfers including electronic business cards and access to online digital content or access control to locking systems. NFC is a standards-based technology that enables simple and safe two-way interactions between electronic devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single touch.

[0013] NFC is not an RFID system, but a wireless data interface between devices, similar to infrared or Bluetooth. In contrast to NFC, Bluetooth wireless technology was designed to replace cables between cell phones, laptops, and other computing and communication devices within a 10-meter range. NFC, however, provides several features with are of interest in relation to RFID systems. For instance, data transmission between two NFC interfaces uses high-frequency magnetic alternating fields in the frequency range of 13.56 MHz. NFC is compatible with existing RFID standards and makes it possible both to read transponders and to emulate transponders, i.e., to behave like transponders. Thus, an NFC interface has a 13.56 MHz transmitter and a 13.56 MHz receiver that are alternately connected to an antenna.

[0014] NFC devices are active devices and are unique in that they can change their mode of operation to be in (i) reader/writer mode, (ii) peer-to-peer mode, or (iii) card emulation mode. The different operating modes are based on the ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 contactless smart card standards.

[0015] On the other hand, an NFC tag is typically a passive device (for example, integrated in a smart poster) that stores data that can be read by an NFC-enabled device. In the following, the terms "NFC card" and "NFC tag" will be used synonymously. Typically, a "NFC card" and "NFC tag" are technically the same, however, contactless cards used in ticketing and payment often include additional technology to store secure data. In reader/writer mode, the NFC device is capable of reading NFC tag types, such as in the scenario of reading an NFC Smart Poster tag. In Peer-to-Peer (P2P) mode, two NFC devices can exchange data. For example, a user can share Bluetooth or WiFi link set up parameters or a user can exchange data such as virtual business cards or digital photos.

[0016] In card emulation mode, the NFC device appears to an external reader much the same as a traditional contactless smart card (RFID card). This enables contactless payments and ticketing by NFC devices without changing the existing infrastructure. This mode is secure and supported by a contactless communication API. In particular, in card emulation mode, a secure element on the device communicates and transacts with an external reader over RFID hardware. The internal security element interacts with an external reader. The application is notified when the external reader has been detected, and, if needed, the application communicates with the secure element, using the contactless communication API connection interface.

[0017] Preferred embodiments of the present invention may be characterized as follows.

[0018] According to a first aspect, the present invention relates to a locking system for managing access of an electronic key to an electronic lock according to claim 1. The system comprises at least one electronic lock which may be unlocked by means of a transponder, preferably by means of an active and/or passive transponder. According to a preferred embodiment, the electronic lock is adapted to be unlocked by an RFID card, e.g., a MIFARE® Classic and/or a MIFARE® DESFire RFID card. The invention is further characterized by providing at least one mobile phone with a NFC device. The NFC device may be integrated in the mobile phone or provided as an additional external device, e.g., as a NFC card or NFC sticker with is attached to the mobile phone. For instance the external NFC device may work as a Near Field Communication (NFC)/Radio Frequency Identification (RFID) Reader. The NFC device preferably comprises an embedded smart-chip.

[0019] The mobile phone is further adapted to install a mobile key application such that the mobile phone can

be used as electronic key for the electronic lock. Moreover, a locking system management (LSM) is provided for managing the access of the mobile phone (preferably also for managing additional active and/or passive transponder and/or RFID cards) to the electronic lock by means of individual key data sets. In particular, it is preferred that each electronic key comprises its own individual key data set. An OTA key server is further provided for storing and distrusting encrypted key data sets, wherein said locking system management (LSM) is adapted to encrypt the key data set in a secure environment of the LSM and to push said encrypted key data set to the OTA (over the air) key server. The secure environment of the LSM may be provided by firewalls which filter the data traffic to and from the LSM. According to the present invention, however, it is further preferred that the OTA server can not download key data sets and preferably also no other data from the LSM. In other words, it is preferred that the key data sets and preferably also any kind of data is actively pushed (sent) from the LSM to the OTA key server. Still in other words, to enhance security the LSM controls actively which data may be transmitted to the OTA key server.

[0020] The mobile phone is adapted to download, by means of the installed mobile key application, the appropriate/dedicated encrypted key data set from the OTA key server via the cellular mobile network and to decrypt the downloaded (encrypted) key data set and to store said decrypted key data set in a secure element of the NFC device. Instead of actively downloading the encrypted key data set from the OTA key server it may additionally or alternatively be possible to push the encrypted key data set from the OTA key server to the mobile phone.

[0021] The NFC device is further adapted to switch in a card emulation mode and to transmit the key data set during said card emulation mode to the electronic lock for unlocking. Thus, the NFC device behaves in the card emulation mode like an RFID card, e.g., a MIFARE® Classic and MIFARE® DESFire RFID card, such that there is no reconfiguration necessary for already installed locks. In other words, the electronic locks, which are adapted to be unlocked by a RFID card (MIFARE® Classic and MIFARE® DESFire RFID card), may be unlocked with the above described adapted mobile phone.

[0022] The encryption on the locking system management and the corresponding decryption on the mobile phone and/or NFC device is preferably achieved by an initial setup of the locking system management and the mobile phone. Preferably, the LSM and the mobile phone negotiate at least one secret key, e.g., a secret key for symmetric encryption and/or at least a pair of keys for asymmetric encryption. Such an initial negotiation is preferably done in a secure environment, e.g., by connecting the mobile phone and/or the NFC device to the LSM via cable or a local read/write device.

[0023] It is preferred that a universal mobile key application may be used for all mobile phones. However, it may be necessary to adapt this mobile key application to the operating system of the mobile phone. The individuality of the electronic key is preferably based on the individual key data set, not on the basis of the basis application. Accordingly, the mobile key application may be distributed via classical data storage medium or may be provided on a server which allows a user to download the application. Preferably, and most conveniently, the mobile key application is provided in an app store, wherein the mobile phone is preferably adapted to download the mobile key application from the app store.

[0024] The locking system management is preferably adapted to manage key data sets for active transponders and/or passive transponder and mobile phones. According to a preferred embodiment, a locking system management may be used for managing a plurality of electronic locks and electronic cylinders. Thus, an advantage of the present invention is based on a flexible locking system management, which can manage a plurality of different electronic keys. For instance, only a subset of electronic keys - which are managed in the locking system management - are defined as electronic keys on the basis of mobile phones. To keep the mobile phones up to date, it may be preferably to automatically updated key data sets on the OTA server whenever the administrator chooses to change access authorizations of any of these electronic keys (based on the mobile phone).

[0025] According to a second aspect, the present invention also relates to a corresponding method for managing access of an electronic key to an electronic lock according to claim 5.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] Various features of the embodiments of the present invention can be more fully appreciated, as the same become better understood with reference to the following detailed description of the embodiments when considered in connection with the accompanying figures, in which:

- Fig. 1 shows a traditional locking system with mechanical keys;
- Fig. 2 shows key distribution system in accordance to a locking system of the present invention; and
- Fig. 3 shows a locking system according to the present invention in more detail.

DETAILED DESCRIPTION OF EMBODIMENTS

[0027] Figure 1 shows a traditional locking system with centrally stored mechanical keys. For instance, a nursing service or a company providing field maintenance stores a plurality of mechanical keys for several locations 1002 in a central key depot 1101. An employee of the nursing service or field maintenance company is leaving his/her home office 1001. Before he/she can unlock the door(s) at the place of action 1002, the employee firstly travels to the central office 1100 (see path "A"), gets the me-

chanical key from the central key depot 1101 for the lock at location 1002 and travels to location 1002 (see path "B"). After finishing work the employee travels back to the central office 1100 (see path "B") for depositing the key at the central key depot 1101. Depositing the keys at the central key depot 1101 ensured that misusage of the key can be avoided or that other employees may use the key at another day. Afterwards the employee travels back to her home office 1001 (see path "A").

[0028] Figure 2 shows a locking system in accordance with the present invention. Instead of mechanical locks, at least one or a plurality of doors at location 102 are provided with electronic locks which may be unlocked with corresponding electronic keys. The electronic keys may be provided as active and/or passive transponders. Like mechanical keys, some electronic keys may be stored at a key depot 1101. Moreover, the electronic keys may be programmed individually at the central office by means of a central Locking-System-Management (LSM), which may be realized as software running on a computer. The administrator may program the individual electronic keys. For instance, an electronic key may be programmed to unlock a particular lock every Monday between 8 am and 6 pm. This provides the advantage that an employee may keep the electronic key, such that a detour via the central office may be avoided. However, for programming the electronic key, the employee has to go to the central office since programming is typically achieved by connecting the electronic key to a card reader directly connected to the LSM.

[0029] Moreover, in case such a programmed electronic key is lost, there is still a potential risk every Monday between 8 am and 6 pm that the lost key may be improperly used. In order to avoid such a misusage, the lock at the location 102 has to be reprogrammed. This may be achieved either by integrating the lock in a network, such that the lock may be programmed by the LSM. However, if the lock is not accessible via a network from the LSM, a portable device, e.g., a laptop or a handheld, may be used to program the lock locally at location 102.

[0030] According to the present invention, such a reprogramming of the lock may be avoided by allowing individual remote control of electronic keys. According to the present invention mobile phones (cellular phones), preferably mobile phones with NFC means may be used as electronic keys. By means of a key distribution service 200, a mobile phone 1 may be individually programmed for unlocking particular electronic locks for a limited time, thus making sure that employees will have to upload their changing access authorizations on a regular basis. For instance, by means of the key distribution service 200, a mobile phone may be programmed every Monday via the cellular network, to get access to specified locks at location 102. In case the employee should not get access to location 102, programming via the cellular mobile network is abandoned.

[0031] Figure 3 shows a preferred embodiment of the locking system according to the present invention in more detail.

[0032] Central part of the key distribution service 200 (see dotted line in Fig. 3) is the locking system management (LSM) 201. The locking system management preferably comprises at least one computer which allows individual management of all electronic keys, preferably including active transponder, passive transponder and/or mobile phones used as electronic keys according to the present invention. The locking system management preferably also allows that some or all of the locks which form part of the locking system may be programmed individually. For instance, some of the locks may be connected to the LSM via a network. Some of the locks may not be connected to the LSM via a network. Programming such locks, however, may be achieved by means of a portable computer (laptop, handheld, smartphone, etc.), e.g., by programming the locks locally using the portable computer.

[0033] The LSM 201 may provide an access table or access array which allows easy management of the individual locks and/or keys. Programming an RFID tag may be achieved by transferring a (individual) "key data set" from the LSM 201 to the RFID tag by means of an RFID reader/writer, wherein the *"key data set"* represents the access control data to an electronic lock, preferably to a plurality of electronic locks of the locking system, further preferred to all electronic locks of the locking system.

[0034] According to the present invention, mobile phones are preferably not re-programmed via a local reader/writer, but preferably via the cellular mobile network.

[0035] Firstly, preparing a mobile phone to operate as a mobile key in accordance with the present invention, a user downloads appropriate software on the mobile phone 1. Preferably, this particular software, which enables a mobile phone to work within the locking system according to the present invention, may be transferred locally from the LSM or an other computer authorized by the LSM. This software, also called "App", "app" (acronym for "Application") or "mobile key application" may be provided by an "app store".

[0036] The app store according to the present invention is a digital application distribution platform, particularly for mobile phones. In particular, the app store allows users to browse and download applications that were developed for the mobile phone. Preferably, the application (app) can be downloaded directly to a target device (the mobile phone), or downloaded onto a computer and afterwards transferred to the mobile phone. Accordingly, a user may download the mobile key application (app) from an app store as illustrated in step 01 of Fig. 3.

[0037] According to the present invention, it is preferred that the mobile phone as used as electronic key comprises an NFC device, e.g., an NFC chip. The NFC device further comprises a secure element. In particular, the secure element may be embedded within the mobile phone in a secure chip, in the SIM card and/or in an ex-

ternal device, attached to the mobile phone. The key data set, which represents or comprises data needed for unlocking a particular lock, is preferably stored within said secure element. Preferably, the key data set is generated individually for each mobile phone 1. Accordingly, it is preferred that each mobile phone stores a unique key data set in the secure element. Since the secure element of an NFC device is adapted to store sensible data securely, a save mobile key is provided.

[0038] According to the present invention, said key data set is preferably transferred from the Locking System Management 201 via an OTA (Over The Air) key server 202, to the mobile phone 1 as follows. Firstly, the key data set with the individual access codes is generated at the LSM 201. Since the LSM 201 may bee seen as the "heart" of the system, remote access to the LSM from outside should be avoided. According to the present invention, the key data set is encrypted (cryptographically secured) at the LSM by means of a secure key. The encrypted key data set is pushed from the LSM 201 to the OTA key server 202 (see step/arrow 02 in Fig. 3). Preferably, the LSM 201 and the OTA key server 201 are connected via TCP/IP, further preferred via the Internet. To enhance security, the key data set is pushed only in the direction from the LSM to the OTA. In other words, it is preferably not possible to download the key data set from the LSM. Still in other words, pushing the key data set represents a one way direction of sensible data which ensures that manipulation of the LSM from outside is impossible. The LSM 201 may be designed such that the administrator actively controls, e.g., by pressing a button, when a new key data set is pushed to the OTA key server. The LSM 201 may additionally or alternatively designed that any amendment of access control relating to a corresponding mobile phone may result in an automatic push of the corresponding amended key data set to the OTA key server. Further preferred, amended key data set(s) may be regularly or according to an underlying timing plan pushed to the OTA key server. It is, however, preferred that only encrypted key data sets are pushed and subsequently stored on the OTA key server. The OTA key server 201 is preferably provided as a trusted service manager (TSM). Such trusted service managers are typically very save. However, remote access to such OTA server can not be totally avoided such that attacker may hack in worst case the OTA key server and download the stored key data sets. However, since only encrypted key data sets are stored, even hacking the OTA server does not provide a safety problem for the locking system according to the present invention.

[0039] The user may then download the encrypted key data set from the OTA key server 201 by means of the mobile key application (the app) already installed on his/her mobile phone 1 (see step 03 in Fig. 3). In other words, the mobile phone network may be used for controlling/managing mobile phones as electronic keys. This provides further advantages over the traditional locking systems which typically suggest connecting the locks via a network for controlling/managing the locks of the locking system with the LSM. Accordingly, the system of the present invention provides further flexibility, especially for locks with are not (logically) connected to the LSM. For instance, a lock may be provided as "hermit lock" anywhere. Access to said lock may still be individually and flexibly managed due to the connection of the LSM to the mobile phone 1 via the cellular network.

[0040] The mobile key application on the mobile phone 1 is adapted to decrypt (decipher) the encrypted key data set on the mobile phone in a secure manner. Preferably, the LSM 201 and the mobile key application on the mobile phone 1 both know the preferably individual secure key for encrypting and/or decrypting the key data set. For instance, once the mobile key application has been installed at the mobile phone, the mobile phone may be physically coupled to the LSM to generate an encrypting and/or decrypting key which is only known by the LSM and the mobile key application on the mobile phone. The encryption/decryption on the LSM/mobile phone may be based on a symmetric key or on the basis of asymmetric keys. This design ensures that solely the mobile key application knowing the secure key may decrypt the encrypted key which is distributed via the OTA key server. After decrypting the key data set, the key data set is stored in the secure element of the NFC device. Thus, since the secure element of the NFC device is safe against manipulation from outside, security of the locking system according to the present invention is guaranteed.

[0041] A user may then use the NFC device with the stored key data set for unlocking the door 2 (see step/arrow 04 in Fig. 3). The NFC device switches into card emulation mode such that NFC device behaves like a typical RFID device. Preferably, the NFC device behaves like a well known MIFARE® card which transmits data for unlocking the electronic lock 2 on the basis of the key data set stored in the secure element on the mobile phone 1. This provides the advantage that legacy installed locks, which are unlocked by means of MIFARE cards, may be unlocked by traditional RFIC cards or by means of mobile phones 1 which are customized according to the present invention.

Claims

1. A locking system for managing access of an electronic key to an electronic lock, the system comprising:

   at least one electronic lock (2) which may be unlocked by means of an RFID card;
   at least one mobile phone (1) and an NFC device, wherein said mobile phone (1) is adapted to install a mobile key application such that the mobile phone can be used as electronic key for the electronic lock (2), wherein said mobile key application is provided at an appstore, wherein

the mobile phone is adapted to download the mobile key application from the appstore;
a locking system management (201) for managing the access of the mobile phone (1) to the electronic lock (2) by means of a key data set;
an OTA key server (202) for storing the encrypted key data sets, wherein said locking system management (201) is adapted to encrypt the key data set and to push said encrypted key data set to the OTA key server (202);
wherein said mobile phone (1) is adapted to download by means of the installed mobile key application the appropriate encrypted key data set from the OTA key server (202) via the cellular mobile network and to decrypt the downloaded key data set and to store said decrypted key data set in a secure element of the NFC device, wherein said NFC device is further adapted to switch into card emulation mode and to transmit the key data set during said card emulation mode to the electronic lock for unlocking.

2. The system according to claim 1, wherein the NFC device is

integrated in the mobile phone (1), preferably i) directly embedded, ii) in a SIM card or iii) in a micro memory card within the mobile phone (1); or
attached as an external device to the mobile phone (1), wherein said mobile phone is connected via a wired connection or via Bluetooth to said NFC device.

3. The system according to claim 1 or 2, wherein the key data set is exclusively transmitted via a push communication from the locking system management to the OTA key server (202).

4. The system according to any of the preceding claims, wherein the locking system management (201) and the mobile phone (1) with the installed mobile key application are adapted to be initialized by negotiating a secret key for symmetric encryption and/or a pair of keys for asymmetric encryption, which is used at the locking system management (201) for encrypting the key data set and used by the mobile key application to decrypt the downloaded key data set.

5. A method for managing access of an electronic key to an electronic lock, preferably on the locking system as claimed in the preceding claims, the method comprising the steps:

providing at least one electronic lock (2) which may be unlocked by means of a RFID card;
providing at least one mobile phone (1) and an NFC device, downloading and installing a mobile key application from an appstore on said mobile phone (1) such that the mobile phone can be used as electronic key for the electronic lock (2);
providing a locking system management (201) for managing the access of the mobile phone (1) to the electronic lock (2) by means of a key data set;
encrypting the key data set on said locking system management (201) and pushing said encrypted key data set to an OTA key server (201);
storing the encrypted key data sets at the OTA key server (201),
downloading by means of the installed mobile key application the appropriate encrypted key data set from the OTA key server (201) via the cellular mobile network, decrypting the downloaded key data set and storing said decrypted key data set in a secure element of the NFC device, and
switching said NFC device into card emulation mode and transmitting the encrypted key data set during said card emulation mode to the electronic lock for unlocking.

6. The method according to claim 5, wherein the NFC device is provided

a) integrated in the mobile phone (1), preferably i) directly embedded, ii) in a SIM card or iii) in a micro memory card within the mobile phone (1); or
b) attached as an external device to the mobile phone (1), wherein said mobile phone is connected via a wired connection or with Bluetooth to said NFC device.

7. The method according to claim 5 or 6, wherein the key data set is exclusively transmitted via a push communication from the locking system management to the OTA key server (202).

8. The method according to any of the preceding method claims, wherein the locking system management (201) and the mobile phone (1) with the installed mobile key application are initialized by negotiating a secret key for symmetric encryption and/or a pair of keys for asymmetric encryption, which is used at the locking system management (201) for encrypting the key data set and used by the mobile key application to decrypt the downloaded key data set.

Patentansprüche

1. Schließsystem zum Verwalten des Zugangs eines elektronischen Schlüssels zu einem elektronischen Schloss, wobei das System aufweist:

mindestens ein elektronisches Schloss (2), das mit Hilfe einer RFID-Karte aufgeschlossen werden kann;
mindestens ein Mobiltelefon (1) und ein NFC-Device, wobei das Mobiltelefon (1) geeignet ist, eine Mobilschlüssel-Applikation zu installieren, so dass das Mobiltelefon als elektronischer Schlüssel für das elektronische Schloss (2) verwendet werden kann, wobei die Mobilschlüssel-Applikation in einem App Store bereitgestellt wird, wobei das Mobiltelefon geeignet ist, die Mobilschlüssel-Applikation aus dem App Store herunterzuladen;
eine Schließsystem-Verwaltung (201) zum Verwalten des Zugangs des Mobiltelefons (1) zum elektronischen Schloss (2) mit Hilfe eines Schlüsseldatensatzes;
einen OTA Key Server (202) zum Speichern der verschlüsselten Schlüsseldatensätze, wobei die Schließsystem-Verwaltung (201) geeignet ist, den Schlüsseldatensatz zu verschlüsseln und den verschlüsselten Schlüsseldatensatz zum OTA Key Server (202) im Push-Betrieb zu übermitteln;
wobei das Mobiltelefon (1) geeignet ist, mit Hilfe der installierten Mobilschlüssel-Applikation den geeigneten verschlüsselten Schlüsseldatensatz vom OTA Key Server (202) über das Mobilfunknetz herunterzuladen sowie den heruntergeladenen Schlüsseldatensatz zu entschlüsseln und den entschlüsselten Schlüsseldatensatz in einem sicheren Element des NFC-Devices zu speichern,
wobei das NFC-Device ferner geeignet ist, in einen Karten-Emulationsmodus umzuschalten und den Schlüsseldatensatz während des Karten-Emulationsmodus zum elektronischen Schloss zum Aufschließen zu senden.

2. System nach Anspruch 1, wobei das NFC-Device in das Mobiltelefon (1) integriert ist, vorzugsweise i) direkt eingebettet, ii) auf einer SIM-Karte oder iii) auf einer Mikrospeicherkarte im Mobiltelefon (1); oder
als externes Device am Mobiltelefon (1) angebracht ist, wobei das Mobiltelefon über eine Drahtverbindung oder über Bluetooth mit dem NFC-Device verbunden ist.

3. System nach Anspruch 1 oder 2, wobei der Schlüsseldatensatz ausschließlich über eine Push-Kommunikation von der Schließsystem-Verwaltung zum OTA Key Server (202) gesendet wird.

4. System nach einem der vorstehenden Ansprüche, wobei die Schließsystem-Verwaltung (201) und das Mobiltelefon (1) mit der installierten Mobilschlüssel-Applikation geeignet sind, durch Aushandeln eines Geheimschlüssels zur symmetrischen Verschlüsselung und/oder eines Schlüsselpaars zur asymmetrischen Verschlüsselung initialisiert zu werden, der in der Schließsystem-Verwaltung (201) zum Verschlüsseln des Schlüsseldatensatzes verwendet wird und durch die Mobilschlüssel-Applikation verwendet wird, um den heruntergeladenen Schlüsseldatensatz zu entschlüsseln.

5. Verfahren zum Verwalten des Zugangs eines elektronischen Schlüssels zu einem elektronischen Schloss, vorzugsweise im Schließsystem nach einem der vorstehenden Ansprüche, wobei das Verfahren die Schritte aufweist:

Bereitstellen mindestens eines elektronischen Schlosses (2), das mit Hilfe einer RFID-Karte aufgeschlossen werden kann;
Bereitstellen mindestens eines Mobiltelefons (1) und eines NFC-Devices,
Herunterladen und Installieren einer Mobilschlüssel-Applikation aus einem App Store auf dem Mobiltelefon (1), so dass das Mobiltelefon als elektronischer Schlüssel für das elektronische Schloss (2) verwendet werden kann;
Bereitstellen einer Schließsystem-Verwaltung (201) zum Verwalten des Zugangs des Mobiltelefons (1) zum elektronischen Schloss (2) mit Hilfe eines Schlüsseldatensatzes;
Verschlüsseln des Schlüsseldatensatzes in der Schließsystem-Verwaltung (201) und im Push-Betrieb erfolgendes Übermitteln des verschlüsselten Schlüsseldatensatzes zu einem OTA Key Server (201);
Speichern der verschlüsselten Schlüsseldatensätze auf dem OTA Key Server (201),
mit Hilfe der installierten Mobilschlüssel-Applikation erfolgendes Herunterladen des geeigneten verschlüsselten Schlüsseldatensatzes vom OTA Key Server (201) über das Mobilfunknetz,
Entschlüsseln des heruntergeladenen Schlüsseldatensatzes und Speichern des entschlüsselten Schlüsseldatensatzes in einem sicheren Element des NFC-Devices und
Umschalten des NFC-Devices in einen Karten-Emulationsmodus und Senden des verschlüsselten Schlüsseldatensatzes während des Karten-Emulationsmodus zum elektronischen Schloss zum Aufschließen.

6. Verfahren nach Anspruch 5, wobei das NFC-Device so vorgesehen ist, dass es

a) in das Mobiltelefon (1) integriert ist, vorzugsweise i) direkt eingebettet, ii) auf einer SIM-Karte oder iii) auf einer Mikrospeicherkarte im Mobiltelefon (1); oder
b) als externes Device am Mobiltelefon (1) angebracht ist, wobei das Mobiltelefon über eine

Drahtverbindung oder mit Bluetooth mit dem NFC-Device verbunden ist.

7. Verfahren nach Anspruch 5 oder 6, wobei der Schlüsseldatensatz ausschließlich über eine Push-Kommunikation von der Schließsystem-Verwaltung zum OTA Key Server (202) gesendet wird.

8. Verfahren nach einem der vorstehenden Verfahrensansprüche, wobei die Schließsystem-Verwaltung (201) und das Mobiltelefon (1) mit der installierten Mobilschlüssel-Applikation durch Aushandeln eines Geheimschlüssels zur symmetrischen Verschlüsselung und/oder eines Schlüsselpaars zur asymmetrischen Verschlüsselung initialisiert werden, der in der Schließsystem-Verwaltung (201) zum Verschlüsseln des Schlüsseldatensatzes verwendet wird und durch die Mobilschlüssel-Applikation verwendet wird, um den heruntergeladenen Schlüsseldatensatz zu entschlüsseln.

Revendications

1. Système de verrouillage pour gérer l'accès d'une clé électronique à un verrou électronique, le système comprenant :

au moins un verrou électronique (2) qui peut être déverrouillé à l'aide d'une carte RFID ;
au moins un téléphone mobile (1) et un dispositif CCP, dans lequel ledit téléphone mobile (1) est adapté pour installer une application clé mobile de sorte que le téléphone mobile peut être utilisé en tant que clé électronique pour le verrou électronique (2), dans lequel l'application clé mobile est prévue au niveau d'un magasin d'applications, dans lequel le téléphone mobile est adapté pour télécharger l'application clé mobile depuis le magasin d'applications ;
une gestion de système de verrouillage (201) pour gérer l'accès du téléphone mobile (1) au verrou électronique (2) au moyen d'un ensemble de données clés ;
un serveur clé OTA (202) pour stocker les ensembles de données clés cryptées, dans lequel ladite gestion de système de verrouillage (201) est adaptée pour crypter l'ensemble de données clés et pour pousser ledit ensemble de données cryptées vers le serveur clé OTA (202) ;
dans lequel ledit téléphone mobile (1) est adapté pour télécharger au moyen de l'application clé mobile installée l'ensemble de données clés cryptées approprié depuis le serveur clé OTA (202) via le réseau mobile cellulaire et pour décrypter l'ensemble de données clés téléchargé et pour stocker ledit ensemble de données clés décryptées dans un élément sécurisé du dispositif CCP,
dans lequel ledit dispositif CCP est en outre adapté pour commuter en mode émulation de carte et pour transmettre l'ensemble de données clés pendant ledit mode émulation de carte au verrou électronique pour déverrouillage.

2. Système selon la revendication 1, dans lequel le dispositif CCP est

intégré dans le téléphone mobile (1), de préférence i) directement incorporé, ii) dans une carte SIM ou iii) dans une carte mémoire micro à l'intérieur du téléphone mobile (1) ; ou
fixé en tant que dispositif externe au téléphone mobile (1), dans lequel ledit téléphone mobile est connecté via une connexion filaire ou par Bluetooth audit dispositif CCP.

3. Système selon la revendication 1 ou 2, dans lequel l'ensemble de données clés est exclusivement transmis via une communication de pousser de la gestion de système de verrouillage vers le serveur clé OTA (202).

4. Système selon l'une quelconque des revendications précédentes, dans lequel la gestion de système de verrouillage (201) et le téléphone mobile (1) pourvu de l'application clé mobile installée sont adaptés pour être initialisés en négociant une clé secrète pour un cryptage symétrique et/ou une paire de clés pour un cryptage asymétrique, laquelle est utilisée au niveau de la gestion de système de verrouillage (201) pour un cryptage de l'ensemble de données clés et utilisée par l'application clé mobile pour décrypter l'ensemble de données clés téléchargé.

5. Procédé de gestion d'accès d'une clé électronique à un verrou électronique, de préférence sur le système de verrouillage selon les revendications précédentes, le procédé comprenant les étapes suivantes :

fourniture d'au moins un verrou électronique (2) qui peut être déverrouillé au moyen d'une carte RFID ;
fourniture d'au moins un téléphone mobile (1) et d'un dispositif CCP, téléchargement et installation d'une application clé mobile depuis un magasin d'applications sur ledit téléphone mobile (1) de sorte que le téléphone mobile peut être utilisé en tant que clé électronique pour le verrou électronique (2) ;
fourniture d'une gestion de système de verrouillage (201) pour gérer l'accès du téléphone mobile (1) au verrou électronique (2) au moyen d'un ensemble de données clés ;
cryptage de l'ensemble de données clés sur la-

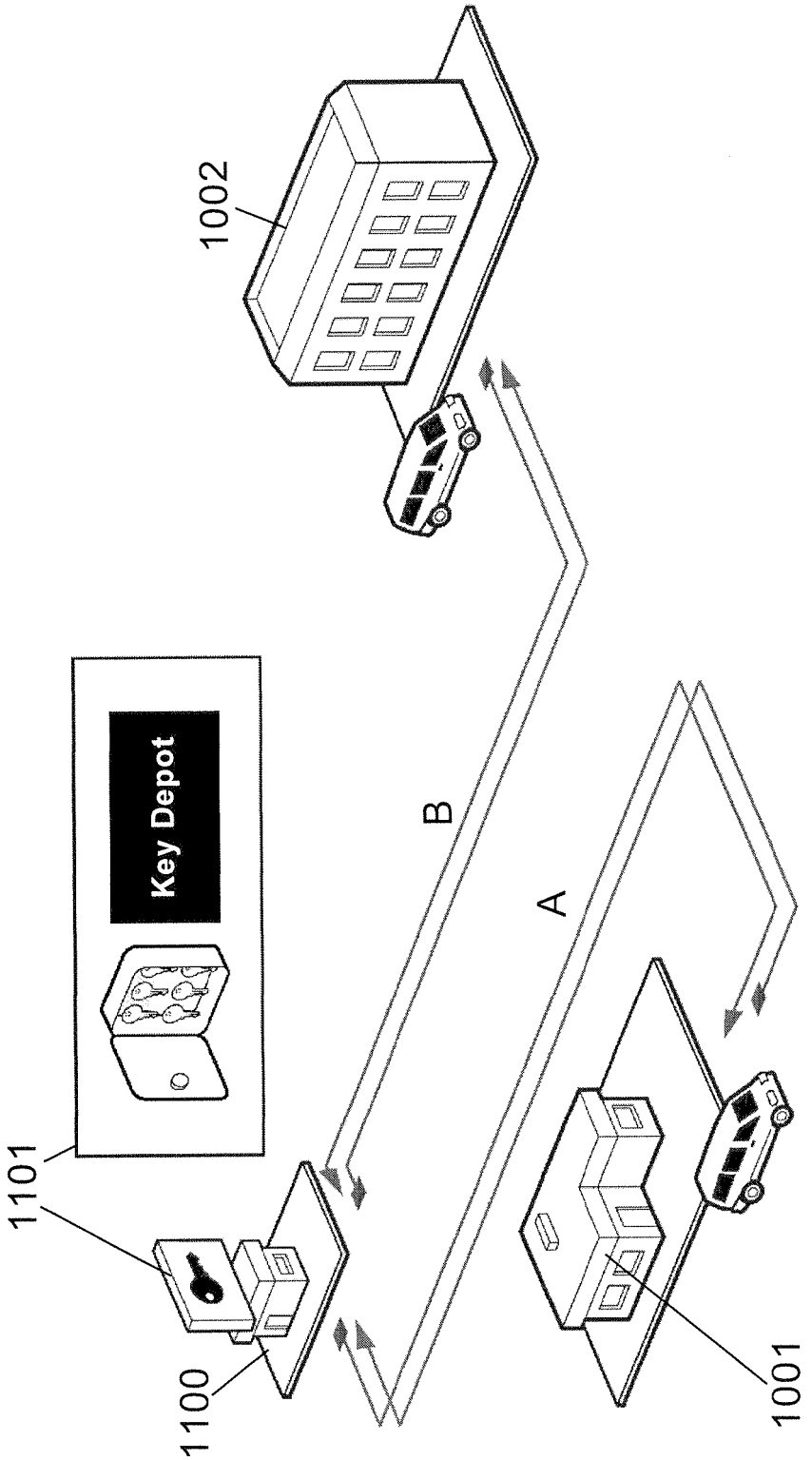
dite gestion de système de verrouillage (201) et pousser dudit ensemble de données clés cryptées vers un serveur clé OTA (201) ;
stockage des ensembles de données clés cryptées au niveau du serveur clé OTA (201),
téléchargement au moyen de l'application clé mobile installée de l'ensemble de données clés cryptées approprié depuis le serveur clé OTA (201) via le réseau mobile cellulaire, décryptage de l'ensemble de données clés téléchargé et stockage dudit ensemble de données clés décryptées dans un élément sécurisé du dispositif CCP, et
commutation dudit dispositif CCP en mode émulation de carte et transmission de l'ensemble de données clés cryptées pendant ledit mode émulation de carte au verrou électronique pour déverrouillage.

6. Procédé selon la revendication 5, dans lequel le dispositif CCP est prévu

a) de manière intégrée dans le téléphone mobile (1), de préférence i) directement incorporé, ii) dans une carte SIM ou iii) dans une carte mémoire micro à l'intérieur du téléphone mobile (1) ; ou
b) fixé en tant que dispositif externe au téléphone mobile (1), dans lequel ledit téléphone mobile est connecté via une connexion filaire ou par Bluetooth audit dispositif CCP.

7. Procédé selon la revendication 5 ou 6, dans lequel l'ensemble de données clés est transmis exclusivement via une communication de pousser de la gestion de système de verrouillage vers le serveur clé OTA (202).

8. Procédé selon l'une quelconque des revendications précédentes du procédé, dans lequel la gestion de système de verrouillage (201) et le téléphone mobile (1) pourvu de l'application clé mobile installée sont initialisés en négociant une clé secrète pour un cryptage symétrique et/ou une paire de clés pour un cryptage asymétrique, laquelle est utilisée au niveau de la gestion de système de verrouillage (201) pour un cryptage de l'ensemble de donnés clés et utilisée par l'application clé mobile pour décrypter l'ensemble de données clés téléchargé.



PRIOR ART

Fig. 1

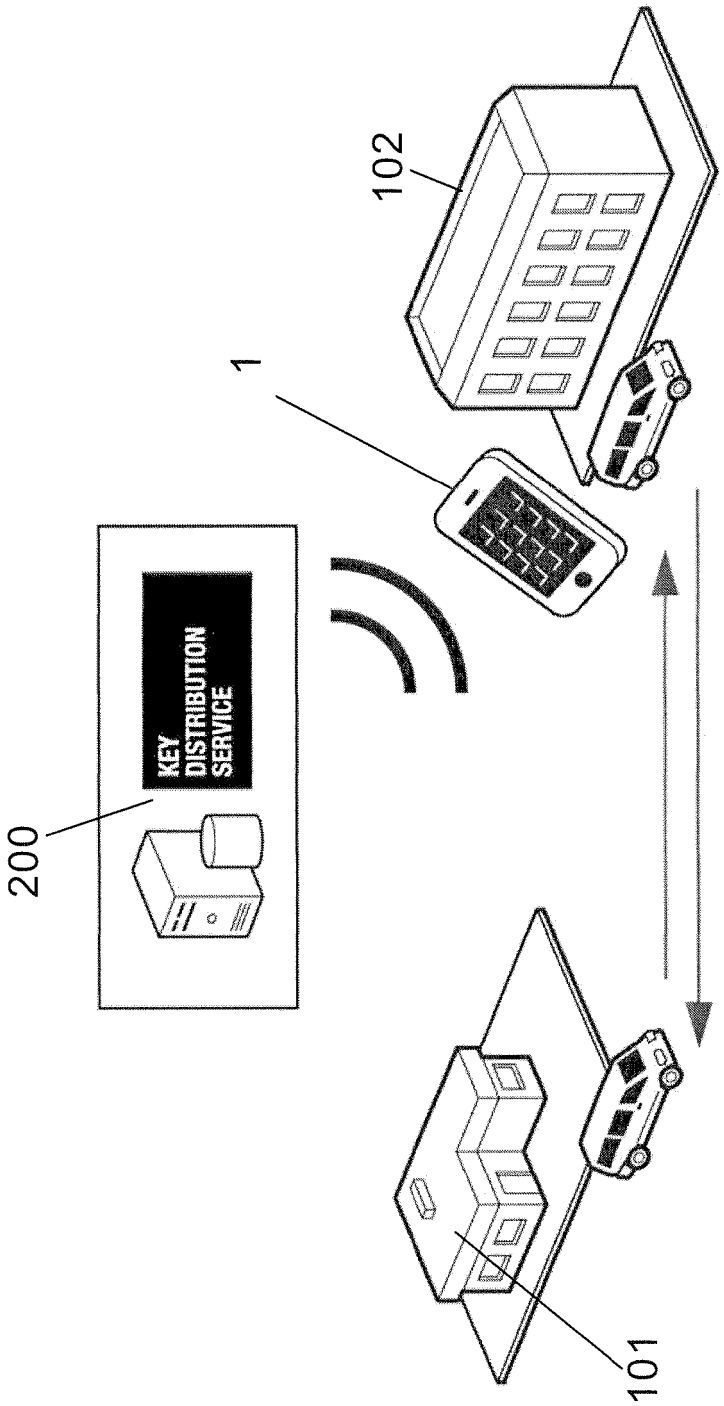


Fig. 2

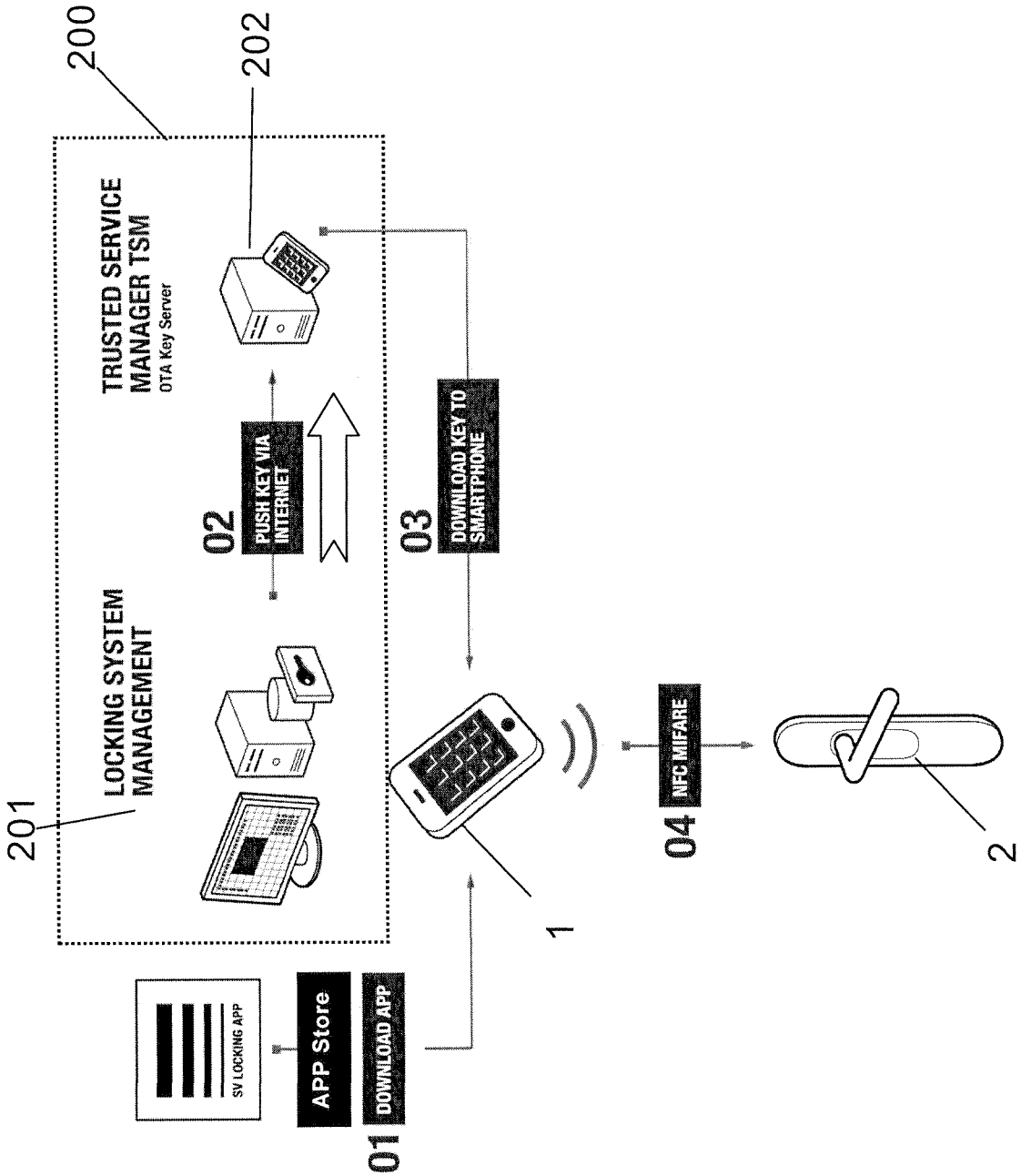

200
202
TRUSTED SERVICE MANAGER TSM
OTA Key Server
LOCKING SYSTEM MANAGEMENT
201
02
PUSH KEY VIA INTERNET
03
DOWNLOAD KEY TO SMARTPHONE
SV LOCKING APP
APP Store
01
DOWNLOAD APP
1
04
NFC MIFARE
2

Fig. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2010306549 A1 **[0004]**