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

(11) **EP 3 107 073 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
21.12.2016 Bulletin 2016/51

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

(21) Application number: **15172118.0**

(22) Date of filing: **15.06.2015**

(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
Designated Validation States:
MA

(71) Applicant: **Assa Abloy AB**
107 23 Stockholm (SE)

(72) Inventors:
- **Strömberg, Stefan**
  112 45 Stockholm (SE)
- **Gärde, Johan**
  135 53 Tyresö (SE)

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

(54) **INVALIDATION OF AN ELECTRONIC KEY**

(57) It is provided a method for invalidating an electronic key for access to a physical space. The method is performed in an invalidation device and comprises the steps of: receiving a central invalidation command from a central server, the central invalidation command comprising an identifier of an electronic key; discovering a presence of the electronic key over short range radio; and transmitting a local invalidation command to the electronic key.

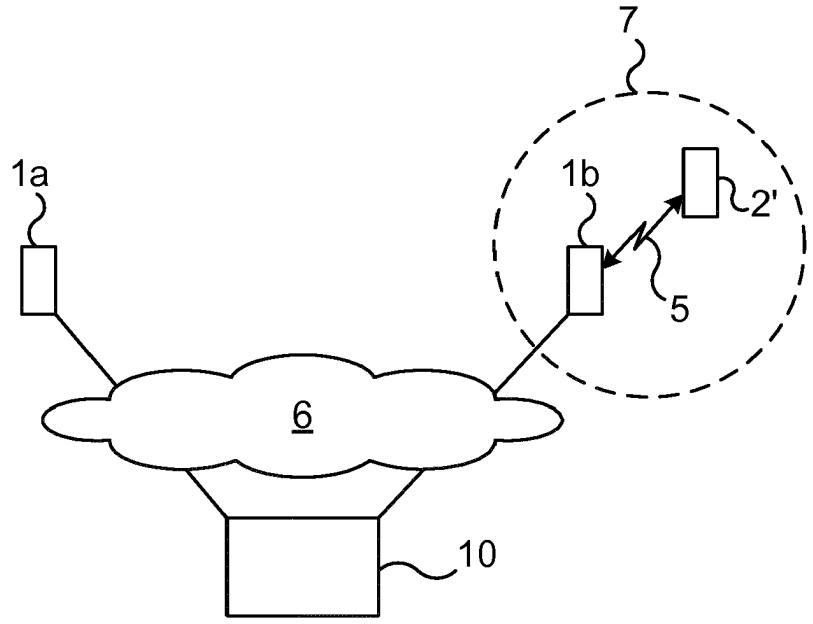

Fig. 2

EP 3 107 073 A1

Description

TECHNICAL FIELD

[0001] The invention relates to a method, an invalidation device, a computer program and a computer program product for invalidating an electronic key, e.g. when the key has been reported lost.

BACKGROUND

[0002] Locks and keys are evolving from the traditional pure mechanical locks. These days, there are wireless interfaces for electronic locks, e.g. by interacting with an electronic key. In some installations, to save power and complexity, the electronic locks are offline without communication ability with a central access control system.

[0003] A major issue is when an electronic key is lost. In such a case, an attacker should be prevented to gain access to closed spaces by using the lost electronic key. When the electronic lock is online, the identity of the electronic key can be added to a black list in the central access control system, and the black list can be sent to the electronic lock. In this way, the electronic lock can block entry for any electronic key on the black list, thus stopping an attacker having found or stolen the lost electronic key.

[0004] However, when the electronic lock is offline, there is no natural way to send a black list to the electronic lock.

SUMMARY

[0005] It is an object to provide a way to invalidate an electronic key which lacks ability to directly communicate with a central server.

[0006] According to a first aspect, it is provided a method for invalidating an electronic key for access to a physical space. The method is performed in an invalidation device and comprises the steps of: receiving a central invalidation command from a central server, the central invalidation command comprising an identifier of an electronic key; discovering a presence of the electronic key over short range radio; and transmitting a local invalidation command to the electronic key.

[0007] The method may further comprise the steps of: receiving a local confirmation message from the electronic key, the local confirmation message indicating a successful invalidation; and transmitting a central confirmation message to the central server, the central confirmation message indicating a successful invalidation.

[0008] The central confirmation message may comprise an indicator of a position of the invalidation device.

[0009] The central invalidation command may comprise a main command and an integrity indicator.

[0010] The integrity indicator may be derived using the main command and a private electronic key.

[0011] The step of discovering may comprise discovering the presence of the electronic key using Bluetooth low energy, BLE.

[0012] The step of receiving a central invalidation command may comprise receiving the central invalidation command over a wide area network.

[0013] According to a second aspect, it is provided an invalidation device for invalidating an electronic key for access to a physical space. The invalidation device comprises: a processor; and a memory storing instructions that, when executed by the processor, cause the invalidation device to: receive a central invalidation command from a central server, the central invalidation command comprising an identifier of an electronic key; discover a presence of the electronic key over short range radio; and transmit a local invalidation command to the electronic key.

[0014] The invalidation device may further comprise instructions that, when executed by the processor, cause the invalidation device to: receive a local confirmation message from the electronic key, the local confirmation message indicating a successful invalidation; and transmit a central confirmation message to the central server, the central confirmation message indicating a successful invalidation.

[0015] The central confirmation message may comprise an indicator of a position of the invalidation device.

[0016] The central invalidation command may comprise a main command and an integrity indicator.

[0017] The invalidation device may form part of a mobile phone.

[0018] The invalidation device may be a device dedicated to the purpose of invalidating electronic keys.

[0019] According to a third aspect, it is provided a computer program for invalidating an electronic key for access to a physical space. The computer program comprises computer program code which, when run on an invalidation device, causes the invalidation device to: receive a central invalidation command from a central server, the central invalidation command comprising an identifier of an electronic key; discover a presence of the electronic key over short range radio; and transmit a local invalidation command to the electronic key.

[0020] According to a fourth aspect, it is provided a computer program product comprising a computer program according to the third aspect and a computer readable means on which the computer program is stored.

[0021] 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

[0022] 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 a situation where a lost electronic key is invalidated using an invalidation device;

Fig 3 is a sequence diagram illustrating communication for invalidation of an electronic key;

Fig 4 is a flow chart illustrating a method for invalidating an electronic key, performed in the invalidation device of Figs 2 and 3;

Fig 5 is a schematic diagram illustrating some components of an invalidation device according to Figs 2 and 3;

Fig 6 is a schematic diagram illustrating an invalidation device provided as part of a mobile phone; and

Fig 7 shows one example of a computer program product comprising computer readable means.

DETAILED DESCRIPTION

[0023] 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.

[0024] Fig 1 is a schematic diagram showing an environment in which embodiments presented herein can be applied. Access to a physical space 16 is restricted by a physical barrier 15 which is selectively unlockable. The physical barrier 15 stands between the restricted physical space 16 and an accessible physical space 14. Note that the accessible physical space 14 can be a restricted physical space in itself, but in relation to this physical barrier 15, the accessible physical space 14 is accessible. The barrier 15 can be a door, gate, hatch, window, drawer, etc. In order to unlock the barrier 15, an access control device 13 is provided. The access control device 13 is connected to a physical lock device 12, which is controllable by the access control device 13 to be set in an unlocked state or locked state. In this embodiment, the access control device 13 is mounted close to the physical lock device 12. The barrier 15 is provided in a surrounding fixed structure, such as a wall or fence.

[0025] The access control device 13 is able to receive and send signals from/to an electronic key 2 over a communication channel 3 which may be a short range wireless interface or a conductive (i.e. galvanic/electric) connection. The electronic key 2 is any suitable device portable by a user and which can be used for authentication over the communication channel 3. The electronic key 2 is typically carried or worn by the user and may be implemented as a physical key, a key fob, wearable device, etc. The short range wireless interface is a radio frequency wireless interface and could e.g. be using Bluetooth, Bluetooth Low Energy (BLE), ZigBee, any of the IEEE 802. 11 standards, any of the IEEE 802.15 standards, wireless USB, etc. Using the communication channel 3, the authenticity of the electronic key 2 can be checked, e.g. using a challenge and response scheme, after which the access control device 13 grants or denies access.

[0026] When access is granted, the access control device 13 sends an unlock signal to the lock device 12, whereby the lock device 12 is set in an unlocked state. In this embodiment, this can e.g. imply a signal over a wire-based communication interface, e.g. using Universal Serial Bus (USB), Ethernet, a serial connection (e.g. RS-485 or RS-232) or even a simple electric connection (e.g. to the lock device 12), or alternatively signal over a wireless communication interface. When the lock device 12 is in an unlocked state, the barrier 15 can be opened and when the lock device 12 is in a locked state, the barrier 15 cannot be opened. In this way, access to a closed space 16 is controlled by the access control device 13. It is to be noted that the access control device 13 and/or the lock device 12 can be mounted in the fixed structure 16 by the physical barrier 15 (as shown) or in the physical barrier 15 itself (not shown). Optionally, the lock device 12 and access control device 13 are combined in one unit. In one embodiment, the lock device (optionally combined with the access control device) is in the form of a padlock or any other suitable implementation.

[0027] The access control device 13 can be implemented as an offline device, without the ability to directly communicate with a central server of an access control system. In this way, the access control device 13 is easier to implement and uses less power. This allows the access control device 13 to be powered for a long time using a battery or by the electronic key. Optionally, energy harvesting of mechanical user actions and/or environmental power (solar power, wind, etc.) can be utilised to prolong the life span of the battery or event to allow the battery to be omitted.

[0028] Fig 2 is a schematic diagram illustrating a situation where an electronic key is invalidated using an invalidation device. A central server 10 of the access control system is responsible for managing keys and locks.

The central server 10 can be accessed by an operator to thereby perform management tasks in the access control system.

[0029] There is a first invalidation device 1a and a second invalidation device 1b. Each one of the first and second invalidation devices are described in more detail below, and can e.g. be implemented as part of a mobile phone or as a dedicated invalidation device. The invalidation devices 1a-b can communicate with an electronic key for invalidation, as explained below, and optionally also for other purposes.

[0030] In this example, a user has lost an electronic key 2' or has had the electronic key 2' stolen. The electronic key 2' then needs to be invalidated to prevent an attacker from gaining access to closed physical spaces, otherwise accessible using the lost electronic key 2'. The central server 10 is made aware of the lost electronic key 2', e.g. by an operator indicating that the electronic key 2' is lost. The central server 10 then sends a central invalidation command to all relevant invalidation devices 1a-b as explained more below.

[0031] The second invalidation device 1b is within range 7 to communicate over a short range radio interface 5 with the lost electronic key 2'. This allows the second invalidation device 1b to communicate with the lost electronic key 2'. In this way, the second invalidation device 1b can send a local invalidation command to the electronic key 2'. The range 7 depends on the type of short range radio which can be used and radio conditions in the vicinity of the electronic key 2'. When communication channel 3 of Fig 1 is wireless, the short range radio interface 5 may be the same as the communication channel 3. However, when the communication channel 3 of Fig 1 is based on a conductive connection, the short range radio interface 5 is not the same as the communication channel 3. The short range radio interface 5 may optionally be used for other purposes, e.g. other maintenance purposes for the electronic key 2'.

[0032] It is to be noted that the first invalidation device 1a is outside the range 7 of the lost electronic key 2', whereby it is unable to invalidate the lost electronic key 2'

[0033] Fig 3 is a sequence diagram illustrating communication for invalidation of an electronic key, e.g. in the environment shown in Fig 2. The sequence is performed to perform invalidation of an electronic key. Hereinafter, the electronic key to be invalidated is referred to as a lost electronic key. However, there may be other reasons for invalidating the electronic key, e.g. the electronic key being stolen or that an employee has ended employment and whose electronic key needs to be invalidated.

[0034] Once the central server 10 is made aware of the lost key, the central server 10 sends a central invalidation command 30 to all relevant invalidation devices 1. This can e.g. be all possible invalidation devices or only invalidation devices in a specific area, e.g. within a specific range from a last known location of the lost electronic key 2'.

[0035] An invalidation device 1 detects the presence 31 of the lost electronic key 2' (e.g. as shown for the second invalidation device 1b of Fig 2). The invalidation device 1 detects that the identity of the electronic key 2' matches the identity of the central invalidation command 30 and thus proceeds with an invalidation. It is to be noted that when an electronic key is detected which does not have an identity matching any received central invalidation command, the invalidation device 1 does not proceed with the invalidation.

[0036] Once the match is confirmed between the lost electronic key 2' and the central invalidation command 30, the invalidation device 1 transmits a local invalidation command 32 to the lost electronic key 2'. Upon receipt of the local invalidation command 32, the lost electronic key 2' makes itself invalid. Optionally, the electronic key 2' verifies the integrity of the invalidation command (as explained below) prior to performing its invalidation procedure. Optionally, the electronic key 2' sends a local confirmation message 33 to the invalidation device 1. The invalidation device 1 can then send a central confirmation message 34 to the central server 10.

[0037] In this way, the central server 10 can initiate an invalidation using all relevant invalidation devices and can optionally be informed of when the invalidation has been successful. Using this method, the lost electronic key 2' can be invalidated even though it has no direct communication link with the central server 10.

[0038] Fig 4 is a flow chart illustrating a method for invalidating an electronic key for access to a physical space. The method is performed in the invalidation device of Figs 2 and 3. The method corresponds to the actions of the invalidation device 1 in Fig 3.

[0039] In a *receive central invalidation command* step 40, a central invalidation command is received from the central server. The central invalidation command comprises an identifier of the electronic key to be invalidated, e.g. of a lost electronic key. The central invalidation command can e.g. be received over a wide area network, such as the Internet.

[0040] Furthermore, the central invalidation command can comprise a main command and an integrity indicator. The integrity can e.g. be derived using the main command and a private electronic key, e.g. using a cryptographic hash function such as SHA-2 (Secure Hash Algorithm 2) or MD-5 (Message Digest algorithm 5).

[0041] In a *discover presence* step 42, a presence of the electronic key to be invalidated is discovered over short range radio. This can e.g. be performed by discovering the presence of the electronic key using BLE. Any other short range radio technology is equally applicable.

[0042] In a *transmit local invalidation command* step 44, a local invalidation command is transmitted to the electronic key to be invalidated. The main command and the integrity indicator of the central invalidation command can form part of the local invalidation command. This allows the electronic key to verify the source of the invalidation, i.e. from the central server. In this way, third par-

ties are prevented from invalidating keys.

[0043] Optionally, the content of the central invalidation command 30 and the local invalidation command 32 is the same. For instance, both can contain an invalidation package which can be encrypted and/or signed for the lost electronic key 2', i.e. using an integrity indicator. This allows the lost electronic key 2' to validate authenticity of the local invalidation command. In such a case, the locating device 1 routes the invalidation package to the lost key 2' and does not (or cannot) examine the contents of the invalidation package.

[0044] In a *receive local confirmation message* step 46, a local confirmation message is received from the electronic key to be invalidated. The local confirmation message indicates a successful invalidation.

[0045] In a *transmit central confirmation message* step 48, a central confirmation message is transmitted to the central server. The central confirmation message indicates a successful invalidation. Optionally, the central confirmation message comprises an indicator of a position (e.g. in form of a longitude and a latitude) of the invalidation device, e.g. obtained using GPS (Global Positioning System) or any other suitable positioning technology. Also, the central confirmation message can comprise an estimated distance (e.g. in metres) to the electronic key from the position of the invalidation device. The distance can be estimated using any suitable method. For instance, the distance can be estimated by measuring received signal strength (i.e. using a received signal strength indicator) and comparing this to transmission power. More specifically, an indicator of the transmission power which is used can be transmitted as part of the message. The receiver can then compare the received signal strength with the power used to transmit it and can thus estimate the distance based on the attenuation of the signal. Alternatively, two-way ranging can be used, measuring the time it takes to transmit a signal and receive its response, which gives a distance indication when divided by two multiplied by the speed of light. The position and optional estimated distance simplifies the retrieval of the electronic key to be able to reprogram and reuse the lost electronic key.

[0046] Fig 5 is a schematic diagram showing some components of the invalidation device of Figs 2 and 3. A processor 60 is provided using any combination of one or more of a suitable central processing unit (CPU), multiprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit etc., capable of executing software instructions 66 stored in a memory 64, which can thus be a computer program product. The processor 60 can be configured to execute the method described with reference to Fig 4 above.

[0047] The memory 64 can be any combination of read and write memory (RAM) and read only memory (ROM). The memory 64 also 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.

[0048] A data memory 66 is also provided for reading and/or storing data during execution of software instructions in the processor 60. The data memory 66 can be any combination of read and write memory (RAM) and read only memory (ROM).

[0049] The invalidation device 1 further comprises an I/O interface 67 for communicating with other external entities. Optionally, the I/O interface 67 also includes a user interface.

[0050] Other components of the invalidation device 1 are omitted in order not to obscure the concepts presented herein.

[0051] Fig 6 is a schematic diagram illustrating an invalidation device 1 provided as part of a mobile phone 4. In such a case, components of the mobile phone 4 can be utilised also by the invalidation device 1.

[0052] In another embodiment, the invalidation device 1 is a device dedicated to the purpose of invalidating electronic keys. In such a case, the dedicated invalidation device 1 can be placed in a location where there is a large chance of discovering a lost electronic key. For instance, the dedicated invalidation device can be placed by the entrance of a building or by a public transport gateway (e.g. underground turnstiles). The dedicated invalidation device 1 does not need to be portable and can thus be connected to a power socket and wireless and/or wire based communication links for communication with the central server. In this way, the dedicated invalidation device 1 can be continuously active.

[0053] Fig 7 shows one example of a computer program product 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 computer program product 64 of Fig 5. 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, such as a removable solid state memory, e.g. a Universal Serial Bus (USB) drive.

[0054] 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 for invalidating an electronic key (2') for access to a physical space (16), the method being performed in an invalidation device (1, 1a, 1b) and

comprising the steps of:

receiving (40) a central invalidation command (30) from a central server (10), the central invalidation command (30) comprising an identifier of an electronic key (2');
discovering (42) a presence of the electronic key (2') over short range radio; and
transmitting (44) a local invalidation command (32) to the electronic key.

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

receiving (46) a local confirmation message (33) from the electronic key (2'), the local confirmation message (33) indicating a successful invalidation; and
transmitting (48) a central confirmation message (34) to the central server, the central confirmation message (34) indicating a successful invalidation.

3. The method according to claim 2, wherein the central confirmation message (34) comprises an indicator of a position of the invalidation device (1, 1a, 1b).

4. The method according to any one of the preceding claims, wherein the central invalidation command (30) comprises a main command and an integrity indicator.

5. The method according to claim 4, wherein the integrity indicator is derived using the main command and a private electronic key.

6. The method according to any one of the preceding claims, wherein the step of discovering (42) comprises discovering the presence of the electronic key (2') using Bluetooth low energy, BLE.

7. The method according to any one of the preceding claims, wherein the step of receiving (40) a central invalidation command comprises receiving the central invalidation command over a wide area network.

8. An invalidation device (1, 1a, 1b) for invalidating an electronic key for access to a physical space (16), the invalidation device (1, 1a, 1b) comprising:

a processor (60); and
a memory (64) storing instructions (66) that, when executed by the processor, cause the invalidation device (1, 1a, 1b) to:

receive a central invalidation command from a central server (10), the central invalidation command (30) comprising an identifier of an electronic key (2');
discover a presence of the electronic key (2') over short range radio; and
transmit a local invalidation command (31) to the electronic key.

9. The invalidation device (1, 1a, 1b) according to claim 8, further comprising instructions (66) that, when executed by the processor, cause the invalidation device (1, 1a, 1b) to:

receive a local confirmation message (33) from the electronic key (2'), the local confirmation message (33) indicating a successful invalidation; and
transmit a central confirmation message (34) to the central server, the central confirmation message (34) indicating a successful invalidation.

10. The invalidation device (1, 1a, 1b) according to claim 9, wherein the central confirmation message (34) comprises an indicator of a position of the invalidation device (1, 1a, 1b).

11. The invalidation device (1, 1a, 1b) according to claim 9 or 10, wherein the central invalidation command (30) comprises a main command and an integrity indicator.

12. The invalidation device (1, 1a, 1b) according to any one of claims 9 to 11, wherein the invalidation device forms part of a mobile phone.

13. The invalidation device (1, 1a, 1b) according to any one of claims 9 to 11, wherein the invalidation device is a device dedicated to the purpose of invalidating electronic keys.

14. A computer program (90) for invalidating an electronic key for access to a physical space (16), the computer program comprising computer program code which, when run on an invalidation device (1, 1a, 1b), causes the invalidation device (1, 1a, 1b) to:

receive a central invalidation command from a central server (10), the central invalidation command (30) comprising an identifier of an electronic key (2');
discover a presence of the electronic key (2') over short range radio; and
transmit a local invalidation command (31) to the electronic key.

15. A computer program product (91) comprising a computer program according to claim 14 and a computer readable means on which the computer program is stored.

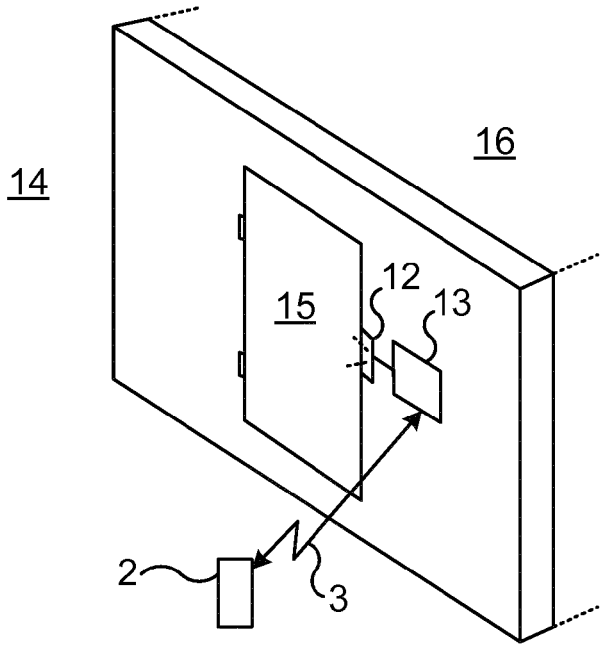

Fig. 1

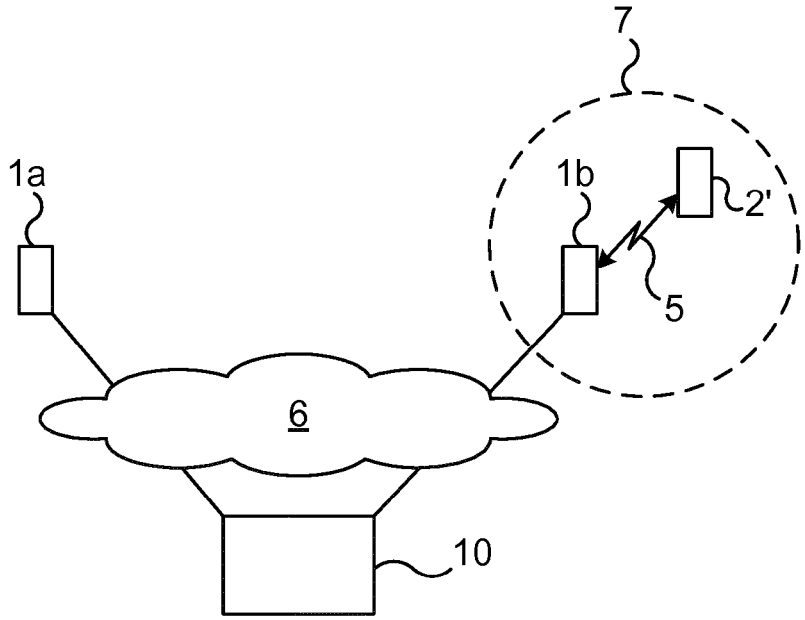

Fig. 2

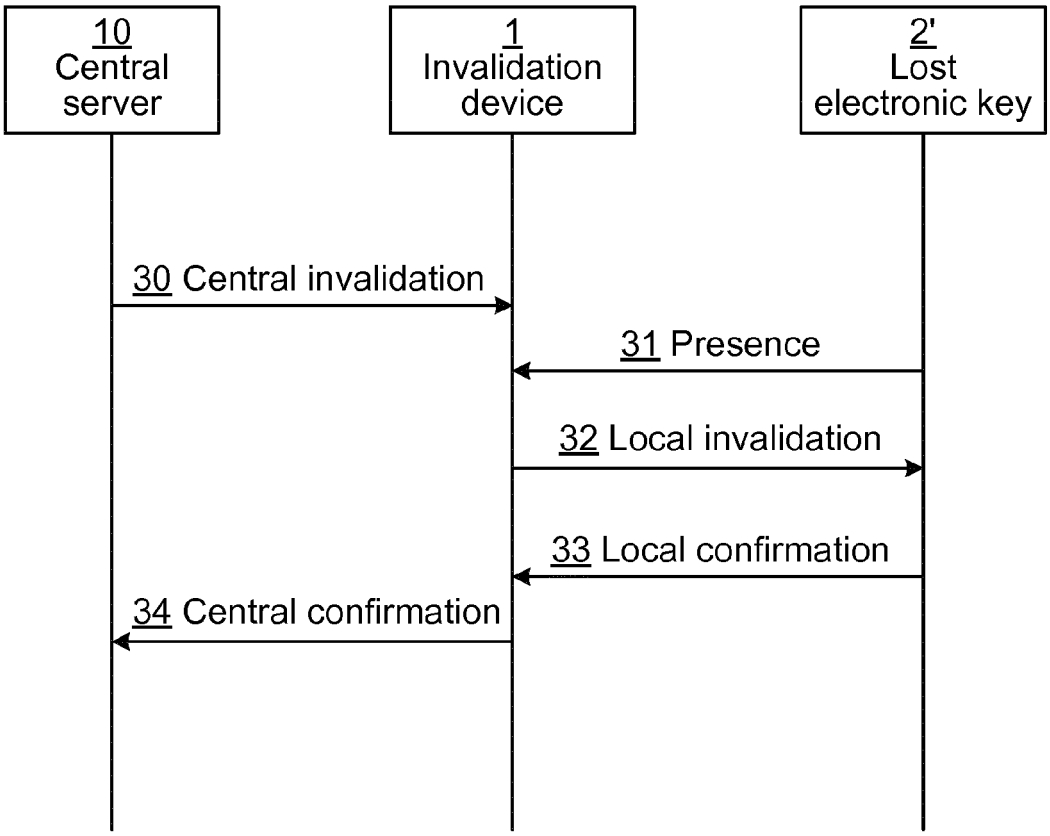
10
Central
server
1
Invalidation
device
2'
Lost
electronic key
30 Central invalidation
31 Presence
32 Local invalidation
33 Local confirmation
34 Central confirmation

Fig. 3

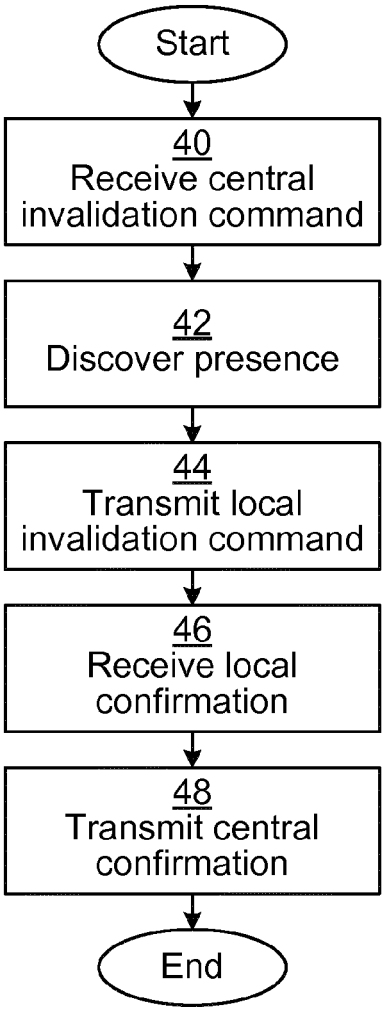

Fig. 4

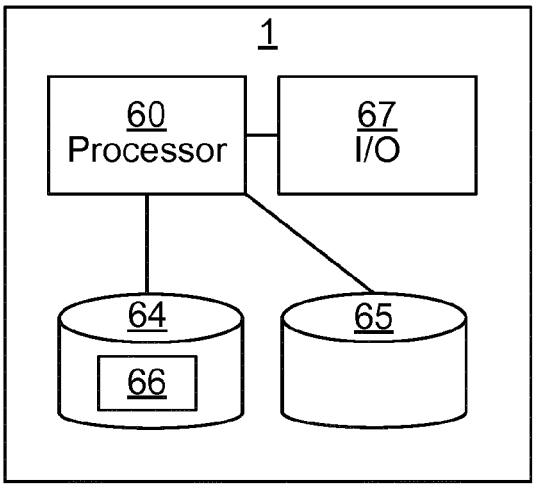

Fig. 5

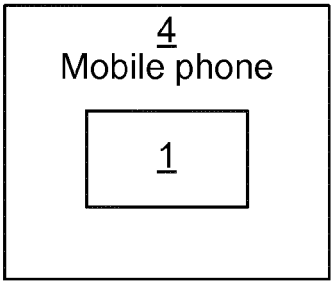

Fig. 6

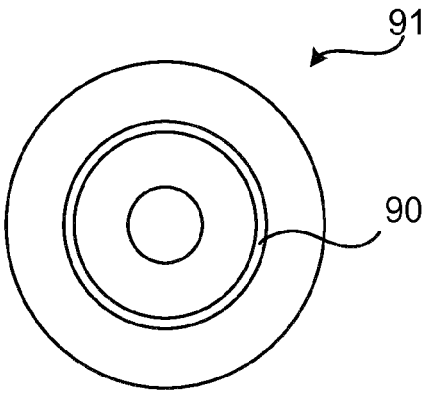

Fig. 7

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 15 17 2118

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 2 821 970 A1 (ASSA ABLOY AB [SE]) 7 January 2015 (2015-01-07) * figures 1,3 * * paragraph [0003] * * paragraph [0026] - paragraph [0031] * * paragraph [0034] * * paragraph [0036] * * paragraph [0045] * * paragraph [0059] * * claims 1,2 *	1-15	INV. G07C9/00
X	EP 2 207 146 A2 (TALLERES ESCORIAZA SA [ES]) 14 July 2010 (2010-07-14) * figure 1 * * paragraph [0007] * * paragraph [0023] * * paragraph [0028] - paragraph [0029] * * paragraph [0031] - paragraph [0034] * * paragraph [0039] *	1-15	
A	EP 1 564 691 A2 (TOKAI RIKA CO LTD [JP]; TOYOTA MOTOR CO LTD [JP]) 17 August 2005 (2005-08-17) * figures 1,4 * * paragraph [0001] * * paragraph [0014] - paragraph [0015] * * paragraph [0019] - paragraph [0020] * * paragraph [0071] - paragraph [0078] * * paragraph [0083] * * paragraph [0089] *	1,2,8,9, 14,15	TECHNICAL FIELDS SEARCHED (IPC) G07C
A	EP 1 568 834 A1 (TOSHIBA KK [JP]) 31 August 2005 (2005-08-31) * paragraph [0001] * * paragraph [0049] - paragraph [0050] * * paragraph [0059] - paragraph [0061] *	1,8,14, 15	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	23 November 2015	Ngandu, William

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 15 17 2118

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2011/140838 A1 (IMEDIO OCANA JUAN [ES]) 16 June 2011 (2011-06-16) * figure 2 * * paragraph [0002] * * paragraph [0005] * * paragraph [0010] * * paragraph [0017] * * paragraph [0027] - paragraph [0040] *	1,2,8,9, 14,15	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	23 November 2015	Ngandu, William

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 15 17 2118

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-11-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2821970 A1	07-01-2015	EP 2821970 A1	07-01-2015
		WO 2015001009 A1	08-01-2015
EP 2207146 A2	14-07-2010	AU 2008306865 A1	09-04-2009
		CA 2711261 A1	09-04-2009
		EP 2207146 A2	14-07-2010
		ES 2323213 A1	08-07-2009
		US 2010223662 A1	02-09-2010
		WO 2009043952 A2	09-04-2009
EP 1564691 A2	17-08-2005	EP 1564691 A2	17-08-2005
		JP 4524122 B2	11-08-2010
		JP 2005226390 A	25-08-2005
		US 2005179519 A1	18-08-2005
EP 1568834 A1	31-08-2005	EP 1568834 A1	31-08-2005
		JP 2004187096 A	02-07-2004
		US 2006143463 A1	29-06-2006
		WO 2004051034 A1	17-06-2004
US 2011140838 A1	16-06-2011	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82