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

(11) **EP 2 800 067 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
05.11.2014 Bulletin 2014/45

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Application number: **14164004.5**

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

(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
Designated Extension States:
BA ME

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

(71) Applicant: **ASSA AB**
631 05 Eskilstuna (SE)

(72) Inventors:
- **Berglund, Jens**
  632 32 Eskilstuna (SE)
- **Bovin, Perla**
  644 33 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)

(54) **Reader device and associated method**

(57) It is presented a reader device arranged to determine access rights of an electronic access key for gaining access to open an electronically controlled physical lock. The reader device supports a plurality of electronic access key protocols and the reader device comprises: a near field radio frequency communication device arranged to read access data from an electronic access key; a controller arranged to determine, based on the access data read from the electronic access key, whether the electronic access key is eligible to open the electronically controlled physical lock; wherein the near field radio frequency communication device is further arranged to read configuration data from an electronic configuration key; and the controller is arranged to inactivate at least one electronic access key protocol in the reader device based on the configuration data. A corresponding method is also presented.

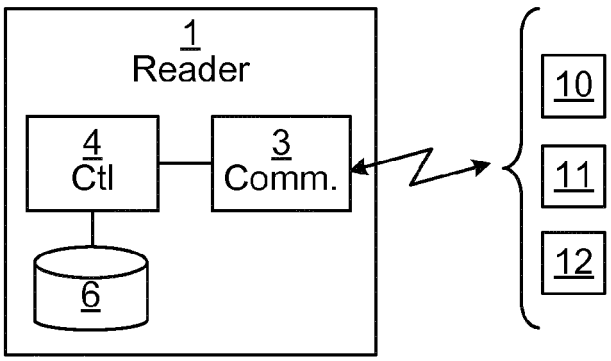

Fig. 2

EP 2 800 067 A2

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.

SUMMARY

[0005] It is an object to simplify installation of reader devices.

[0006] According to a first aspect, it is presented a reader device arranged to read access rights of an electronic access key for gaining access to open an electronically controlled physical lock. The reader device supports a plurality of electronic access key protocols and the reader device comprises: a near field radio frequency communication device arranged to read configuration data from an electronic configuration key; a controller arranged to inactivate at least one electronic access key protocol in the reader device based on the configuration data; wherein the near field radio frequency communication device is further arranged to read access data from an electronic access key; and the reader device is arranged to send the access data to a controller unit for determining whether the electronic access key is eligible to open the electronically controlled physical lock.

[0007] 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.

[0008] In one embodiment, the reader device is only responsive to configuration data during a configuration period, the configuration period ending a configuration duration after when the reader device is powered up. This reduces the risk of random people being able to reconfigure the lock, e.g. to circumvent access control of the reader device.

[0009] 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.

[0010] 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.

[0011] The near field radio frequency communication device is further arranged to read reset data from an electronic reset key; and the controller may be 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.

[0012] The electronic reset key may support an electronic access key protocol which is supported by the reader device and which has not been inactivated. In other words, it is here ensured that the reader device is able to read the electronic reset key without any need of modification.

[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 for reading access rights of an electronic access key for gaining access to open an electronically controlled physical lock. The method is performed in a reader device supporting a plurality of electronic access key protocols. The method comprises the steps of: reading configuration data from an electronic configuration key; inactivating at least one electronic access key protocol in the reader device based on the configuration data; reading access data from an electronic access key; and sending the access data to a controller unit for determining

whether the electronic access key is eligible to open the electronically controlled physical lock.

[0015] The method may further comprise the step of ending a configuration period at a time being a configuration duration after when the reader device is powered up; and wherein the step of inactivating is only performed during the configuration period.

[0016] The configuration data may comprise a communication control command section and a communication control parameter section.

[0017] The method may further comprise the step, after the step of reading the configuration data, of: applying an installation specific configuration for at least one electronic access key protocol, based on the configuration data.

[0018] The method may further comprise the steps of: reading reset data from an electronic reset key; and resetting 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.

[0019] The step of reading the reset data may comprise using an electronic access key protocol which is supported by the reader device and which has not been inactivated.

[0020] The step of reading the configuration data and the step of reading the data may comprise reading around a centre frequency of 13.56 MHZ.

[0021] 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.

[0022] 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

[0023] 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 environment 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 electronic reset key of Fig 2 according to one embodiment;

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

[0024] 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, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout the description.

[0025] 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.

[0026] 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.

[0027] 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.

[0028] 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.

[0029] 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).

[0030] 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).

[0031] 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.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] The controller 4 can be configured to execute the method described with reference to Fig 9 below.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] Optionally, 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 EV1, MIFARE Ultralight C, MIFARE DESFire, MIFARE DESFire EV1, MIFARE Plus, MIFARE sam av2, and Near Field Communication (NFC).

[0040] 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.

[0041] Fig 4 is a schematic diagram illustrating an electronic reset key 12 of Fig 2 according to one embodiment. 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.

[0042] 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 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.

[0043] Fig 6 is a schematic graph illustrating operation of the reader device 1 of Figs 1 and 2 according to one embodiment. At time to, 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 t1, which is a configuration duration after the power on time to. The configuration duration represents an amount of time (e.g. a certain number of seconds) and can e.g. be a parameter which is stored in the reader device.

[0044] After the time t1, 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 electronica access keys are provided in the vicinity of its near field radio frequency communication device 3.

[0045] Optionally, the reader device is also only responsive to electronic reset keys in the configuration period 30, and not during the normal operation period 31.

[0046] 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.

[0047] 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.

[0048] 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.

[0049] 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. en end validity date.

[0050] Optionally, the reader device 1 is integrated with the user interface device 9.

[0051] 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.

[0052] Fig 9 is a flow chart illustrating one embodiment of a method performed in the reader device of Fig 1 and 2.

[0053] In a *read config* step 50, configuration data is read from an electronic configuration key.

[0054] 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.

[0055] 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.

[0056] In an optional *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.

[0057] 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.

[0058] 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.

[0059] In an optional *read reset data* step 58, reset data is read from an electronic reset key. The reading of the reset data comprises using an electronic access key protocol which is supported by the reader device and which has previously been inactivated.

[0060] In an optional *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.

[0061] 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 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).

2. The reader device (1) according to claim 1, wherein the reader device (1) is only responsive to configuration data during a configuration period, the configuration period ending a configuration duration after when the reader device (1) is powered up.

3. The reader device (1) according to any one of the preceding claims, wherein the configuration data (20) comprises a communication control command section (21) and a communication control parameter section (22).

4. 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).

5. The reader device (1) according to any one of the preceding claims, 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.

6. The reader device (1) according to claim 5, wherein the electronic reset key (12) supports an electronic access key protocol which is supported by the reader device (1) and which has not been inactivated.

7. 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.

8. A method 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, the method comprising the steps of:

reading (50) configuration data (20) from an electronic configuration key (11);
inactivating (52) at least one electronic access key protocol in the reader device based on the configuration data (20);
reading (54) access data (26) from an electronic access key (10); and

sending (56) 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).

9. The method according to claim 8, further comprising the step of ending (53) a configuration period at a time being a configuration duration after when the reader device (1) is powered up; and wherein the step of inactivating (52) is only performed during the configuration period.

10. The method according claim 8 or 9, wherein the configuration data (20) comprises a communication control command section (21) and a communication control parameter section (22).

11. The method according to any one of claims 8 to 10, 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).

12. The method according to any one of claims 8 to 11, further comprising the steps of:

reading (58) reset data from an electronic reset key (12); and
resetting (60) 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.

13. The method according to claim 12, wherein the step of reading (58) the reset data comprises using an electronic access key protocol which is supported by the reader device (1) and which has not been inactivated.

14. The method according to any one of claims 8 to 13, wherein the step of reading the configuration data (50) and the step of reading the data (54) comprises reading around a centre frequency of 13.56 MHZ.

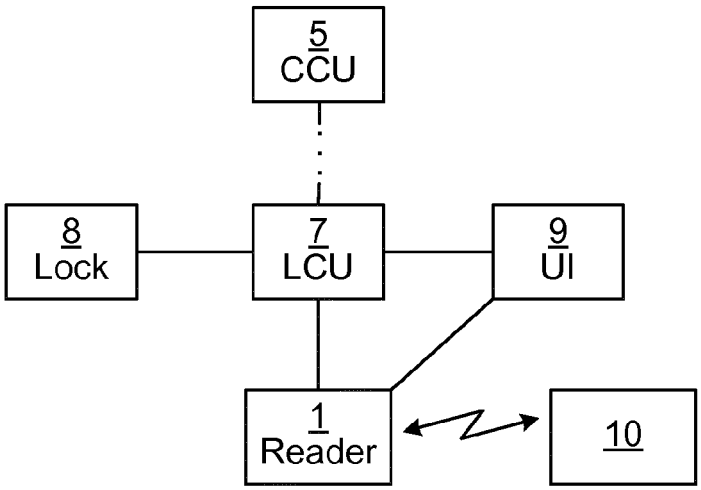

Fig. 1

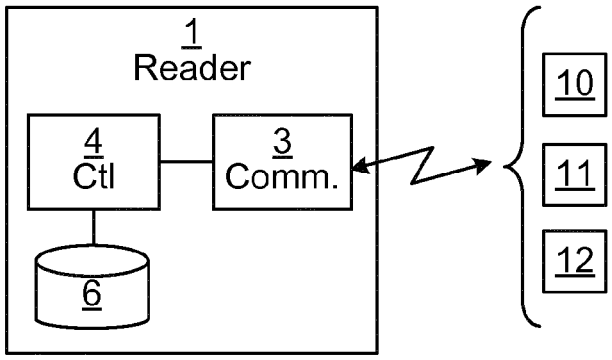

Fig. 2

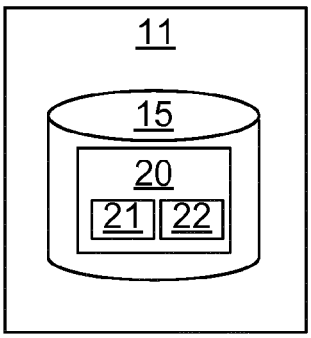

Fig. 3

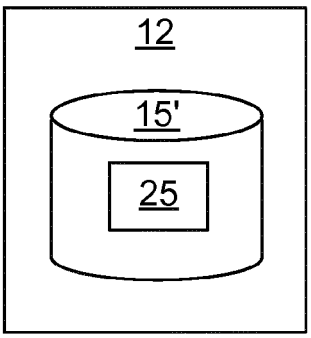

Fig. 4

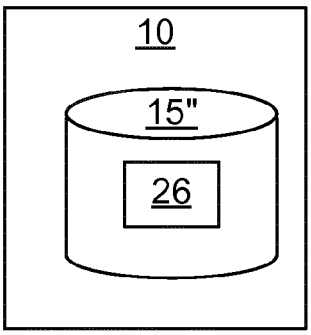

Fig. 5

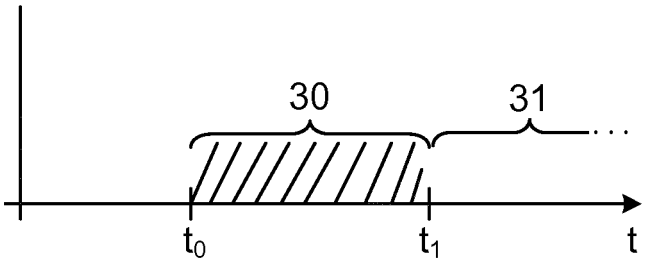

Fig. 6

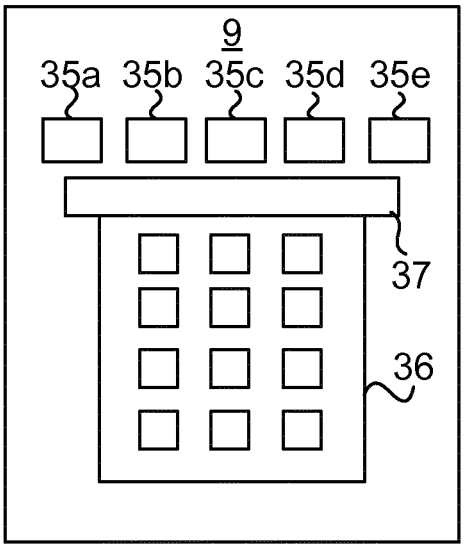

Fig. 7

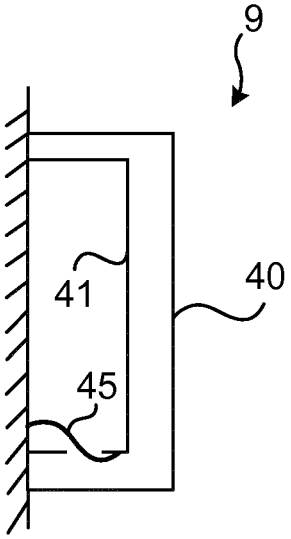

Fig. 8

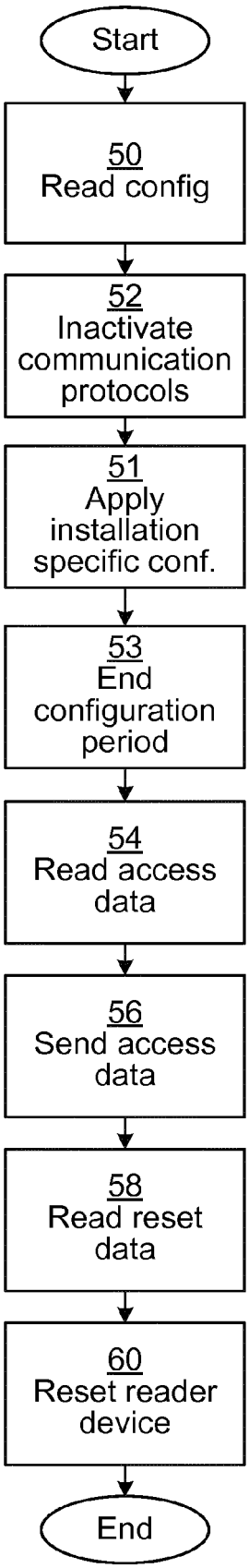
Start
50
Read config
52
Inactivate communication protocols
51
Apply installation specific conf.
53
End configuration period
54
Read access data
56
Send access data
58
Read reset data
60
Reset reader device
End

Fig. 9