



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
18.05.2016 Bulletin 2016/20

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

(21) Application number: **14193065.1**

(22) Date of filing: **13.11.2014**

(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

- **Gärde, Johan**
135 53 Tyresö (SE)
- **Persson, Johan**
116 61 Stockholm (SE)
- **Cronfalk, Linnea**
116 43 Stockholm (SE)
- **Strömberg, Stefan**
112 45 Stockholm (SE)

(71) Applicant: **ASSA ABLOY AB**
107 23 Stockholm (SE)

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

(72) Inventors:
• **Gustafsson, Niklas**
141 39 Huddinge (SE)

(54) **Proxy key, proxy reader and associated methods**

(57) It is presented a proxy key for providing access to a locked physical space when a physical key and a reader are located at different sites. The proxy key comprises: a physical interface for interacting with the reader; a remote communication interface for electronic commu-

nication with a remote physical key; and a relay module configured to relay electronic communication between the reader and the remote physical key to thereby emulate the remote physical key in communication with the reader. A corresponding proxy reader is also presented.

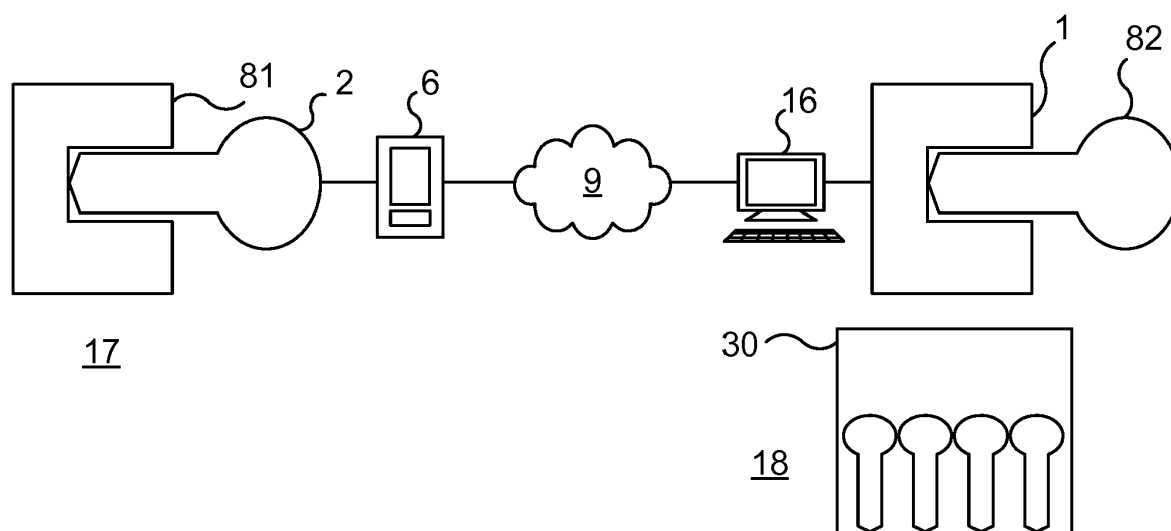


Fig. 3

Description

TECHNICAL FIELD

[0001] The invention relates to a proxy key, a proxy reader and associated methods for providing access to a locked physical space when a physical key and a reader are located at different sites.

BACKGROUND

[0002] Access control systems based on electronic access are provided today using a variety of different topologies. One such solution is shown in Fig 1.

[0003] Access to a physical space 7 is restricted by a physical barrier 8 (e.g. a door or gate) which is selectively unlockable. In order to unlock the barrier 8, a reader 81 is provided. The reader 81 has a physical interface 14 with a corresponding physical interface 4 of a physical key 82 to allow electronic communication between the reader 81 and the physical key 82. In this way, authentication can be performed and the reader 81 can unlock the barrier 8 when access should be granted.

[0004] However, in some instances, the system of Fig 1 becomes overwhelmingly complex due to the need for the physical key 82 to unlock the physical barrier 8. For instance, security companies need to have physical keys to access all buildings they are expected to guard. One way to solve this is that all physical keys are stored in a central location, and if a patrolling guard has to respond to an alarm the guard first has to drive to fetch the physical key, then drive to the location and afterwards return the physical key at the central location. This is a very time consuming process which prolongs the response times and is inefficient. Moreover, there is a significant logistic problem of fetching and returning all relevant physical keys, with the associated risk of losing physical keys.

SUMMARY

[0005] It is an object to provide a convenient way and to provide access to physical spaces using physical keys.

[0006] According to a first aspect, it is presented a proxy key for providing access to a locked physical space when a physical key and a reader are located at different sites. The proxy key comprises: a physical interface for interacting with the reader; a remote communication interface for electronic communication with a remote physical key; and a relay module configured to relay electronic communication between the reader and the remote physical key to thereby emulate the remote physical key in communication with the reader. Using the proxy key, access can be granted using the remote physical key without requiring the physical key to be at the site of the reader. Using this solution, the reader can communicate with the remote physical key as if the reader and physical key were in direct physical contact.

[0007] The physical interface may comprise connectors for galvanic connection with the reader.

tors for galvanic connection with the reader.

[0008] The remote communication interface may comprise an interface for communicating with an intermediary mobile phone to communicate with the remote physical key via a cellular network.

[0009] The physical interface may comprise a mechanical interface to open a lock associated with the reader when access to the locked physical space is granted.

[0010] The relay module may be configured to relay challenge and response communication between the reader and the remote physical key.

[0011] The remote communication interface may be configured to communicate with the remote physical key via a remote proxy reader.

[0012] According to a second aspect, it is presented a method for providing access to a locked physical space when a physical key and a reader are located at different sites. The method is performed in a proxy key and comprises the step of: relaying electronic communication between the reader via a physical interface, and the remote physical key, via a remote communication interface, to thereby emulate the remote physical key in communication with the reader.

[0013] The step of relaying electronic communication may comprise relaying challenge and response communication between the reader and the remote physical key.

[0014] According to a third aspect, it is presented a proxy reader for providing access to a locked physical space when a physical key and a reader are located at different sites. The proxy reader comprises: a physical interface for electronic communication with a physical key; a remote communication interface for electronic communication with the remote reader; and a relay module configured to relay electronic communication between the physical key and the remote reader to thereby emulate the remote reader in communication with the physical key.

[0015] The physical interface may comprise connectors for galvanic connection with the physical key.

[0016] The relay module may be configured to relay challenge and response communication between the physical key and the remote reader.

[0017] The remote communication interface may be configured to communicate with the remote physical reader via a remote proxy key.

[0018] According to a fourth aspect, it is presented a method for providing access to a locked physical space when a physical key and a reader are located at different sites. The method is performed in a proxy reader and comprises the step of: relaying electronic communication between the physical key, via a physical interface, and the remote reader, via a remote communication interface, to thereby emulate the remote reader in communication with the physical key.

[0019] The step of relaying electronic communication may comprise relaying challenge and response communication between the physical key and the remote reader.

[0020] 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

[0021] 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 according to the prior art;

Fig 2 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied;

Fig 3 is a schematic diagram illustrating an alternative environment in which embodiments presented herein can be applied;

Fig 4 is a schematic diagram illustrating an embodiment of a proxy key of Figs 2-3;

Figs 5A-B are schematic diagrams illustrating embodiments of a proxy reader of Figs 2-3;

Fig 6 is a flow chart illustrating a method performed in the proxy key of Figs 2-3 according to one embodiment; and

Fig 7 is a flow chart illustrating a method performed in the proxy reader of Figs 2-3 according to one embodiment.

DETAILED DESCRIPTION

[0022] 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.

[0023] Fig 2 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied. Access to a physical space 7 is restricted by a physical barrier 8 which is selectively unlockable. For

instance, the barrier 8 can be a door, gate, window, etc. In order to unlock the barrier 8, a reader 81 is provided. The reader 81 has a physical interface for interacting with a physical interface of a physical key 82 to allow electronic communication between the reader 81 and the physical key 82. In this way, authentication can be performed and the reader can unlock the barrier 8 when access should be granted.

[0024] However, here the reader 81 and the physical key 82 are at different sites; the reader 81 is at a local site 17 and the physical key 82 is at a central site 18. This prevents the reader 81 from physically interacting with the physical key 82; instead, the reader physically interacts with a proxy key 2. Optionally, the reader 81 is powered by the proxy key 2. The proxy key 2 in turn comprises a remote communication interface 63 for electronic communication with the physical key 82 via a communication network 9 and a proxy reader 1. In this way, the physical key 82 can be located remotely from the reader 81 and still communicate. The communication network 9 is of any suitable type that allows electronic communication between the proxy key 2 and the proxy reader 1 between the different sites 17, 18. For example, the communication network 9 can e.g. be a wide area network such as the Internet, a cellular communication network or a combination of the two, optionally also using local area networks (wired or wireless) as needed.

[0025] The proxy key 2 comprises a relay module 5 which is configured to relay electronic communication between the reader 81 and the remote physical key 82. In this way, the proxy key 2 emulates the remote physical key 82 in communication with the reader 81. In other words, the reader 81 is under the impression that it communicates with the remote physical key 82. In order to perform its relay function, the relay module 5 can comprise software stored in a memory of the proxy key 2 to be executed by a processor of the proxy key 2. Alternatively or additionally, the relay module 5 comprises hardware, such as an application specific integrated circuit (ASIC), field programmable gate array (FPGA), and/or discrete (digital and/or analogue) components, to perform its relay function.

[0026] Analogously, the proxy reader 1 comprises its own relay module 15 which is configured to relay electronic communication between the physical key 82 and the remote reader 81. In this way, the proxy reader 1 emulates the remote reader 81 in communication with the physical key 82. In other words, the physical key 82 is under the impression that it communicates with the remote reader 81. In order to perform its relay function, the relay module 15 can comprise software stored in a memory of the proxy reader 1 to be executed by a processor of the proxy reader 1. Alternatively or additionally, the relay module 15 comprises hardware, such as an application specific integrated circuit (ASIC), field programmable gate array (FPGA), and/or discrete (digital and/or analogue) components, to perform its relay function.

[0027] Communication between the reader 81 and the physical key is here bidirectional.

[0028] Using the system shown in Fig 2, access can be remotely granted using the physical key 82. For example, at the local site 17, a security guard may need access to the physical locked space 7. The guard would then contact the central site 18 and request access. At the central site 18, an operator can then take an appropriate physical key from a secure storage 30 (such as a safe, or a key storage within an otherwise secured area) and insert the appropriate physical key 82 into the proxy reader 1. Once the proxy reader 1 and the proxy key 2 are in communication over the communication network 9, the guard at the local site 17 can insert the proxy key 2 in the reader 81. Using the system, the reader 81 then communicates with the physical key 82 as if the reader 81 and physical key 82 were in direct physical contact.

[0029] The reader 81 can then send a challenge to the physical key 82 which calculates and sends a response to the reader 81 to verify its identity. Analogously, the key 82 can send a challenge to the reader 81 which calculates and sends a response to the physical key 82 to verify its identity. In this way, the barrier is unlocked (under the assumption that the correct physical key 82 is inserted in the proxy reader).

[0030] Using the challenge/response algorithm, the intermediate nodes, such as the proxy key 2, the proxy reader 1 and any nodes in the communication network 9 are not able to sniff and store the communication between the reader 81 and the physical key 82 to later gain access without the presence of the physical key 82 in the proxy reader 1.

[0031] In this way, the central location can hold all keys to all buildings required for the security company. This is logistically efficient where the guard in the field never needs to retrieve a physical key. Instead, the central operator would insert the required key on demand in the proxy reader for the guard. Moreover, the risk of losing keys for the customer is essentially eliminated since all keys can be kept in central secure storage.

[0032] Another use case is if a handyman needs access to a house when the owner is at work. The local site is then the house and the central site 18 is work. The owner could then insert the physical key 82 for the house in the proxy reader which is in communication with the proxy key 2 of the handyman. In this way, the owner can selectively give access to the house to the handyman as necessary.

[0033] Fig 3 is a schematic diagram illustrating an alternative environment in which embodiments presented herein can be applied. In this embodiment, an example of a communication path between the proxy key 2 and the proxy reader 11 is shown in more detail. Specifically, the proxy key 2 communicates with a mobile phone 6 (or tablet computer or laptop computer) at the local site 17, which in turn communicates with an electronic device 16, such as a computer, a mobile phone, a tablet computer, etc., at the central site 18. The electronic device 16, in

turn, communicates with the proxy reader 1. The proxy key 2 thus comprises an interface for communicating with an intermediary mobile phone to communicate with the remote physical key via a cellular network.

[0034] The communication between the proxy key 2 and the mobile phone 6, as well as the communication between the proxy reader 1 and the electronic device 15, can occur using any suitable current or future communication protocol. For instance, the communication can be wire-based (e.g. using Universal Serial Bus, USB) to reduce or even remove the need for any battery in the proxy key. Alternatively or additionally, the communication can be wireless (e.g. using Bluetooth, WiFi, NFC (Near Field Communication), etc.).

[0035] Fig 4 is a schematic diagram illustrating an embodiment of a proxy key 2 of Figs 2-3. 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 stored in a memory 65, which can thus be a computer program product. For instance, when the relay module 5 comprises software elements, parts or all of the relay module 5 are implemented as software instructions stored in the memory 65. The processor 60 can be configured to execute the method described with reference to Fig 6 below.

[0036] The memory 65 can be any combination of read and write memory (RAM) and read only memory (ROM). The memory 65 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.

[0037] 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).

[0038] A power supply 68 provides power to the components of the proxy key 2. The power supply can be implemented using a battery (rechargeable and/or disposable) or using a wired connection to a mobile phone (or tablet computer or laptop computer).

[0039] The remote communication interface 63 is provided for communicating with remote external entities, such as the proxy reader.

[0040] The proxy key 2 comprises physical interface 4 for interacting with a reader. The physical interface 4 comprises a connector 22 and optionally a mechanical interface 23 (such as a blade), which are electrically insulated from each other by an insulator 24. Optionally, two (or more) dedicated connectors can be provided for communication with the reader.

[0041] The physical interface 4 provides a dual terminal connection between the proxy key 2 and a reader 81 when the proxy key 2 is inserted in the socket of the reader 81. The dual terminal connection is used for electronic communication between the proxy key 2 and the

reader 81 and optionally for powering the reader 82 by transferring electric power from the power supply 68 of the proxy key 2 to the reader 81.

[0042] The connection using the connectors 22, 23 can be galvanic or inductive. In the case of an inductive connection, the connectors do not need to physically connect to the reader but be physically positioned to allow communication over the inductive interface.

[0043] Figs 5A-B are schematic diagrams illustrating embodiments of a proxy reader of Figs 2-3. Looking first to Fig 5A, it is illustrated an embodiment where the proxy reader 1 relies on the electronic device 16 for software functions.

[0044] Here, the electronic device 16 comprises a processor 70' of 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 stored in a memory 75', which can thus be a computer program product.

[0045] The memory 75' can be any combination of read and write memory (RAM) and read only memory (ROM). The memory 75' 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.

[0046] A data memory 76' is also provided for reading and/or storing data during execution of software instructions in the processor 70'. The data memory 76' can be any combination of read and write memory (RAM) and read only memory (ROM).

[0047] In the proxy reader 1, the remote communication interface 73 is provided for communicating with remote external entities, such as the proxy key (via the electronic device 16 and communication network). In this embodiment, the remote communication interface 73 comprises the relay module 15, relaying communication between the proxy reader 1 and the proxy key.

[0048] The proxy reader 1 comprises physical interface 14 for interacting with a physical key. The physical interface 14 comprises a first connector 32 and a second connector 33, which are electrically insulated from each other.

[0049] The physical interface 14 thus provides a dual terminal connection between the proxy reader 1 and a physical key when the physical key is inserted in the socket of the proxy reader 1. The dual terminal connection is used for electronic communication between the proxy reader 1 and the physical key and optionally for powering the proxy reader 1 by receiving electric power from the physical key.

[0050] The connection using the connectors 32, 33 can be galvanic or inductive. In the case of an inductive connection, the connectors do not need to physically connect with the physical key, but be physically positioned to allow communication over the inductive interface.

[0051] Using the embodiment of Fig 5A, the proxy reader 1 can be made very simple, making it cost-effective

and robust.

[0052] In the embodiment shown in Fig 5B, the proxy reader 1 comprises its own processor 70, memory 75 and data memory 76. Hence, when the relay module 15 comprises software elements, a part of or all of the relay module 15 is implemented as software instructions stored in the memory 75. The processor 70 can be configured to execute the method described with reference to Fig 7 below. The remote communication interface 73 optionally includes all components necessary to connect to the communication network, e.g. using a cellular network connection or a WiFi connection.

[0053] Using the embodiment of Fig 5B, the proxy reader can be made self reliant, whereby the electronic device 16 is made redundant.

[0054] Fig 6 is a flow chart illustrating a method for providing access to a locked physical space when a physical key and a reader are located at different sites. The method is performed in the proxy key 2 of Figs 2-3 according to one embodiment.

[0055] In a relay communication step 40, the proxy key 2 relays electronic communication between the reader and the remote physical key. The relaying of communication occurs via the physical interface and the remote communication interface, to thereby emulate the remote physical key in communication with the reader.

[0056] Fig 7 is a flow chart illustrating a method for providing access to a locked physical space when a physical key and a reader are located at different sites. The method is performed in the proxy reader 1 of Figs 2-3 according to one embodiment.

[0057] In a relay communication step 50, the proxy reader 1 relays electronic communication between the physical key and the remote reader. The relaying of communication occurs via a physical interface and the remote communication interface, to thereby emulate the remote reader in communication with the physical key.

[0058] 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 proxy key (2) for providing access to a locked physical space (7) when a physical key (82) and a reader (81) are located at different sites (17, 18), the proxy key comprising:

a physical interface (4) for interacting with the reader (81);

a remote communication interface (63) for electronic communication with a remote physical key (82); and

a relay module (5) configured to relay electronic

- communication between the reader (81) and the remote physical key (82) to thereby emulate the remote physical key (82) in communication with the reader (81).
2. The proxy key (2) according to claim 1, wherein the physical interface (4) comprises connectors for galvanic connection with the reader (81).
 3. The proxy key (2) according to claim 1 or 2, wherein the remote communication interface (63) comprises an interface for communicating with an intermediary mobile phone to communicate with the remote physical key (82) via a cellular network.
 4. The proxy key (2) according to any one of the preceding claims, wherein the physical interface (4) comprises a mechanical interface to open a lock associated with the reader when access to the locked physical space (7) is granted.
 5. The proxy key (2) according to any one of the preceding claims, wherein the relay module (5) is configured to relay challenge and response communication between the reader (81) and the remote physical key (82).
 6. The proxy key (2) according to any one of the preceding claims, wherein the remote communication interface (63) is configured to communicate with the remote physical key (82) via a remote proxy reader (1).
 7. A method for providing access to a locked physical space (7) when a physical key (82) and a reader (81) are located at different sites (17, 18), the method being performed in a proxy key (2) and comprising the step of:
 - relaying (40) electronic communication between the reader (81) via a physical interface (4), and the remote physical key (82), via a remote communication interface (63), to thereby emulate the remote physical key (82) in communication with the reader (81).
 8. The method according to claim 7, wherein the step of relaying (40) electronic communication comprises relaying challenge and response communication between the reader (81) and the remote physical key (82).
 9. A proxy reader (1) for providing access to a locked physical space (7) when a physical key (82) and a reader (81) are located at different sites (17, 18), the proxy reader comprising:
 - a physical interface (14) for electronic communication with a physical key (82);
 - a remote communication interface (73) for electronic communication with the remote reader (81); and
 - a relay module (15) configured to relay electronic communication between the physical key (82) and the remote reader (81) to thereby emulate the remote reader (81) in communication with the physical key (82).
 10. The proxy reader (1) according to claim 9, wherein the physical interface (14) comprises connectors for galvanic connection with the physical key (82).
 11. The proxy reader (1) according to claim 9 or 10, wherein the relay module is configured to relay challenge and response communication between the physical key (82) and the remote reader (81).
 12. The proxy reader (1) according to any one of claims 9 to 11, wherein the remote communication interface (73) is configured to communicate with the remote physical reader (81) via a remote proxy key (2).
 13. A method for providing access to a locked physical space (7) when a physical key (82) and a reader (81) are located at different sites (17, 18), the method being performed in a proxy reader (1) and comprising the step of:
 - relaying (50) electronic communication between the physical key (82), via a physical interface (14), and the remote reader (81), via a remote communication interface (73), to thereby emulate the remote reader (81) in communication with the physical key (82).
 14. The method according to claim 13, wherein the step of relaying (50) electronic communication comprises relaying challenge and response communication between the physical key (82) and the remote reader (81).

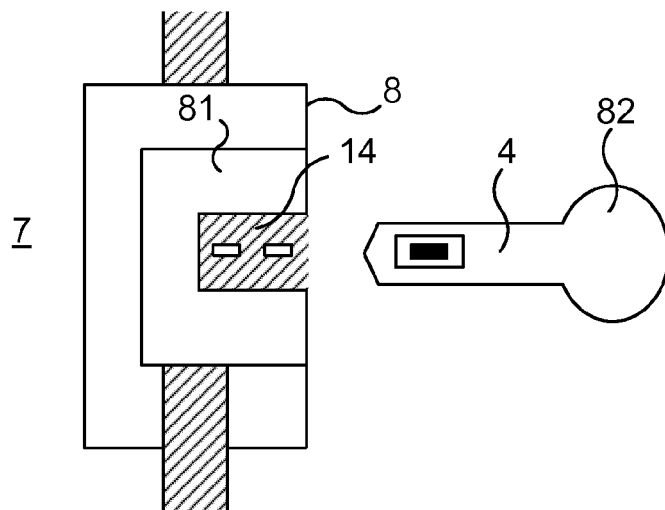


Fig. 1

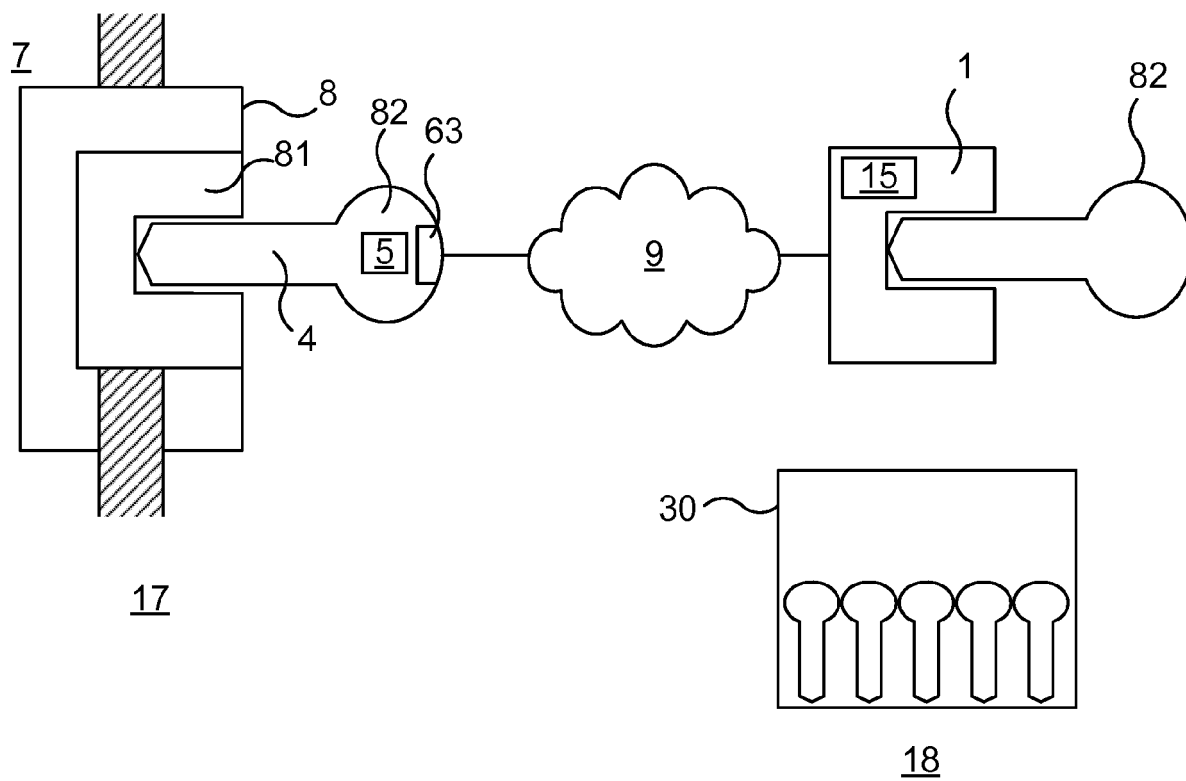


Fig. 2

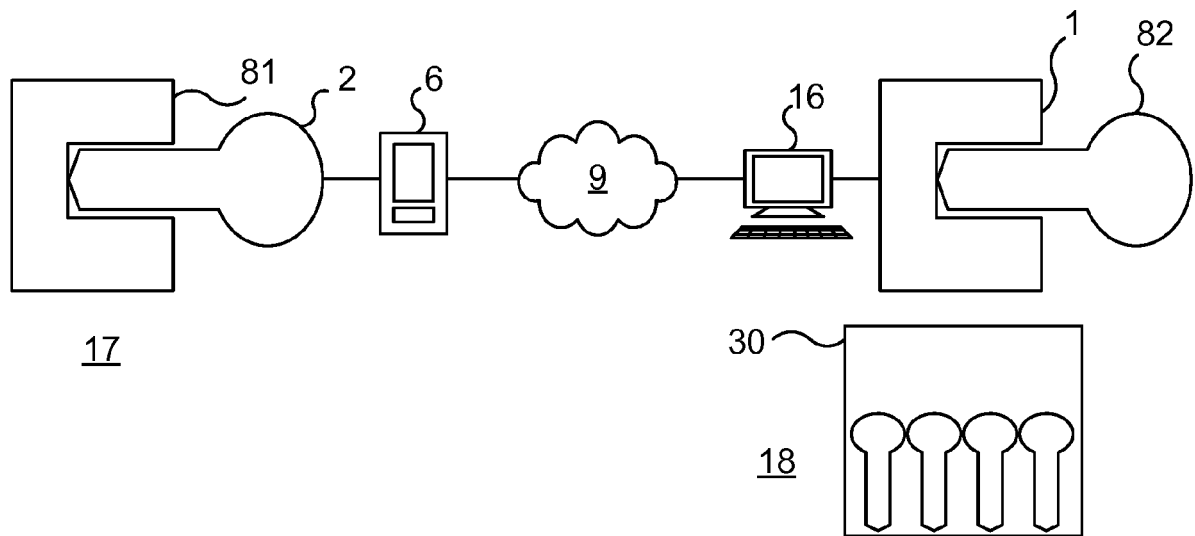


Fig. 3

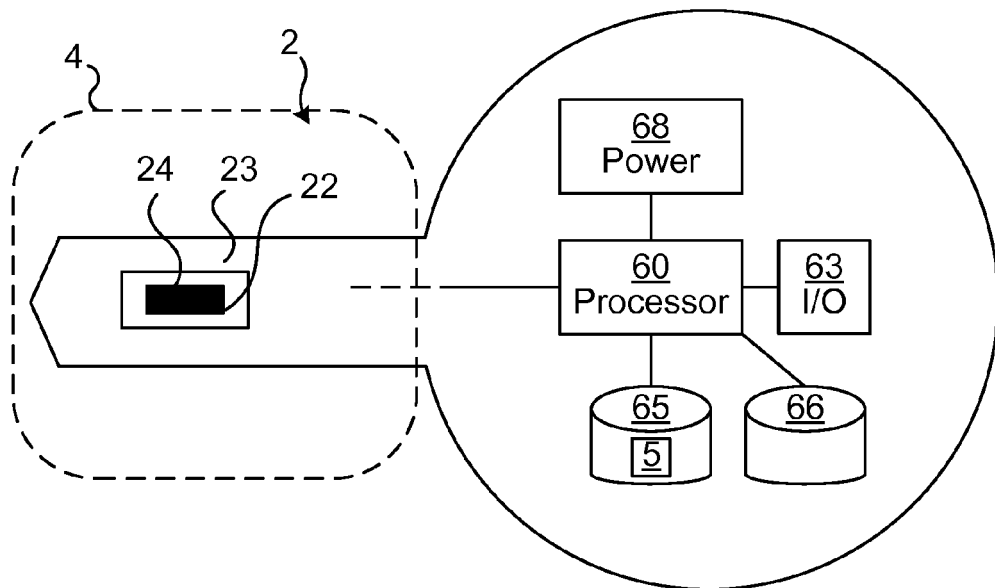


Fig. 4

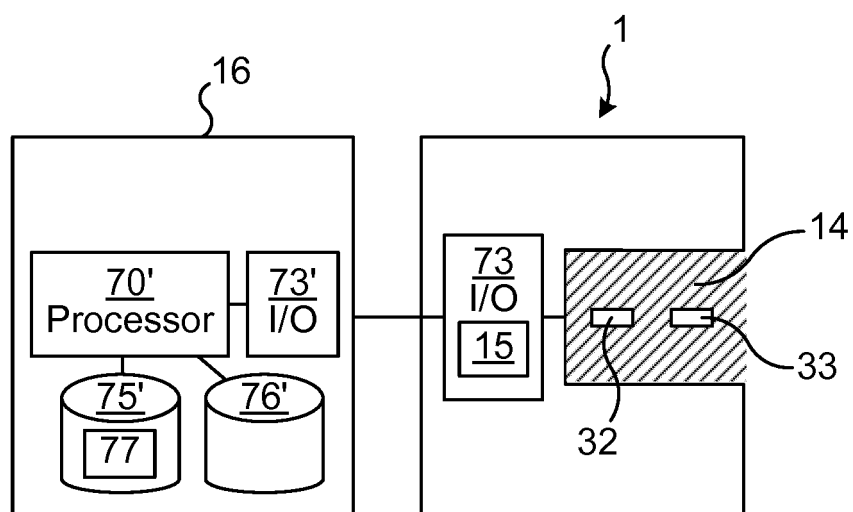


Fig. 5A

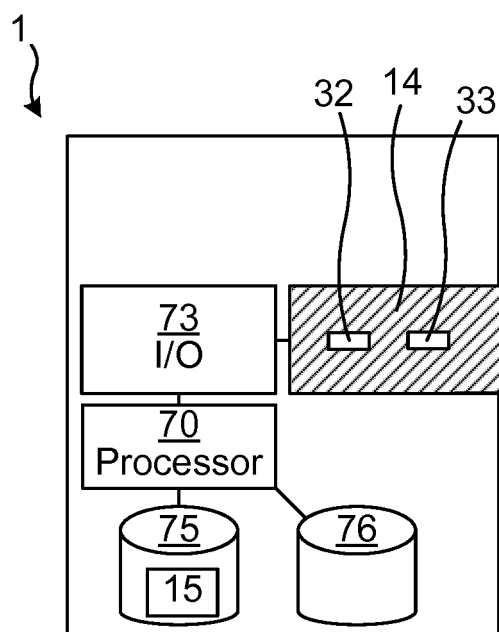


Fig. 5B

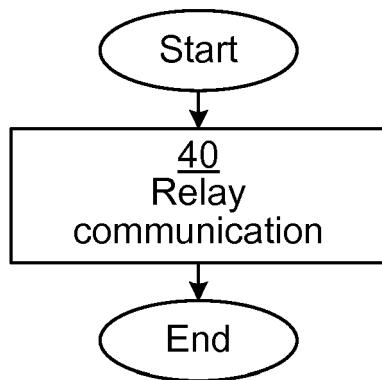


Fig. 6

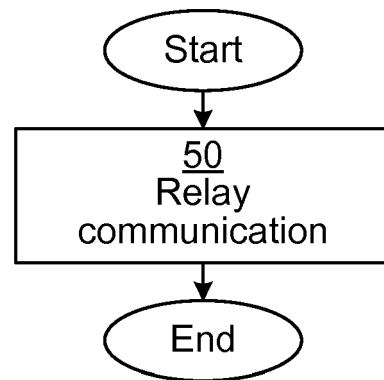


Fig. 7



EUROPEAN SEARCH REPORT

 Application Number
 EP 14 19 3065

5

10

15

20

25

30

35

40

45

50

55

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	GB 2 340 642 A (ROVER GROUP [GB] ROVER GROUP [GB]; BAYERISCHE MOTOREN WERKE AG [DE]) 23 February 2000 (2000-02-23) * abstract * * page 2, line 7 - page 5, line 7 * * page 5, line 14 - page 9, line 18 * -----	1-14	INV. G07C9/00
Y	EP 0 282 339 A2 (SECURITY SERVICES PLC [GB]) 14 September 1988 (1988-09-14) * abstract * * column 1, line 1 - column 2, line 52 * * column 2, line 62 - column 4, line 65 * -----	1-14	
Y	EP 2 573 738 A1 (DELPHI TECH INC [US]) 27 March 2013 (2013-03-27) * abstract * * paragraph [0004] - paragraph [0015] * * paragraph [0026] - paragraph [0040] * -----	1-14	
A	US 2006/082434 A1 (BREY THOMAS A [US]) 20 April 2006 (2006-04-20) * abstract * * paragraph [0009] - paragraph [0016] * -----	1-14	TECHNICAL FIELDS SEARCHED (IPC) G07C
A	DE 197 53 401 A1 (MARQUARDT GMBH [DE]) 10 June 1999 (1999-06-10) * abstract * * page 1, line 1 - page 2, line 52 * * page 4, line 29 - page 6, line 35 * -----	1-14	
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 27 May 2015	Examiner Teutloff, Ivo
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 03.02 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 14 19 3065

5 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.

27-05-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2340642 A	23-02-2000	NONE	
EP 0282339 A2	14-09-1988	EP 0282339 A2 GB 2202354 A US 4926665 A	14-09-1988 21-09-1988 22-05-1990
EP 2573738 A1	27-03-2013	CN 103010153 A EP 2573738 A1 US 2013069761 A1	03-04-2013 27-03-2013 21-03-2013
US 2006082434 A1	20-04-2006	NONE	
DE 19753401 A1	10-06-1999	NONE	