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

(11) **EP 2 919 202 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
22.04.2020 Bulletin 2020/17

(51) Int Cl.:
G07C 9/00 *(2020.01)*

(21) Application number: **14158580.2**

(22) Date of filing: **10.03.2014**

(54) **RFID powered lock device**

RFID-angetriebene Verriegelungsvorrichtung

Dispositif de verrouillage à alimentation RFID

(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:
16.09.2015 Bulletin 2015/38

(73) Proprietor: **ASSA ABLOY AB**
107 23 Stockholm (SE)

(72) Inventors:
- **Holmström, Ingemar**
  192 56 Sollentuna (SE)
- **Einberg, Fredrik**
  141 41 Huddinge (SE)

(74) Representative: **Kransell & Wennborg KB**
P.O. Box 27834
115 93 Stockholm (SE)

(56) References cited:
EP-A1- 2 157 552
EP-A1- 2 592 601
EP-A2- 1 541 795
WO-A1-2005/054609
WO-A2-2007/079332
US-A1- 2002 024 420
US-A1- 2007 205 902
US-B2- 6 957 767

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).

EP 2 919 202 B1

Description

TECHNICAL FIELD

[0001] The invention relates to a lock device which is powered using RFID (Radio Frequency Identification) and associated method, computer program and computer program product.

BACKGROUND

[0002] Lock devices and key devices are evolving from the traditional pure mechanical locks. These days, various types of electronic key devices can be used to unlock lock devices. For example, wireless communication such as RFID, NFC (Near Field Communication), etc. or galvanic electronic connections can be used to communicate credentials from the key device to the lock device which can thereby grant or deny access.

[0003] However, the lock device needs to be powered by a power supply in some way to perform electronic access control, and unlock the lock device. This can e.g. be achieved using batteries, fixed line power, etc. For battery powered lock devices, this creates a maintenance requirement to make sure that the batteries do not run out. For fixed line powered locks, installation is made complex since an electrical power line needs to be drawn to the lock.

[0004] US 2010/0085160 discloses an electronic lock and key system utilising RFID. US2002/024420 A1 discloses a key for selectively allowing access to an enclosure having an unpowered lock and a lock controller. The key comprises: a housing. Located within the housing are: a processor operative to build variable signals for transmission from the key to the lock controller and to interpret the variable signals received by the key from the lock controller; a storage device in communication with the processor, the storage device operative to store data for building and interpreting the variable signals being alternately transmitted between the key and the lock controller for validating that the key is authorized to access the enclosure; a data transmitter in communication with the processor, the data transmitter operative to wirelessly transmit signals from the key to the lock controller, to inductively transmit an access request signal to the lock controller upon proper alignment with the lock controller, and to transmit an interrogation response signal in response to receiving to a variable interrogation request; a data receiver in communication with the processor, the data receiver operative to receive the variable interrogation signal; and a power transmitter in communication with the processor for wirelessly transmitting power to the lock controller simultaneously with the transmission of data.

[0005] EP 2 592 601 A1 discloses an electromechanical lock. The lock comprises an electronic circuitry means for providing a wireless interface for a communication device to proceed authentication with the communication device, and issue an open command provided that the authentication is successful; actuator means to receive the open command to set the lock in a mechanically openable state, the electronic circuitry means being configured to receive wirelessly from the communication device operating power for the electronic circuitry means and the actuator means. EP 2 157 552 A1 relates to an electromechanical lock with electronic circuitry configured to receive wirelessly from a communication device operating power for communication with the operating device, the lock further comprising a generator for powering an actuator configured to set the lock in a mechanically openable state. It would be greatly beneficial if there were to be a way to omit the battery or fixed line power of locks in the prior art.

SUMMARY

[0006] It is an object to provide a lock device which does not need battery power or main line power.

[0007] Accordingly, the invention for which protection is sought is defined by the independent claims and relates to a method performed in a lock device according to claim 1, a lock device according to claim 4, a computer program according to claim 5 and a computer program product according to claim 6. Advantageous embodiments of the invention are defined by the dependent claims. Embodiments and examples of the description not falling within the scope of the appended claims do not form part of the invention and are provided for illustration purposes only.

[0008] 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

[0009] The invention is now described, by way of example, with reference to the accompanying drawings, in which:

Fig 1 is a schematic diagram showing an environment in which embodiments presented herein can be applied;

Fig 2 is a schematic diagram illustrating some components of the key device and the lock device of Fig 1 and how these interact according to one embodiment;

Figs 3A-B are schematic sequence diagrams further illustrating the interaction between the key device

and the lock device 1 of Fig 1 according to various embodiments;

Figs 4A-B are flow charts illustrating methods according various embodiments performed in the lock device of Figs 1-3; and

Fig 5 is a schematic diagram showing one example of a computer program product comprising computer readable means.

DETAILED DESCRIPTION

[0010] 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.

[0011] Fig 1 is a schematic diagram showing an environment in which embodiments presented herein can be applied.

[0012] In this example, there is a door 15 which mechanically interacts with a lock device 1 using a mechanical interface 17, such as a bolt. A key device 10 can interact with the lock device 1, after which the lock device 1 determines whether to grant access, and the lock device 1 is set in an unlocked state when access is granted. When the lock device 1 is in an unlocked state, the door 15 can be opened and when the lock device 1 is in a closed state, the door cannot be opened. In this way, access to a closed space 16 is controlled by the lock device 1. It is to be noted that the lock device 1 can be located in a fixed structure by the door, such as the door frame (not shown) or in the door 15 (as shown).

[0013] Fig 2 is a schematic diagram illustrating some components of the key device 10 and the lock device 1 of Fig 1 and how these interact according to one embodiment.

[0014] The key device 10 and the lock device 1 interact using RFID so that the lock device 1 can be set in an unlocked state when it grants access to the key device.

[0015] In the prior art for RFID based locks and keys, the key device is a passive RFID tag (or behaves like one) and the lock device is an RFID reader. An advantage of that is that the key device does not need to have any other energy source than the energy received over wireless energy transfer from the RFID reader. Common passive RFID standards used in this field are ISO/IEC 14443 and ISO/IEC 15693, both using an RF carrier of 13,56 MHz to create a field suitable for energy and data transfer. It shall be noted that embodiments presented herein are not limited to the use of these standards only. Other frequencies including high frequency, low frequency (such as 125 KHz), ultra high frequency (such as 900 MHz) or any other suitable frequency may equally well be used.

[0016] It is to be noted that herein, the term reader refers to the side generating the RF carrier driving the RF field and transmitting data e.g. via direct modulation (such as amplitude-shift keying) of the carrier. The term tag used herein refers to the side receiving data and energy from the reader and transmitting data back, e.g. via load modulation of the RF field. Referring to mentioned standards other names for the reader and tag are Proximity Coupling Device -PCD and Printed Integrated Circuit Card - PICC (as used in ISO/IEC 14443) and Vicinity Coupling Device - VCD and Vicinity Integrated Circuit Card - VICC (as used in ISO/IEC 15693).

[0017] However, the inventors have realised that instead, since the key device 10 these days is often a powered device, such as a mobile phone, the key device 10 can be the RFID reader and the lock device 1 can behave as an RFID tag. In this way, the lock device 1 can receive energy using wireless energy transfer from the key device, i.e. from the RF field created by the key device. In this way, the lock device 1 does not need any battery, fixed line power, etc. Furthermore, complementary energy harvesting, e.g. solar cells, is used to reduce the amount of energy that has to be harvested from the RF field.

[0018] Hence, the lock device 1 is a passive RFID device, i.e. a tag type device, and the key device is an active RFID reader.

[0019] The key device 10 thus comprises an RFID reader 12 connected to an antenna 13. Furthermore, the key device 10 comprises a power source 13, such as one or more of a rechargeable or disposable battery, and a controller 11. The controller 11 can be any combination of one or more of a suitable central processing unit (CPU), multiprocessor, microcontroller unit (MCU), digital signal processor (DSP), application specific integrated circuit etc., capable of executing software instructions or otherwise controllable to behave according to predetermined logic. The key device 10 may be implemented as a mobile phone, a smartphone, a key fob, credit card shaped device, etc.

[0020] A memory 18 is provided which can store credential data of the key device 10. The credential data in the key is used to determine whether a key is to be granted access to open a lock. In other words, credential data can be considered to be access rights to a lock. The memory 18 can be any combination of read and write memory (RAM) and read only memory (ROM). The memory 18 also comprises persistent storage, which, for example, can be any single one or combination of solid state memory, magnetic memory, or optical memory storing a computer program with software instructions for performing the steps of the key device described with reference to Figs 3A-B below.

[0021] Other components of the key device, such as user interface components, etc. are omitted here for rea-

sons of clarity.

[0022] The lock device 1, in turn, comprises a passive RFID transceiver 2 with a connected antenna 6. The RFID reader 12 and the passive RFID transceiver 2 interact over a wireless interface 17 which is used both to transfer energy from the RF field generated by the RFID reader 12 to the passive RFID transceiver 2 and for communication in either direction, as shown in more detail in Figs 3A-B and described below.

[0023] An energy harvester 8 is configured to use energy harvesting as an additional energy source, e.g. using solar cells, mechanical to electrical conversion of a door handle, etc.

[0024] The electrical energy from the passive RFID transceiver 2 and the energy harvester 8 is stored in energy storage 7. The energy storage can e.g. be a capacitor and/or battery. The passive RFID transceiver itself is powered from the RF field. The excess energy is stored in the energy storage which is the power source for all other components in the lock device.

[0025] A controller 3 controls the general operation of the lock device. 1. The controller 3 can be any combination of one or more of a suitable central processing unit (CPU), multiprocessor, microcontroller unit (MCU), digital signal processor (DSP), application specific integrated circuit (ASIC) etc., capable of executing software instructions or otherwise configured to behave according to predetermined logic.

[0026] In one embodiment, the controller 3 receives credential data from the passive RFID transceiver 2. In this way, the controller 3 makes an access decision, determining whether to grant access and unlock the lock device for the key device 10 communicating with the passive RFID transceiver. The credential data can be checked locally, e.g. checking against data in a memory 14 such as lock identification data, comprising a unique lock ID and optionally a lock group ID (a lock can belong to a group of locks) and a site ID. The memory 14 can be any combination of read and write memory (RAM) and read only memory (ROM). The memory 14 also comprises persistent storage, which, for example, can be any single one or combination of solid state memory, magnetic memory, or optical memory, storing a computer program with software instructions for performing the method according to the embodiments described below.

[0027] In a non-claimed embodiment, it is the key device 10 that makes the access decision and sends the result of the access decision to the lock device.

[0028] Based on the access decision in the lock device or the key device, unlocking is conditionally performed. If the lock device 1 is not to be unlocked, no action needs to be performed and the lock device 1 remains in a closed state.

[0029] Optionally, user feedback is provided using a user interface 9 to inform of the denied access. If the lock device 1 is to be unlocked, the controller 3 provides an unlock signal to a motor driver 4. Optionally, user feedback of the granted access can be provided using the user interface in a way that differs from any user feedback for denied access. For example, denied access can be indicating by lighting a red light emitting diode (LED) (not shown) and granted access can be indicated by lighting a green LED. Alternatively or additionally, denied access is indicated by blinking the LED while granted access is indicated with a solid lit LED. Alternatively or additionally a message of the result can be shown on a display.

[0030] The motor driver 4 then sends a motor control signal to a motor 5 to operate in order to set the lock device 1 in an unlocked state. Optionally, the motor driver 4 is part of the motor 5. Once the motor 5 is provided with the motor control signal, it is activated and can thereby move a mechanical interface, e.g. to allow movement of the bolt 17 of Fig 1, to set the lock device 1 in an unlocked state. The motor 5 can e.g. be a direct current motor which can be made small, energy efficient and at low cost. The motor 5 uses the energy stored in the energy storage 7 to perform the unlock action. Once in the unlocked state, a knob or handle can then be used by the user to manually move the lock bolt so that it is possible to open the door. This user actuated mechanical action is harvested by an energy harvester 8 comprising a mechanical to electrical power converter (connected to the handle or knob), to thereby store electrical energy in the energy storage 7.

[0031] Unlocked state is here to be interpreted that the lock mechanism has been actuated in a way so that it is possible to move the bolt or other physical arrangement to gain access to the access controlled space. The bolt could be driven by a motor as well, but in such arrangement additional energy harvesting and/or a battery may be required.

[0032] In one embodiment, there is no motor and motor driver and instead the controller, when access is granted, sends a signal to a solenoid (not shown) to set the lock device 1 in an unlocked state.

[0033] Figs 3A-B are schematic sequence diagrams further illustrating the interaction between the key device 10 and the lock device 1 of Fig 1 according to various embodiments. First, the embodiment of Fig 3A will be described, where the access decision is made in the lock device.

[0034] When the key device 10 approaches the lock device 1, the key device 10 transmits an RF (Radio Frequency) carrier 20 to the lock device 1.

[0035] This causes the lock device 1 to wake up, i.e. to enter an active state, and to start receiving energy over the wireless interface with the key device 10.

[0036] The key device 10 will then initiate an RFID initialisation 22 with the lock device 1. This can e.g. comprise anti-collision procedures to resolve any potential situation with several tags in the vicinity of the key device (being the RFID reader). This will result in the key device 10 obtaining the RFID UID (Unique Identifier) of the lock device. The UID may, but does not need to, be used as a lock identifier for a later access decision. The lock device 1 and the key device 10 then perform a mutual au-

thentication 23 to achieve a secure communication channel between the key device 10 and the lock device 1. The mutual authentication may be based on cryptographic principles. For example, a 3-pass mutual authentication algorithm could be used.

[0037] At this stage, the key device 10 is ready to send its credential data to the lock device 1. Since the key device is an RFID reader, this is done using a write credentials command 21.

[0038] Once the lock device 1 has received the credential data in the write credentials command 21, it performs an access decision 25 based on this, e.g. comparing with lock identification data. The lock identification data previously stored in the lock device comprises a lock ID and optionally a site ID and lock group ID. The credential data received from the key comprises one or more of a list of supported site IDs, lock IDs, and lock group IDs. The lock checks the credential data of the write command for a match with the lock identification data stored in the lock device.

[0039] Optionally, the lock device 1 transmits the result 26 of the access decision to the key device 10, which allows the key device 10 to notify the user 29, e.g. using a display of a host device of the key device, such as a mobile phone.

[0040] If the access decision results in granted access, the lock device 1 unlocks 28 and enters an unlocked state.

[0041] Now, the non-claimed embodiment of Fig 3B will be described, where the access decision is made in the key device. Only the communication and execution which differs from what is described with reference to Fig 3A will be described here.

[0042] In this embodiment, it is the key device 10 which performs the access decision 25'. The lock identification data 24 is read from the lock device 1 after the mutual authentication. In the access decision 25', the key device 10 then checks the lock identification against the credential data stored in the key for an access decision.

[0043] When the access decision 25' results in granted access, the key device 10 sends an unlock command 30 to the lock device 1 which subsequently unlocks 28 the lock the device.

[0044] Optionally, if access is denied, the key device 10 also notifies the lock device 1 by sending an access denied message to the lock device 1.

[0045] Optionally, the key device 10 notifies the user 29 of the result of the access decision 25'.

[0046] Optionally, the lock device 1 notifies the user about the access decision it has received from the key device 10 via LEDs as previously described or in other ways.

[0047] Figs 4A-B are flow charts illustrating methods according various embodiments performed in the lock device of Figs 1-3. The method is performed to controllably unlock the lock device.

[0048] In a *start to receive wireless energy* step 40, energy is received from a key device using wireless energy transfer. The energy is received in the passive RFID transceiver (2 of Fig 2) of the lock device, which is thus transferred from the RFID reader (12 of Fig 2) of the key device. The passive RFID transceiver itself is powered from the RF field. The excess energy is stored in the energy storage which is the power source for all other components in the lock device. This step corresponds to the wake up and start receiving energy 21 of Figs 3A-B.

[0049] In an *enter active state* step 42, the lock device enters an active state when sufficient energy has been harvested to power a sufficient number of components to make the lock device operational. It is to be noted though, at this stage, that the motor and motor driver do not need to be powered. This step corresponds to the wake up and start receiving energy 21 of Figs 3A-B.

[0050] In an *exchange RFID data* step 44, RFID data is exchanged with the RFID reader, i.e. the key device. This step can include RFID initialisation (22 of Figs 3A-B) where the key device (RFID reader) initiates an anti-collision sequence with the lock device to resolve any potential situation with several tags in the vicinity of the RFID reader. This will result in the key device obtaining the RFID UID of the lock device. The UID may, but does not need to, be used as a lock identifier. Moreover, this step can include performing mutual authentication (23 of Figs 3A-B) to achieve a secure communication channel between the key device 10 and the lock device 1.

[0051] In a *obtain access decision* step 46, an access decision is obtained. This access decision can be received from the key device or the lock device can make this access decision based on the RFID data. This step corresponds to the access decision 25 of Fig 3A and the access decision 25' of Fig 3B.

[0052] Optionally, there is a *transmit result* step 47, where the result of the access decision is transmitted to the key device, e.g. for notification to the user, when the access decision is made by the lock device. This corresponds to the transmission of the results message 26 of Fig 3A.

[0053] In a conditional *access granted* step 48, the result of the *obtain access decision* step 46 is evaluated. If access is granted, then the method proceeds to a conditional *sufficient energy* step 49. Otherwise, the method proceeds to a *notify user* step 53, or if this step is not performed, to an *enter idle state* step 52.

[0054] In the conditional *sufficient energy* step 49, it is determined whether wireless energy more than a threshold amount has been received. This can e.g. be done by measuring a voltage across the energy storage (7 of Fig 2). The threshold amount can then be defined as a threshold voltage. The threshold amount is determined such that there is sufficient energy to unlock the lock device. Optionally, the threshold amount is set such that there is some margin of error. If there is sufficient energy stored in the lock device, the method proceeds to an *unlock* step 50. Otherwise, the method proceeds to a *receive more energy* step 51.

[0055] In the *receive more energy* step 51, more wire-

less energy is received from the key device and stored in the energy storage.

[0056] In the *unlock* step, the lock device is mechanically unlocked, e.g. by sending a control signal to a motor (5 of Fig 2) or a solenoid. This step corresponds to the unlock 28 of Figs 3A-B.

[0057] There is a *receive additional energy* step 38, which can be performed in parallel to the *start to receive wireless energy* step 40. In this step, another energy source is utilised using energy harvesting such as using solar cells, mechanical to electrical conversion of a door handle, etc. It is to be noted that in such a case, the conditional *sufficient power* step 49 determines if the lock device in total has sufficient power from both wireless energy transfer and the energy received in the *receive additional energy* step 38.

[0058] After the *unlock* step 50, there is an optional *notify user* step 53. In this step, if the preceding step was the *unlock* step 50, the user is notified either that the lock device is unlocked. On the other hand, if the preceding step was the conditional *access granted* step 48, access was denied, and the user is notified that access was denied. The notification of the user can e.g. occur using light emitting diodes (LEDs) of different colours or different blinking patterns of a single LED. When the lock device is in unlocked state, the user can open the door and the door can be set in a locked state again, e.g. by manually actuating a lock mechanism of the lock device. As explained above, the mechanical energy of the user opening the door and/or locking the door can optionally be harvested and stored as electrical energy in the energy storage (7 of Fig 2) of the lock device.

[0059] In the *enter idle state* step 52, the lock device returns to the idle state to conserve energy.

[0060] The method can then be repeated once wireless power is received again from a key device.

[0061] It is to be noted that the method does not need to be performed sequentially as described above. In particular, the lock device 1 can receive wireless energy at the same time as it performs other steps, such as entering the active state, exchanging RFID data and makes the access decision.

[0062] Fig 4B is a flow chart illustrating an embodiment of the *exchange RFID data* step 44 of Fig 4A according to one embodiment. There are here two substeps: an *initialisation* sub-step 44a and a *receive write command* sub-step 44b.

[0063] In the *initialisation* substep 44a, the key device initiates the communication with the lock device. This substep corresponds to the RFID initialisation 22 of Figs 3A-B and may comprise anti-collision procedures to resolve any potential situation with several tags in the vicinity of the key device (being the RFID reader). This will result in the key device obtaining the RFID UID of the lock device.

[0064] In *receive write command* step 44b, a command is received from the key device to write credential data. This is the credential data used in the *obtain access decision* step 46 of Fig 4A.

[0065] Fig 5 is a schematic diagram showing one example of a computer program product 90 comprising computer readable means. On this computer readable means a computer program 91 can be stored, which computer program can cause a processor to execute a method according to embodiments described herein. In this example, the computer program product is an optical disc, such as a CD (compact disc) or a DVD (digital versatile disc) or a Blu-Ray disc. As explained above, the computer program product could also be embodied in a memory of a device, such as the memory 14 of Fig 2. While the computer program 91 is here schematically shown as a track on the depicted optical disk, the computer program can be stored in any way which is suitable for the computer program product.

[0066] 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 method performed in a lock device (1), the method comprising the steps of:

   receiving (40), in a passive Radio-frequency Identification, RFID, transceiver (2), energy from a key device (10) comprising an RFID reader (12), using wireless energy transfer;
   receiving (38) additional energy from an additional energy source (7) based on energy harvesting;
   entering (42) an active state from an idle state;
   exchanging (44) RFID data with the RFID reader, comprising receiving (44a) a request of an identifier of the lock device, and receiving (44b) a command to write credential data, the credential data comprising one or more of a list of site identifiers, lock identifiers and lock group identifiers;
   obtaining (46) an access decision based on the RFID data by making the access decision based on comparing the credential data against lock identification data in memory of the lock device (1); and
   mechanically unlocking (50) the lock device (1) when access is granted and wireless energy more than a threshold amount has been received and when the lock device in total has sufficient energy from both wireless energy transfer and the energy received in the receiving additional energy step.

2. The method according to any one of the preceding

claims, wherein the step of mechanically unlocking (50) comprises sending a control signal to a motor or a solenoid.

3. The method according to any one of the preceding claims, further comprising the step of:
transmitting (47) a result of the access decision to the key device (10).

4. A lock device (1) comprising:

a passive Radio-frequency Identification, RFID, transceiver (2) arranged to receive energy from a key device (10) comprising an RFID reader (12), using wireless energy transfer from a key device (10) such that the lock device enters an active state from an idle state, the passive RFID transceiver being further arranged to exchange RFID data with the RFID reader, to receive a request of an identifier of the lock device (1), and to receive a command to write credential data, the credential data comprising one or more of a list of site identifiers, lock identifiers and lock group identifiers;
a controller (3);
a memory (14) storing instructions that, when executed by the controller, causes the lock device (1) to obtain an access decision based on the RFID data, wherein the instructions to obtain an access decision comprise instructions that, when executed by the processor, causes the lock device (1) to make the access decision based on comparing the credential data against lock identification data in memory of the lock device (1);
an additional energy source (7) based on energy harvesting; and
an actuator (4) arranged to perform a mechanical unlocking action when access is granted and wireless energy more than a threshold amount has been received and when the lock device in total has sufficient energy from both wireless energy transfer and the additional energy source.

5. A computer program (91) comprising computer program code which, when run on a lock device (1), causes the lock device (1) to perform the method according to any one of claims 1 to 3.

6. A computer program product (90) comprising a computer program according to claim 5 and a computer readable means on which the computer program is stored.

Patentansprüche

1. Verfahren, das in einer Verriegelungsvorrichtung (1) durchgeführt wird, wobei das Verfahren die folgenden Schritte umfasst:

Empfangen (40), in einem passiven Radiofrequenzidentifikations- (RFID-) Sendeempfänger (2), von Energie aus einer Schlüsselvorrichtung (10), die ein RFID-Lesegerät (12) umfasst, unter Verwendung von drahtloser Energieübertragung;
Empfangen (38) von zusätzlicher Energie aus einer zusätzlichen Energiequelle (7) auf Basis von Energieernte;
Eintreten (42) in einen aktiven Zustand aus einem Ruhezustand;
Austauschen (44) von RFID-Daten mit dem RFID-Lesegerät, umfassend das Empfangen (44a) einer Anfrage eines Identifikators der Verriegelungsvorrichtung und das Empfangen (44b) eines Befehls zum Schreiben von Anmeldedaten, wobei die Anmeldedaten eines oder mehrere einer Liste von Ortsidentifikatoren, Verriegelungsidentifikatoren und Verriegelungsgruppenidentifikatoren umfassen;
Erhalten (46) einer Zugangsentscheidung auf Basis der RFID-Daten, indem die Zugangsentscheidung auf Basis des Vergleichens der Anmeldedaten mit Verriegelungsidentifikationsdaten im Speicher der Verriegelungsvorrichtung (1) getroffen wird; und
mechanisches Entriegeln (50) der Verriegelungsvorrichtung (1), wenn Zugang gewährt wird und drahtlose Energie über einer Schwellenmenge empfangen wurde und wenn die Verriegelungsvorrichtung insgesamt ausreichend Energie sowohl aus der drahtlosen Energieübertragung als auch der im Schritt des Empfangens zusätzlicher Energie empfangenen Energie aufweist.

2. Verfahren nach einem der vorangehenden Ansprüche, wobei der Schritt des mechanischen Entriegelns (50) das Senden eines Steuersignals an einen Motor oder ein Solenoid umfasst.

3. Verfahren nach einem der vorangehenden Ansprüche, ferner umfassend den Schritt des:
Übermittelns (47) eines Ergebnisses der Zugangsentscheidung an die Schlüsselvorrichtung (10).

4. Verriegelungsvorrichtung (1), umfassend:

einen passiven Radiofrequenzidentifikations- (RFID-) Sendeempfänger (2), der angeordnet ist, um Energie aus einer Schlüsselvorrichtung (10), die ein RFID-Lesegerät (12) umfasst, unter Verwendung von drahtloser Energieübertragung aus einer Schlüsselvorrichtung (10) zu empfangen, so dass die Verriegelungsvorrich-

tung aus einem Ruhezustand in einen aktiven Zustand eintritt, wobei der passive RFID-Sendeempfänger ferner angeordnet ist, um RFID-Daten mit dem RFID-Lesegerät auszutauschen, um eine Anfrage eines Identifikators der Verriegelungsvorrichtung (1) zu empfangen und um einen Befehl zum Schreiben von Anmeldedaten zu empfangen, wobei die Anmeldedaten eines oder mehrere einer Liste von Ortsidentifikatoren, Verriegelungsidentifikatoren und Verriegelungsgruppenidentifikatoren umfassen;
eine Steuereinheit (3);
einen Speicher (14), der Anweisungen speichert, die bei Ausführung durch die Steuereinheit herbeiführen, dass die Verriegelungsvorrichtung (1) eine Zugangsentscheidung auf Basis der RFID-Daten erhält, wobei die Anweisungen zum Erhalt einer Zugangsentscheidung Anweisungen umfassen, die bei Ausführung durch den Prozessor herbeiführen, dass die Verriegelungsvorrichtung (1) die Zugangsentscheidung auf Basis des Vergleichens der Anmeldedaten mit den Verriegelungsidentifikationsdaten im Speicher der Verriegelungsvorrichtung (1) trifft;
eine zusätzliche Energiequelle (7) auf Basis von Energieernte; und
einen Aktor (4), der angeordnet ist, um einen mechanischen Entriegelungsvorgang durchzuführen, wenn Zugang gewährt wird und drahtlose Energie über einer Schwellenmenge empfangen wurde und wenn die Verriegelungsvorrichtung insgesamt ausreichend Energie sowohl aus der drahtlosen Energieübertragung als auch der zusätzlichen Energiequelle aufweist.

5. Computerprogramm (91), umfassend Computerprogrammcode, der bei Ausführung auf einer Verriegelungsvorrichtung (1) herbeiführt, dass die Verriegelungsvorrichtung (1) das Verfahren nach einem der Ansprüche 1 bis 3 durchführt.

6. Computerprogrammprodukt (90), umfassend ein Computerprogramm nach Anspruch 5 und ein computerlesbares Medium, auf dem das Computerprogramm gespeichert ist.

Revendications

1. Procédé réalisé dans un dispositif de verrouillage (1), le procédé comprenant les étapes consistant à :

recevoir (40), dans un émetteur-récepteur (2) d'identification par radiofréquence passive, RFID, de l'énergie provenant d'un dispositif de clé (10) comprenant un lecteur de RFID (12), en utilisant un transfert d'énergie sans fil ;
recevoir (38) de l'énergie supplémentaire à partir d'une source d'énergie supplémentaire (7) en fonction d'une récupération d'énergie ;
entrer (42) dans un état actif à partir d'un état de veille ;
échanger (44) des données de RFID avec le lecteur de RFID, comprenant la réception (44a) d'une requête d'un identificateur du dispositif de verrouillage, et la réception (44b) d'une commande afin d'écrire des données d'accréditation, les données d'accréditation comprenant au moins l'une parmi une liste d'identificateurs de sites, d'identificateurs de verrouillage et d'identificateurs de groupes de verrouillage ;
obtenir (46) une décision d'accès en fonction des données de RFID en prenant la décision d'accès en fonction de la comparaison des données d'accréditation par rapport aux données d'identification de verrouillage en mémoire du dispositif de verrouillage (1) ; et
déverrouiller mécaniquement (50) le dispositif de verrouillage (1) lorsque l'accès est accordé et qu'une énergie sans fil supérieure à une valeur de seuil a été reçue et lorsque le dispositif de verrouillage a en tout une énergie suffisante provenant à la fois du transfert d'énergie sans fil et de l'énergie reçue dans l'étape de réception d'énergie supplémentaire.

2. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de déverrouillage mécanique (50) comprend l'envoi d'un signal de commande à un moteur ou à un solénoïde.

3. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre l'étape consistant à :
transmettre (47) un résultat de la décision d'accès au dispositif de clé (10).

4. Dispositif de clé (1) comprenant :

un émetteur-récepteur (2) d'identification par radiofréquence passive, RFID, agencé pour recevoir de l'énergie provenant d'un dispositif de clé (10) comprenant un lecteur de RFID (12), en utilisant un transfert d'énergie sans fil à partir d'un dispositif de clé (10) de telle sorte que le dispositif de verrouillage entre dans un état actif à partir d'un état de veille, l'émetteur-récepteur de RFID passif étant en outre agencé pour échanger des données de RFID avec le lecteur de RFID, pour recevoir une demande d'un identificateur du dispositif de verrouillage (1), et pour recevoir une commande afin d'écrire des données d'accréditation, les données d'équitation comprenant au moins l'une parmi une liste d'identificateurs de sites, d'identificateurs de verrouillage et d'identificateurs de groupes de

verrouillage ;
un dispositif de commande (3) ;
une mémoire (14) stockant des instructions qui, lorsqu'elles sont exécutées par le dispositif de commande, amène le dispositif de verrouillage (1) à obtenir une décision d'accès en fonction des données de RFID, dans lequel les instructions pour obtenir une décision d'accès comprennent des instructions qui, lorsqu'elles sont exécutées par le processeur, amènent le dispositif de verrouillage (1) à prendre la décision d'accès en fonction d'une comparaison des données d'accréditation par rapport aux données d'identification de verrouillage en mémoire du dispositif de verrouillage (1) ;
une source d'énergie supplémentaire (7) en fonction d'une récupération d'énergie ;
un actionneur (4) agencé pour réaliser une action de déverrouillage mécanique lorsque l'accès est accordé et de l'énergie sans fil supérieure à une quantité de seuil a été reçue et lorsque le dispositif de verrouillage a en tout une énergie suffisante provenant à la fois du transfert d'énergie sans fil et de la source d'énergie supplémentaire.

5. Programme informatique (91) comprenant un code de programme informatique qui, lorsqu'il est exécuté sur un dispositif de verrouillage (1), amène le dispositif de verrouillage (1) à réaliser le procédé selon l'une quelconque des revendications 1 à 3.

6. Produit de programme informatique (90) comprenant un programme informatique selon la revendication 5 et un support lisible par ordinateur sur lequel le programme informatique est stocké.

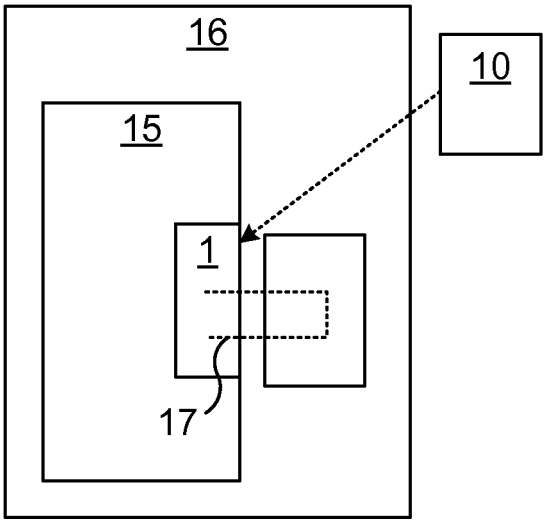

16
10
15
1
17

Fig. 1

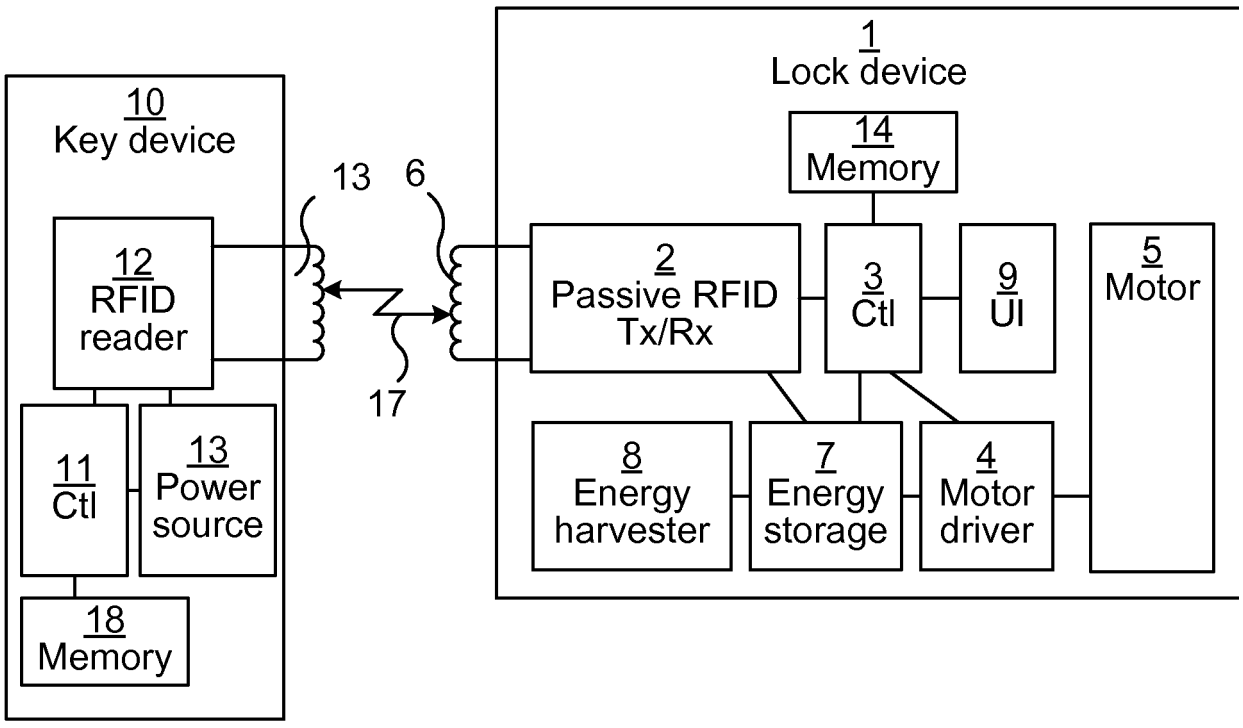

1
Lock device
14
Memory
10
Key device
13
6
12
RFID
reader
2
Passive RFID
Tx/Rx
3
Ctl
9
UI
5
Motor
17
11
Ctl
13
Power
source
8
Energy
harvester
7
Energy
storage
4
Motor
driver
18
Memory

Fig. 2

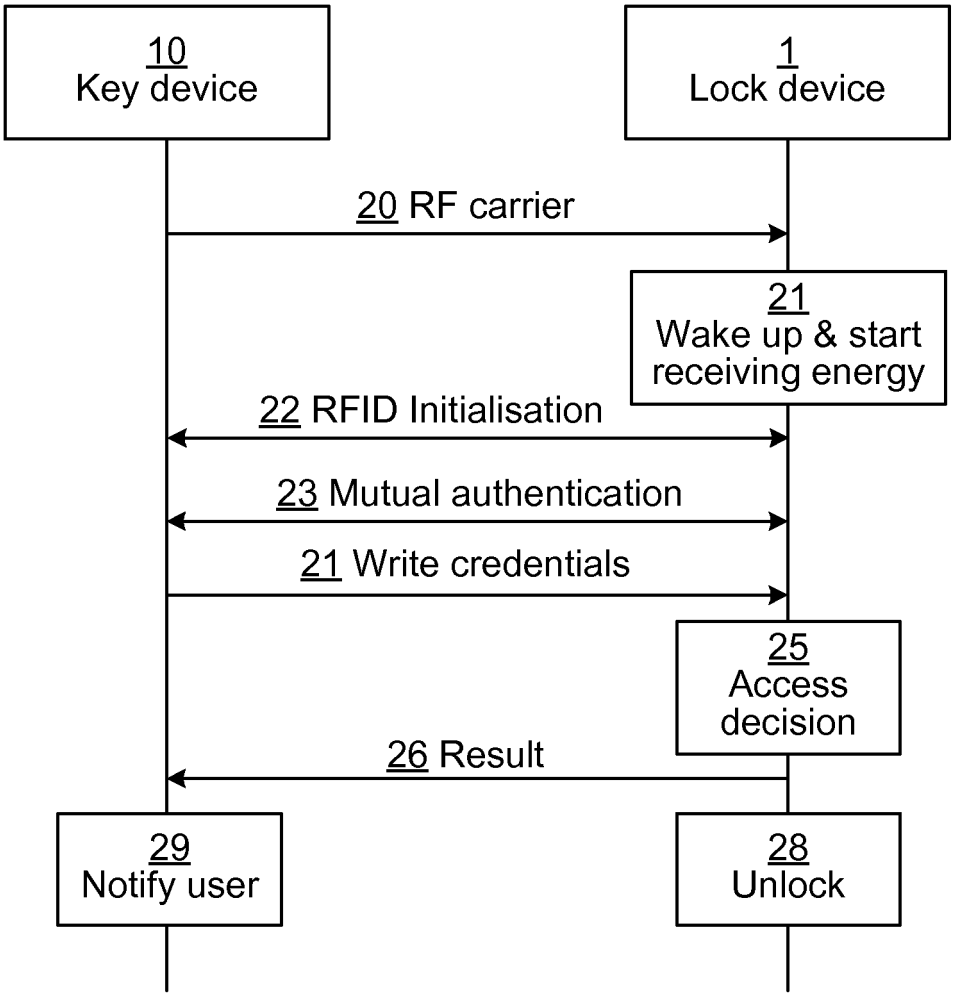

10
Key device
1
Lock device
20 RF carrier
21
Wake up & start
receiving energy
22 RFID Initialisation
23 Mutual authentication
21 Write credentials
25
Access
decision
26 Result
29
Notify user
28
Unlock

Fig. 3A

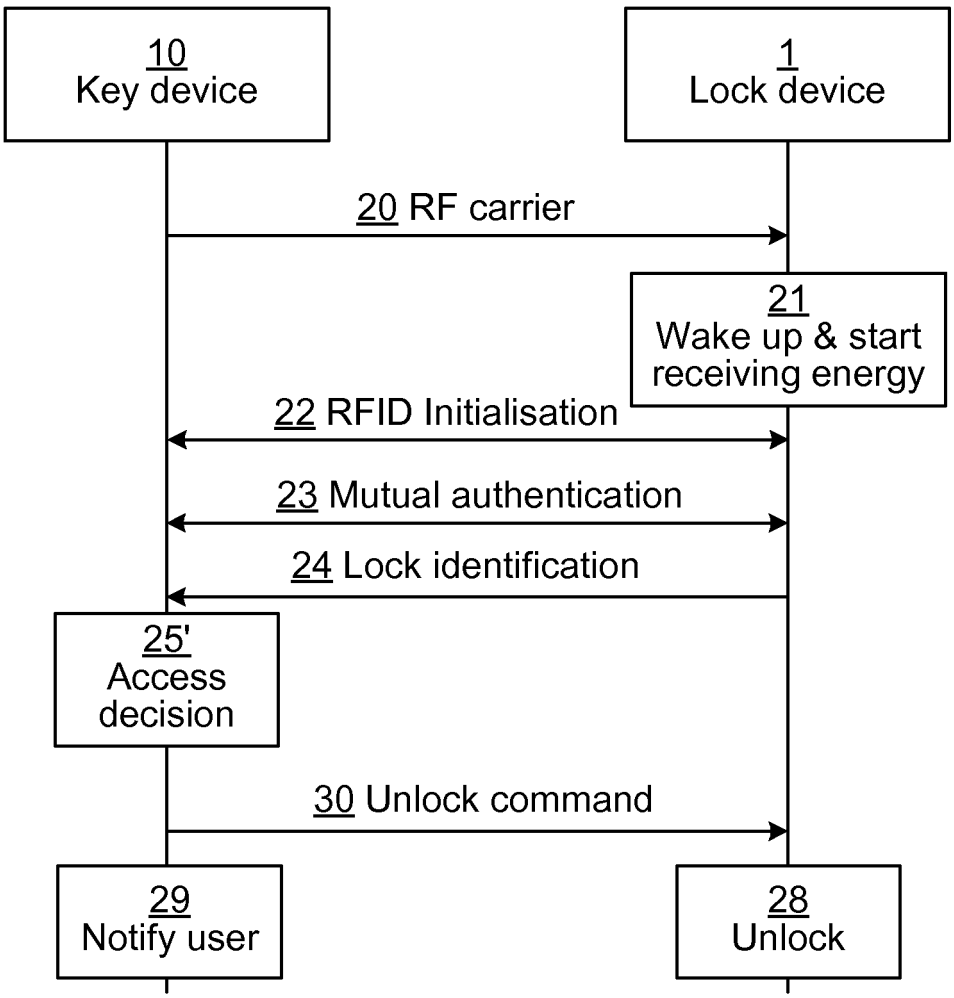

10
Key device
1
Lock device
20 RF carrier
21
Wake up & start
receiving energy
22 RFID Initialisation
23 Mutual authentication
24 Lock identification
25'
Access
decision
30 Unlock command
29
Notify user
28
Unlock

Fig. 3B

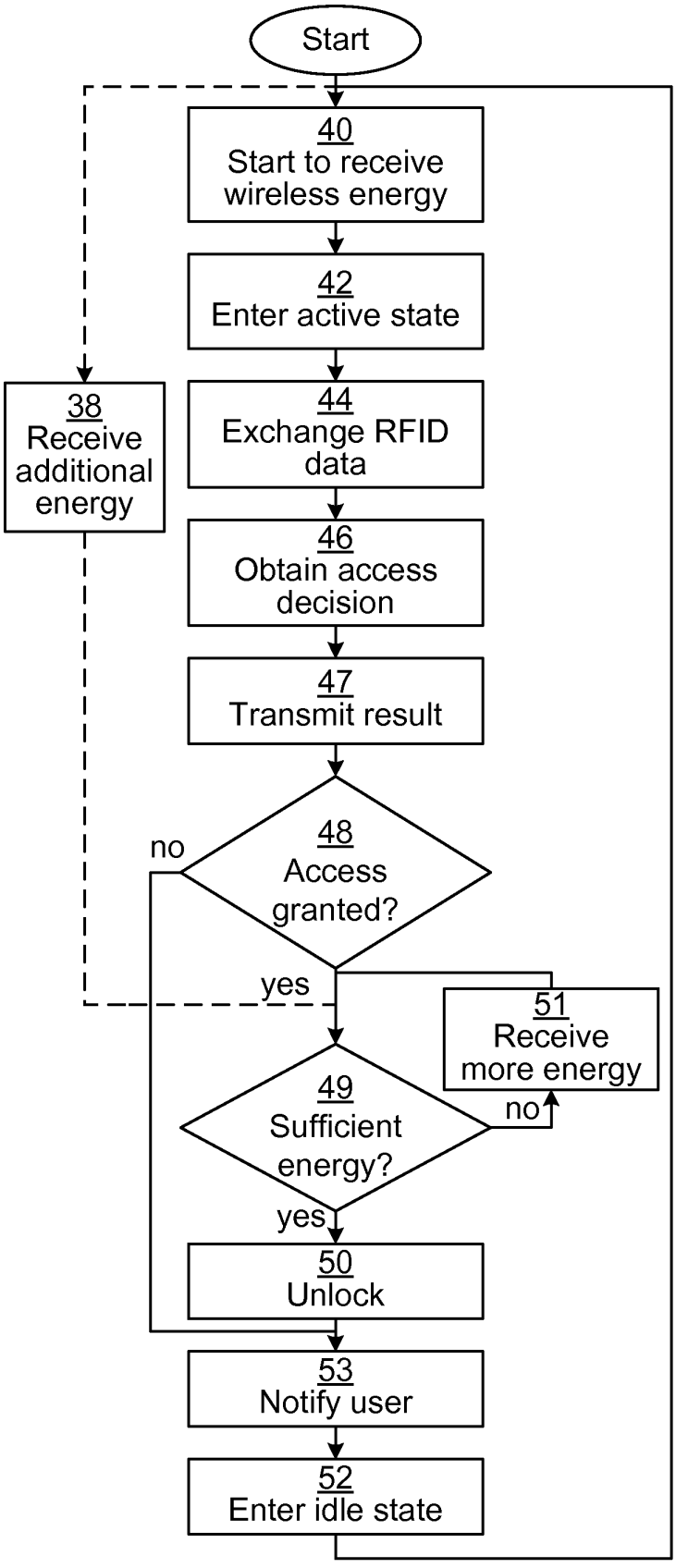


Fig. 4A

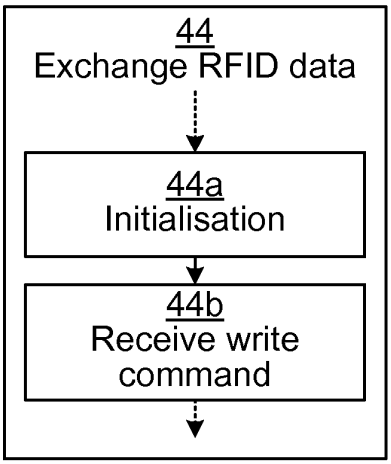


Fig. 4B

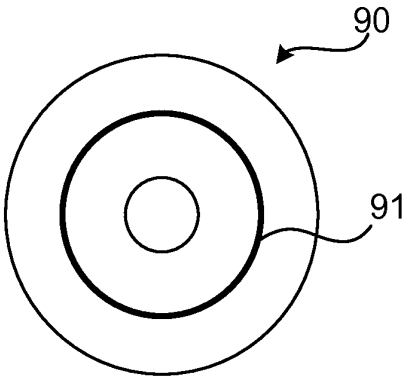


Fig. 5

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 20100085160 A **[0004]**
- US 2002024420 A1 **[0004]**
- EP 2592601 A1 **[0005]**
- EP 2157552 A1 **[0005]**