

(19)



(11)

EP 2 800 067 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:

04.05.2022 Bulletin 2022/18

(51) International Patent Classification (IPC):

G07C 9/00 (2020.01)

(21) Application number: **14164004.5**

(52) Cooperative Patent Classification (CPC):

G07C 9/00817; G07C 9/00309; G07C 9/00571

(22) Date of filing: **09.04.2014**

(54) READER DEVICE AND ASSOCIATED METHOD

LESEVORRICHTUNG UND ZUGEHÖRIGES VERFAHREN

DISPOSITIF DE LECTURE ET PROCÉDÉ ASSOCIÉ

(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**

(30) Priority: **03.05.2013 SE 1350544**

(43) Date of publication of application:

05.11.2014 Bulletin 2014/45

(73) Proprietor: **ASSA ABLOY Opening Solutions
Sweden AB**

631 05 Eskilstuna (SE)

(72) Inventors:

- **Berglund, Jens
635 20 Eskilstuna (SE)**

- **Munhoz, Perla
643 31 Torshälla (SE)**

- **Sevallius, Patrik
136 73 Vendelsö (SE)**

- **Blomqvist, Fredrik
162 65 Vällingby (SE)**

- **Johansson Kjerstad, Ove
196 34 Kungsängen (SE)**

(74) Representative: **Kransell & Wennborg KB**

**P.O. Box 27834
115 93 Stockholm (SE)**

(56) References cited:

**EP-A1- 2 584 539 US-A1- 2003 028 814
US-A1- 2006 224 901 US-A1- 2012 096 131**

EP 2 800 067 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description**TECHNICAL FIELD**

[0001] The invention relates to a reader device arranged to determine access rights of an electronic access key.

BACKGROUND

[0002] It is known to use near field wireless access keys to allow or deny access to physical locks, controlling whether it is possible to open a door or not. In such systems, reader devices are used on the lock side to read access information stored on the near field wireless access keys.

[0003] There are many different protocols used for reading the access information. Hence, reader devices need to be appropriate for the correct protocol or protocols to be used in a particular installation.

[0004] It would be greatly beneficial if there were a way to simplify the installation of reader devices.

[0005] US 2003/028814 A1 discloses a smart card access control system. US 2006/224901 A1 discloses a system and method for remotely assigning and revoking access credentials using a near field communication equipped mobile phone. US 2012/096131 A1 discloses systems and methods for interacting with access control devices. EP 2 584 539 A1 discloses a method for configuring an electromechanical lock. US 5,537,103 discloses a programmer for contact readable electronic control system and programming method therefor.

SUMMARY

[0006] It is an object to simplify installation of reader devices.

[0007] According to a first aspect, it is presented a reader device according to appended claim 1.

[0008] By using the electronic configuration key, the configuration of the reader device is effected using only local communication. This is a more secure way to configure the reader device compared to e.g. remote configuration from a central administration node. After installation, the electronic configuration key could e.g. be locked away in a safe location such as a safe. Moreover, this reader device could be provided with a great amount of electronic access key protocols enabled from the start, and the reader device is then configured by inactivating protocols which are not to be used, using the electronic configuration key. In this way, an installation operator could e.g. have a stock of generic, unconfigured, multi-protocol reader devices in stock. This reduces or even eliminates the need to keep installation specific reader devices. These generic reader devices are then easily configured for a particular installation by simply using an electronic configuration key, without any need of the reader device being connected to any external devices;

it is sufficient that the reader device is only connected to power.

[0009] By only being responsive to configuration data during a configuration period the risk is reduced of random people being able to reconfigure the lock, e.g. to circumvent access control of the reader device.

[0010] The configuration data may comprise a communication control command section and a communication control parameter section. In this way, a configuration specific to a particular installation site can be achieved.

[0011] The controller may be further arranged to apply an installation specific configuration for at least one electronic access key protocol, based on the configuration data. Installation specific is here to be interpreted as specific to a specific installation, such as a site or a company. In this way, security can be improved and/or customised compared to the generic configuration of the reader device.

[0012] The near field radio frequency communication device is further arranged to read reset data from an electronic reset key; and the controller arranged to reset the reader device based on the reset data, to thereby enable all of the supported plurality of electronic access key protocols in the reader device. By resetting the radio device, the reader device can again be set in a generic mode, allowing a new configuration to be applied. This can e.g. be useful in the case of a changed configuration of an existing installation (such as due to an upgrade to a more secure protocol) or for reuse of the reader device in another installation.

[0013] The near field radio frequency communication device may be operable around a centre frequency of 13.56 MHz.

[0014] According to a second aspect, it is presented a method according to appended claim 5.

[0015] It is to be noted that the term "electronic access key protocol", whenever used in the claims or description of this document, is to be interpreted as a way in which a reader device reads data from an electronic access key.

[0016] Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The invention is now described, by way of example, with reference to the accompanying drawings, in which:

Fig 1 is a schematic diagram illustrating an environ-

ment where embodiments presented herein can be applied;

Fig 2 is a schematic diagram illustrating a reader device of Fig 1 and its communication with various electronic keys according to one embodiment;

Fig 3 is a schematic diagram illustrating an electronic configuration key of Fig 2 according to one embodiment;

Fig 4 is a schematic diagram illustrating an unclaimed embodiment of an electronic reset key of Fig 2;

Fig 5 is a schematic diagram illustrating an electronic configuration key of Fig 2 according to one embodiment;

Fig 6 is a schematic graph illustrating operation of the reader device of Figs 1 and 2 according to one embodiment;

Fig 7 is a schematic diagram illustrating a user interface device of the reader device of Fig 2 according to one embodiment;

Fig 8 is a schematic side view of the user interface device of Fig 7 according to one embodiment; and

Fig 9 is a flow chart illustrating one embodiment of a method performed in the reader device of Fig 1 and 2.

DETAILED DESCRIPTION

[0018] The invention will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete. Like numbers refer to like elements throughout the description.

[0019] Fig 1 is a schematic diagram illustrating a system where embodiments presented herein can be applied. An electronically controlled physical lock 8 is controlled by a local control unit 7. Optionally, the electronically controlled physical lock 8 can also be controlled by a conventional mechanical key.

[0020] A reader device 1 communicates with an electronic access key 10, in possession of a user, using near field radio frequency communication. A user interface device 9 allows the user to input data into and read data from the system.

[0021] The electronically controlled physical lock 8 is controllable by the local control unit 7 to be in a locked or unlocked state, depending on the electronic access key 10. In this way, access to a physical space can be controlled. For example a door can be controlled to be able to be opened when the electronically controlled physical lock 8 is in an unlocked state and not to be able to be opened when the electronically controlled physical lock 8 is in a locked state. Optionally, the local control unit 7 is configured to use additional security measures

to gain access, e.g. by requiring a code to be entered using the user interface device 9 or using biometrics.

[0022] A central control unit 5 enables administration of the system and can configure one or more local control units 7. In one embodiment, the central control unit allows the reader device 1 to receive software upgrades remotely. As explained in more detail below, the reader device 1 can subsequently be configured to make use of the software upgrade, e.g. to use a new electronic access key protocol, using an electronic configuration key readable by the reader device 1.

[0023] Each local control unit 7 can e.g. be a computer with a central processing unit, memory, input/output unit(s), etc. The communication between the local control unit 7, user interface device 9, reader device 1 and the electronically controlled physical lock 8 can occur using any suitable electronic access key protocol, e.g. using a controller area network (CAN) bus, Ethernet, universal serial bus (USB), serial connections (e.g. RS-232, RS-422, etc.) and/or parallel connections (e.g. Centronics).

[0024] The communication between the local control unit 7 and the central control unit 5 can e.g. occur using a wide area protocol such as Internet Protocol (IP), whereby the local control unit 7 and the central control unit can be situated in remote locations far from each other and can e.g. communicate via the Internet (e.g. using an encrypted connection).

[0025] The central control unit 5 can e.g. be a general purpose computer with display, keyboard, etc., with appropriate software installed, allowing an operator to configure one or more connected local control unit, e.g. belonging to one company or installation.

[0026] The local control unit 7, user interface device 9, reader device 1, and electronically controllable physical lock 8 can be e.g. powered by a connection to a mains AC (alternating current) source, optionally via a chargeable backup power storage device such as a rechargeable battery.

[0027] Optionally, one or more of the local control unit 7, user interface device 9, reader device 1, and electronically controllable physical lock 8 can be combined in a single physical device.

[0028] Fig 2 is a schematic diagram illustrating a reader device 1 of Fig 1 and its communication with various electronic keys 10-12 according to one embodiment. The reader device 1 comprises a controller 4 using any combination of one or more of a suitable central processing unit (CPU), multiprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit (ASIC), field programmable gate array (FPGA) etc., capable of execution inherent to the controller 4 and/or according to software instructions stored in a computer program product 6. The computer program product 6 is memory being any combination of read and write memory (RAM) and read only memory (ROM). The memory comprises persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted

memory.

[0029] The controller 4 can be configured to execute the method described with reference to Fig 9 below.

[0030] The reader device 1 also comprises a near field radio frequency communication device 3 arranged to communicate with one or more of electronic keys 10-12 using near field communication. Near field is here to interpreted as a distance between the reader and the electronic key where electric and magnetic components produced directly by currents and charge-separations dominate. The reader device 1 supports a plurality of electronic access key protocols. However, as explained in more detail below, one or more electronic access key protocols can be inactivated using an electronic configuration key 11. The near field radio frequency communication device 3 comprises appropriate transmitter and receiver circuitry to read data from a nearby electronic key 10-12. For example, the near field radio frequency communication device 3 can comprise circuitry to send a signal to the electronic key 10-12 which energises the electronic key such that data stored on the electronic key is sent to and received by the near field radio frequency communication device 3.

[0031] Using the near field radio frequency communication device 3, the reader device 1 can communicate with an electronic access key 10, an electronic configuration key 11 and/or an electronic reset key. As explained above, the electronic access key 10 is read by the reader device 1, and evaluated by the local control unit 7 to allow or deny access. The local control unit 7 is thus arranged to determine, based on access data read from the electronic access key 10, whether the electronic access key 10 is eligible to open the electronically controlled physical lock 8.

[0032] Furthermore, the near field radio frequency communication device 3 is arranged to read configuration data from an electronic configuration key 11. The controller 4 is arranged to inactivate electronic access key protocol in the reader device based on the configuration data 20. Moreover, installation specific configuration can be applied. This is explained in more detail with reference to Fig 6 below.

[0033] The near field radio frequency communication device 3 is further arranged to read reset data from an electronic reset key 12. Based on the reset data, the controller 4 is arranged to conditionally reset the reader device, to thereby enable all of the supported plurality of electronic access key protocols in the reader device. Also, the reset can optionally remove any installation specific configuration to thereby reset the reader device to a generic state. For example, the reader device 1 can support any combination of the following protocols using 13.56 MHz centre frequency (in effect 13.553 MHz to 13.567 MHz): MIFARE Classic, MIFARE Ultralight, MIFARE Ultralight EVi, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1, MIFARE Plus, MIFARE samav2, and Near Field Communication (NFC).

[0034] Fig 3 is a schematic diagram illustrating an elec-

tronic configuration key 11 of Fig 2 according to one embodiment. The electronic configuration key 11 comprises a memory 15 holding configuration data 20 which, when read by a reader device in a configuration period, makes the reader device 1 inactivate one or more electronic access key protocols. Moreover, the configuration data 20 can control how the electronic access key protocol is to function, e.g. which sectors to read on the electronic access key, etc. Optionally, the configuration data 20 comprises a communication control command section 21 and a communication control parameter section 22. The electronic configuration key 11 can use any protocol supported by the reader device 1. The electronic configuration key 11 supports one of the electronic access key protocol used by the reader device.

[0035] Fig 4 is a schematic diagram illustrating an unclaimed embodiment of an electronic reset key 12 of Fig 2. The electronic reset key 12 comprises a memory 15' holding reset data 25 which, when read by a reader device in a configuration period, makes the reader device 1 inactivate one or more electronic access key protocols. Since the electronic reset key 12 is used to reset the reader device, it supports an electronic access key protocol which an, already configured reader device, is configured to support.

[0036] Fig 5 is a schematic diagram illustrating an electronic access key 10 of Fig 2 according to one embodiment. The electronic access key 10 comprises a memory 15" holding access data 26 which, when read by a reader device in a configuration period, allows the reader device to determine whether to grant or deny access. The electronic access key 10 supports an electronic access key protocol which is supported by the reader device 1.

[0037] Fig 6 is a schematic graph illustrating operation of the reader device 1 of Figs 1 and 2 according to one embodiment. At time t_0 , the reader device is powered up. During a configuration period 30, the reader device is arranged to read any electronic configuration key 11 provided within range of the near field radio frequency communication device 3. The configuration period ends at time t_i , which is a configuration duration after the power on time t_0 . The configuration duration represents an amount of time (e.g. a certain number of seconds) and is a parameter which is stored in the reader device. After the time t_i , the reader device 1 is in a normal operation period 31 and grants or denies access using the electronically controlled physical lock in dependence on what electronically access keys are provided in the vicinity of its near field radio frequency communication device 3.

[0038] The reader device is also only responsive to electronic reset keys in the configuration period 30, and not during the normal operation period 31. Using the configuration period 30, a greater degree of security is provided, since a configuration, and optionally reset, of the reader device using appropriate electronic keys can only be performed during a relatively short period. This reduces the risk of unauthorised attempts to configure and/or reset the reader device 1, e.g. to gain unlawful access

to a physical space.

[0039] Fig 7 is a schematic diagram illustrating a user interface device of the user interface device 9 of Fig 2 according to one embodiment. The user interface device 9 comprises a plurality of operation indicators 35a-e, an optional display 37 and an alphanumeric keypad 36.

[0040] The operation indicators 35a-e can for instance indicate when access is allowed, access is denied, or that a code sequence needs to be entered on the keypad. The operation indicators 35a-e can be provided using different coloured lights and/or different symbols. In one embodiment, operation indicators using green and red are provided at either end of the set of operation indicators. For example, the first operation indicator 35a can be red and the last operation indicator 35e can be green, or vice versa. In this way, there is less risk of colour blind users confusing a green operation indicator for a red operation indicator or vice versa, since the user will eventually learn from experience which end corresponds to which coloured operation indicator. For example, a green operation indicator can indicate that an intrusion detection system is disarmed and a red operation indicator can indicate that an intrusion detection system is armed. While Fig 7 illustrates five operation indicators 35a-e, any suitable number of operation indicators can be provided.

[0041] The display 37 is used to convey configurable information to the user. In one embodiment, the display 37 is used to, upon granted access, display until how long the electronic access key is valid, e.g. an end validity date.

[0042] Optionally, the reader device 1 is integrated with the user interface device 9.

[0043] Fig 8 is a schematic side view of the user interface device 9 of Figs 1 and 7 according to one embodiment. It is here shown how a cable 45 connects the user interface device 9 with other components of the system (see Fig 1). The cable 45 is guided by a frame 41. In the space behind the frame 41, any excess cable can be stored. In this way, installation of an outer shell 40 can be done after the cable 45 is provided in a suitable way, which simplifies installation of the user interface device.

[0044] Fig 9 is a flow chart illustrating one embodiment of a method performed in the reader device of Fig 1 and 2.

[0045] In a *read config* step 50, configuration data is read from an electronic configuration key.

[0046] In an *inactivate electronic access key protocol* step 52, one or more electronic access key protocols in the reader device are inactivated based on the configuration data.

[0047] In an optional apply installation specific configuration step (51) an installation specific installation is applied for at least one electronic access key protocol, based on the configuration data. This can be used to improve and customise the security from the generic configuration.

[0048] In an *end configuration period* step 53, a configuration period (see 30 of Fig 6) is ended at a time which is a configuration duration after when the reader device

1 is powered up. In this way, the *inactivate electronic access key protocol* step 52 is only performed during the configuration period.

[0049] In a *read access data* step 54, access data is read from an electronic access key. This step can be performed a significant amount of time after the previous steps.

[0050] In a *send access data* step 56, the reader device sends the access data, e.g. to the local control unit. Thereby, the local control unit can determine, based on the access data read from the electronic access key, whether the electronic access key is eligible to gain access to the electronically controlled physical lock. When access is granted, the electronically controlled physical lock is set in the unlocked state. Otherwise, the electronically controlled physical lock is set (or remains) in the locked state. The method can repeat the *read access data* step 54 and *send access data* step 56 as necessary, in a normal operation mode of the reader device.

[0051] In a *read reset data* step 58, reset data is read from an electronic reset key.

[0052] In a *reset reader device* step 60, the reader device is conditionally reset based on the reset data, i.e. when the reset data is considered to be valid reset data. In this way, all of the supported plurality of electronic access key protocols are enabled in the reader device to allow reconfiguration of the reader device.

[0053] The invention has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims.

Claims

1. A reader device (1) arranged to read access rights of an electronic access key (10) for gaining access to open an electronically controlled physical lock (8), the reader device (1) supporting a plurality of electronic access key protocols for entering into communication with an electronic access key and the reader device (1) comprising:

a near field radio frequency communication device (3) arranged to read configuration data (20) from an electronic configuration key (11);

a controller (4) arranged to inactivate at least one electronic access key protocol in the reader device based on the configuration data (20); wherein the near field radio frequency communication device (3) is further arranged to read access data (26) from an electronic access key (10); and the reader device is arranged to send the access data (26) to a controller unit for determining whether the electronic access key (10) is eligible to open the electronically controlled

- physical lock (8), wherein the near field radio frequency communication device (3) is further arranged to read reset data from an electronic reset key (12); and
 the controller (4) is arranged to reset the reader device based on the reset data, to thereby enable all of the supported plurality of electronic access key protocols in the reader device; wherein the reader device (1) is only responsive to configuration data and reset data during a configuration period, wherein the configuration period starts when the reader device is powered up and the configuration period ends a configuration duration after when the reader device (1) is powered up, wherein the configuration duration represents an amount of time and the configuration duration is a parameter which is stored in the reader device.
2. The reader device (1) according to claim 1, wherein the configuration data (20) comprises a communication control command section (21) and a communication control parameter section (22).
 3. The reader device (1) according to any one of the preceding claims, wherein the controller (4) is further arranged to apply an installation specific configuration for at least one electronic access key protocol, based on the configuration data (20).
 4. The reader device (1) according to any one of the preceding claims, wherein the near field radio frequency communication device (3) is operable around a centre frequency of 13.56 MHZ.
 5. A method for configuring a reader device according to claim 1 for reading access rights of an electronic access key (10) for gaining access to open an electronically controlled physical lock (8), the method being performed in a reader device (1) supporting a plurality of electronic access key protocols for entering into communication with an electronic access key, wherein the reader device is responsive, only during a configuration period, both to configuration data from an electronic configuration key and to reset data from an electronic reset key, the method comprising the steps of:
 - starting the configuration period when the reader device is powered up;
 - reading (50), when an electronic configuration key is provided, configuration data (20) from an electronic configuration key (11);
 - inactivating (52), when an electronic configuration key is provided, at least one electronic access key protocol in the reader device based on the configuration data (20);
 - reading (58), when an electronic reset key is pro-

vided, reset data from an electronic reset key (12); and
 resetting (60) when an electronic reset key is provided, the reader device (1) based on the reset data, to thereby enable all of the supported plurality of electronic access key protocols in the reader device; and
 ending (53) the configuration period at a time being a configuration duration after when the reader device (1) is powered up; and wherein the steps of inactivating (52) and resetting (60) are only performed during the configuration period, wherein the configuration duration represents an amount of time and the configuration duration is a parameter which is stored in the reader device.

6. The method according to claim 5, wherein the configuration data (20) comprises a communication control command section (21) and a communication control parameter section (22).
7. The method according to any one of claims 5 to 6, further comprising the step, after the step of reading the configuration data, of:
 - applying (51) an installation specific configuration for at least one electronic access key protocol, based on the configuration data (20).
8. The method according to any one of claims 5 to 7, wherein the method further comprises a step of reading (54) access data (26) from an electronic access key (10), and wherein the step of reading the configuration data (50) and the step of reading the access data (54) comprise reading around a centre frequency of 13.56 MHZ.

Patentansprüche

1. Leservorrichtung (1), die angeordnet ist, Zugriffsrechte für einen elektronischen Zugriffsschlüssel (10) zu lesen, um Zugriff zu erhalten, um ein elektronisch gesteuertes physisches Schloss (8) zu öffnen, wobei die Leservorrichtung (1) eine Vielzahl von elektronischen Zugriffsschlüsselprotokollen zum Eintreten in eine Kommunikation mit einem elektronischen Zugriffsschlüssel unterstützt und die Leservorrichtung (1) Folgendes umfasst:
 - eine Nahfeldfunkfrequenzkommunikationsvorrichtung (3), die angeordnet ist, Auslegungsdaten (20) aus einem elektronischen Auslegungsschlüssel (11) zu lesen;
 - eine Steuerung (4), die angeordnet ist, mindestens ein elektronisches Zugriffsschlüsselprotokoll in der Leservorrichtung auf Basis der Auslegungsdaten (20) zu deaktivieren;

- wobei die Nahfeldfunkfrequenzkommunikationsvorrichtung (3) ferner angeordnet ist, Zugriffsdaten (26) aus einem elektronischen Zugriffsschlüssel (10) zu lesen; und die Leservorrichtung angeordnet ist, die Zugriffsdaten (26) zum Bestimmen, ob der elektronische Zugriffsschlüssel (10) zum Öffnen des elektronisch gesteuerten physischen Schlosses (8) qualifiziert ist, an eine Steuereinheit zu senden, wobei die Nahfeldfunkfrequenzkommunikationsvorrichtung (3) ferner angeordnet ist, Rücksetzdaten aus einem elektronischen Rücksetzschlüssel (12) zu lesen; und die Steuerung (4) ist angeordnet, die Leservorrichtung auf Basis der Rücksetzdaten zurückzusetzen, um dadurch alle der unterstützten Vielzahl von elektronischen Zugriffsschlüsselprotokollen in der Leservorrichtung zu aktivieren; wobei die Leservorrichtung (1) nur während einer Auslegungsperiode auf Auslegungsdaten und Rücksetzdaten reagiert, wobei die Auslegungsperiode beginnt, wenn die Leservorrichtung eingeschaltet wird, und die Auslegungsperiode eine Auslegungsdauer beendet, nachdem die Leservorrichtung (1) eingeschaltet wurde, wobei die Auslegungsdauer eine Zeitmenge repräsentiert und die Auslegungsdauer ein Parameter ist, der in der Leservorrichtung gespeichert ist.
2. Leservorrichtung (1) nach Anspruch 1, wobei die Auslegungsdaten (20) einen Kommunikationssteuerbefehlsbereich (21) und einen Kommunikationssteuerparameterbereich (22) umfassen.
 3. Leservorrichtung (1) nach einem der vorhergehenden Ansprüche, wobei die Steuerung (4) ferner angeordnet ist, eine installationsspezifische Auslegung auf Basis der Auslegungsdaten (20) für mindestens ein elektronisches Zugriffsschlüsselprotokoll anzuwenden.
 4. Leservorrichtung (1) nach einem der vorhergehenden Ansprüche, wobei die Nahfeldfunkfrequenzkommunikationsvorrichtung (3) um eine Mittenfrequenz von 13,56 MHz betreibbar ist.
 5. Verfahren zum Auslegen einer Leservorrichtung nach Anspruch 1 zum Lesen von Zugriffsrechten eines elektronischen Zugriffsschlüssels (10), um Zugriff zu erhalten, um ein elektronisch gesteuertes physisches Schloss (8) zu öffnen, wobei das Verfahren in einer Leservorrichtung (1) durchgeführt wird, die eine Vielzahl von elektronischen Zugriffsschlüsselprotokollen zum Eintreten in eine Kommunikation mit einem elektronischen Zugriffsschlüssel unterstützt, wobei die Leservorrichtung nur während einer Auslegungsperiode sowohl auf Auslegungsdaten von einem elektronischen Auslegungsschlüssel als auch auf Rücksetzdaten von einem elektronischen Rücksetzschlüssel reagiert, wobei das Verfahren die folgenden Schritte umfasst:
 5. Beginnen einer Auslegungsperiode, wenn die Leservorrichtung eingeschaltet wird;
 6. Lesen (50) von Auslegungsdaten (20) von einem elektronischen Auslegungsschlüssel (11), wenn ein elektronischer Auslegungsschlüssel bereitgestellt wird;
 7. Deaktivieren (52) von mindestens einem elektronischen Zugriffsschlüsselprotokoll in der Leservorrichtung auf Basis der Auslegungsdaten (20), wenn ein elektronischer Auslegungsschlüssel bereitgestellt wird;
 8. Lesen (58) von Rücksetzdaten aus einem elektronischen Rücksetzschlüssel (12), wenn ein elektronischer Rücksetzschlüssel bereitgestellt wird; und
 9. Rücksetzen (60) der Leservorrichtung (1) auf Basis der Rücksetzdaten, um dadurch alle der unterstützten Vielzahl von elektronischen Zugriffsschlüsselprotokollen in der Leservorrichtung zu aktivieren, wenn ein elektronischer Rücksetzschlüssel bereitgestellt wird; und
 10. Beenden (53) der Auslegungsperiode zu einer Zeit, bei der es sich um eine Auslegungsdauer handelt, nachdem die Leservorrichtung (1) eingeschaltet wurde; und wobei die Schritte des Deaktivierens (52) und des Rücksetzens (60) nur während der Auslegungsperiode durchgeführt werden, wobei die Auslegungsdauer eine Zeitmenge repräsentiert und die Auslegungsdauer ein Parameter ist, der in der Leservorrichtung gespeichert ist.
 6. Verfahren nach Anspruch 5, wobei die Auslegungsdaten (20) einen Kommunikationssteuerbefehlsbereich (21) und einen Kommunikationssteuerparameterbereich (22) umfassen.
 7. Verfahren nach einem der Ansprüche 5 bis 6, das ferner nach dem Schritt des Lesens der Auslegungsdaten den folgenden Schritt umfasst: Anwenden (51) einer installationsspezifischen Auslegung auf Basis der Auslegungsdaten (20) für mindestens ein elektronisches Zugriffsschlüsselprotokoll.
 8. Verfahren nach einem der Ansprüche 5 bis 7, wobei das Verfahren ferner einen Schritt des Lesens (54) von Zugriffsdaten (26) aus einem elektronischen Zugriffsschlüssel (10) umfasst und wobei der Schritt des Lesens der Auslegungsdaten (50) und der Schritt des Lesens der Zugriffsdaten (54) das Lesen um eine Mittenfrequenz von 13,56 MHz umfassen.

Revendications

1. Dispositif de lecture (1) agencé pour lire des droits d'accès d'une clé d'accès électronique (10) pour obtenir un accès pour ouvrir un verrou physique à commande électronique (8), le dispositif de lecture (1) prenant en charge une pluralité de protocoles de clé d'accès électronique pour entrer en communication avec une clé d'accès électronique et le dispositif de lecture (1) comprenant :

un dispositif de communication par radiofréquence en champ proche (3) agencé pour lire des données de configuration (20) depuis une clé de configuration électronique (11) ; un dispositif de commande (4) agencé pour désactiver au moins un protocole de clé d'accès électronique dans le dispositif de lecture sur la base des données de configuration (20) ; dans lequel le dispositif de communication par radiofréquence en champ proche (3) est en outre agencé pour lire des données d'accès (26) depuis une clé d'accès électronique (10) ; et le dispositif de lecture est agencé pour envoyer les données d'accès (26) à une unité de commande pour déterminer si la clé d'accès électronique (10) est admissible pour ouvrir le verrou physique à commande électronique (8), dans lequel le dispositif de communication par radiofréquence en champ proche (3) est en outre agencé pour lire des données de réinitialisation depuis une clé de réinitialisation électronique (12) ; et le dispositif de commande (4) est agencé pour réinitialiser le dispositif de lecture sur la base des données de réinitialisation, pour activer de ce fait l'intégralité de la pluralité prise en charge de protocoles de clé d'accès électronique dans le dispositif de lecture ; dans lequel le dispositif de lecture (1) ne répond à des données de configuration et à des données de réinitialisation qu'au cours d'une période de configuration, dans lequel la période de configuration commence lorsque le dispositif de lecture est mis sous tension et la période de configuration se termine une durée de configuration après la mise sous tension du dispositif de lecture (1), dans lequel la durée de configuration représente une quantité de temps et la durée de configuration est un paramètre qui est stocké dans le dispositif de lecture.

2. Dispositif de lecture (1) selon la revendication 1, dans lequel les données de configuration (20) comprennent une section d'instruction de commande de communication (21) et une section de paramètre de commande de communication (22).

3. Dispositif de lecture (1) selon l'une quelconque des

revendications précédentes, dans lequel le dispositif de commande (4) est en outre agencé pour appliquer une configuration spécifique à l'installation pour au moins un protocole de clé d'accès électronique, sur la base des données de configuration (20).

4. Dispositif de lecture (1) selon l'une quelconque des revendications précédentes, dans lequel le dispositif de communication par radiofréquence en champ proche (3) est utilisable autour d'une fréquence centrale de 13,56 MHz.

5. Procédé de configuration d'un dispositif de lecture selon la revendication 1 pour lire des droits d'accès d'une clé d'accès électronique (10) pour obtenir un accès pour ouvrir un verrou physique à commande électronique (8), le procédé étant réalisé dans un dispositif de lecture (1) prenant en charge une pluralité de protocoles de clé d'accès électronique pour entrer en communication avec une clé d'accès électronique, dans lequel le dispositif de lecture répond, uniquement au cours d'une période de configuration, à la fois à des données de configuration depuis une clé de configuration électronique et à des données de réinitialisation depuis une clé de réinitialisation électronique, le procédé comprenant les étapes suivantes :

le démarrage de la période de configuration lorsque le dispositif de lecture est mis sous tension ; la lecture (50), lorsqu'une clé de configuration électronique est fournie, de données de configuration (20) depuis une clé de configuration électronique (11) ;

la désactivation (52), lorsqu'une clé de configuration électronique est fournie, d'au moins un protocole de clé d'accès électronique dans le dispositif de lecture sur la base des données de configuration (20) ;

la lecture (58), lorsqu'une clé de réinitialisation électronique est fournie, de données de réinitialisation depuis une clé de réinitialisation électronique (12) ; et

la réinitialisation (60), lorsqu'une clé de réinitialisation électronique est fournie, du dispositif de lecture (1) sur la base des données de réinitialisation, pour activer de ce fait l'intégralité de la pluralité prise en charge de protocoles de clé d'accès électronique dans le dispositif de lecture ; et

la terminaison (53) de la période de configuration à un temps qui est une durée de configuration après la mise sous tension du dispositif de lecture (1) ; et dans lequel les étapes de la désactivation (52) et de la réinitialisation (60) ne sont réalisées qu'au cours de la période de configuration, dans lequel la durée de configuration représente une quantité de temps et la durée de

configuration est un paramètre qui est stocké dans le dispositif de lecture.

6. Procédé selon la revendication 5, dans lequel les données de configuration (20) comprennent une section d'instruction de commande de communication (21) et une section de paramètre de commande de communication (22). 5
7. Procédé selon l'une quelconque des revendications 5 et 6, comprenant en outre, après l'étape de la lecture des données de configuration, l'étape suivante : l'application (51) d'une configuration spécifique à l'installation pour au moins un protocole de clé d'accès électronique, sur la base des données de configuration (20) . 10 15
8. Procédé selon l'une quelconque des revendications 5 à 7, dans lequel le procédé comprend en outre une étape de lecture (54) de données d'accès (26) depuis une clé d'accès électronique (10), et dans lequel l'étape de la lecture des données de configuration (50) et l'étape de la lecture des données d'accès (54) comprennent la lecture autour d'une fréquence centrale de 13,56 MHz. 20 25

30

35

40

45

50

55

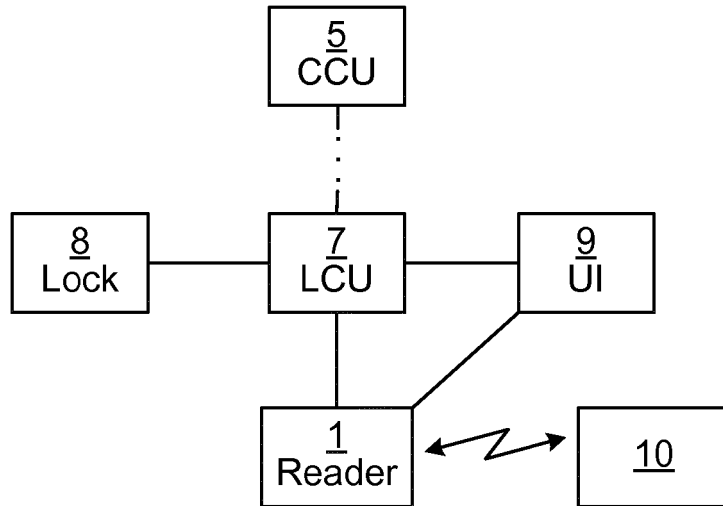


Fig. 1

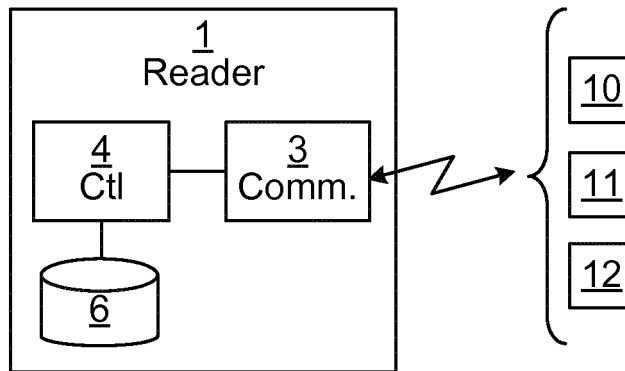


Fig. 2

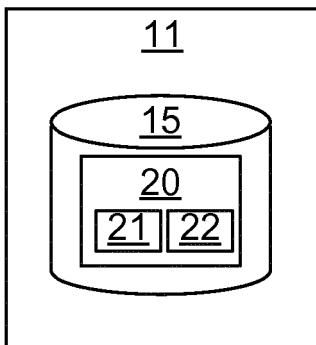


Fig. 3

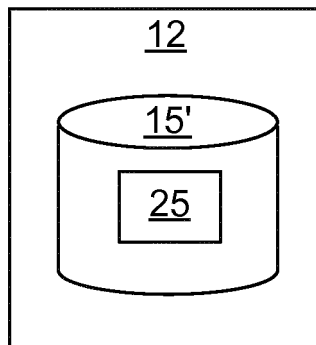


Fig. 4

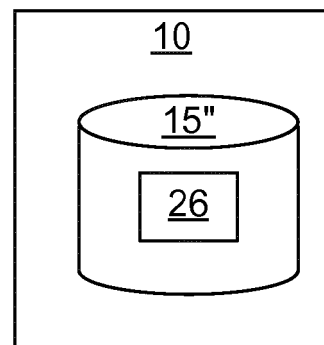


Fig. 5

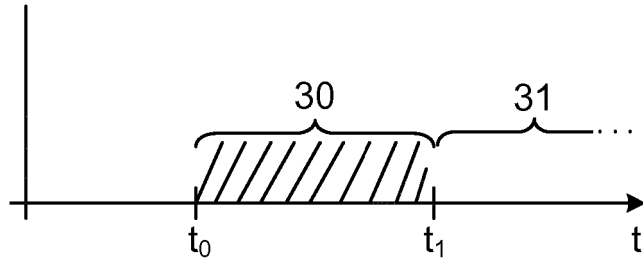


Fig. 6

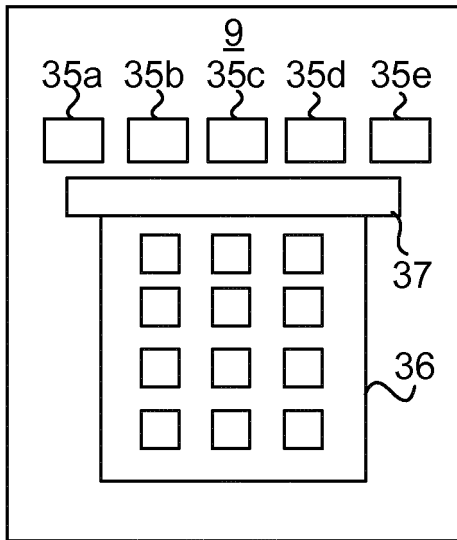


Fig. 7

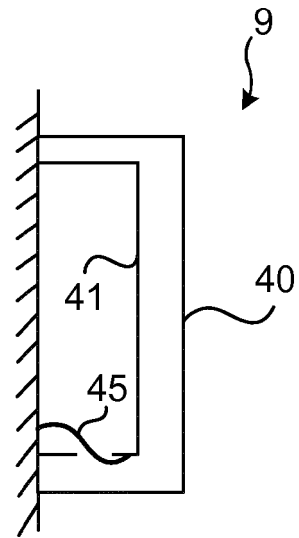


Fig. 8

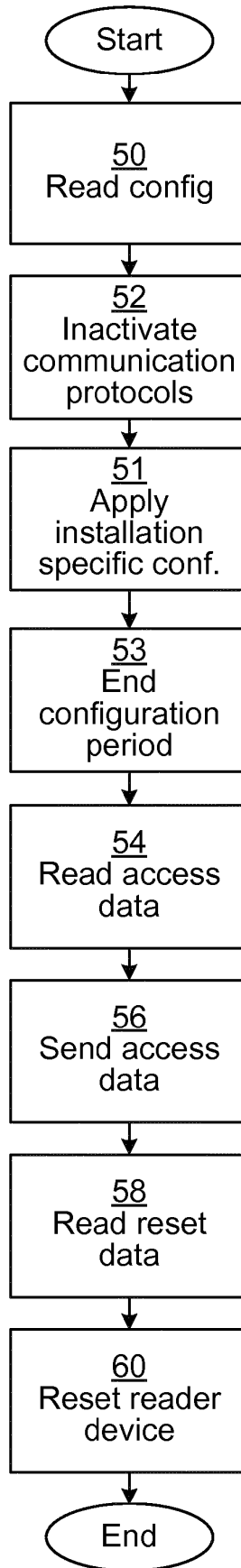


Fig. 9

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 2003028814 A1 [0005]
- US 2006224901 A1 [0005]
- US 2012096131 A1 [0005]
- EP 2584539 A1 [0005]
- US 5537103 A [0005]