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

(11) EP 3 062 294 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.08.2016 Bulletin 2016/35

(51) Int Cl.:
G07C 9/00 $^{(2006.01)}$

(21) Application number: **15156996.9**

(22) Date of filing: **27.02.2015**

(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

(71) Applicant: **Kibix AG**
9470 Buchs (CH)

(72) Inventor: **Rietschel, Johannes**
8600 Dübendorf (CH)

(74) Representative: **Bremi, Tobias Hans**
Isler & Pedrazzini AG
Postfach 1772
8027 Zürich (CH)

(54) Method and devices for upgrading an existing access control system

(57) Method for upgrading an existing access control system. The existing access control system comprises at least one access point which is controlled by a reader unit (1) for reading authorization information from a portable token (6) and a corresponding unlocking device (3), the reader unit (1) is in wired connection via at least one 1st control line (4) communicatively connected to an access controller (2), and said access controller (2) is in wired connection via at least one 2nd control line (5) communicatively connected to said unlocking device (3). The said access controller (2) controls the locking state of said unlocking device (3) via said 2nd control line (5) by verifying identification information transmitted via 1st control line (4) from said reader unit (1). The upgrading method comprises the steps of interposing into the at least one 1st control line (4) an interception unit (9), said interception unit (9) adapted to and allowing for receiving and, if needed after temporarily withholding said identification information from said reader unit (1), only transmitting it to the access control unit (2) once said interception unit (9) has verified permission to access independently via a 2nd communication with a holder of said token (6).

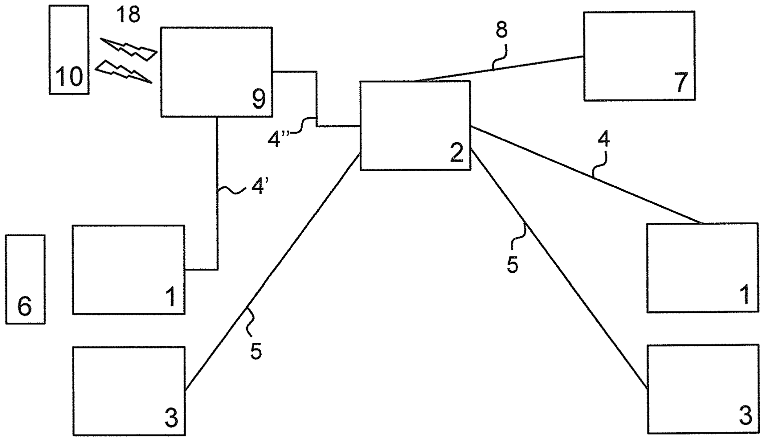

FIG. 2

EP 3 062 294 A1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The present invention relates to a method for upgrading an existing access control system for increasing access control security and functionality. Furthermore it relates to a method of operating such an upgraded access control system, to a correspondingly upgraded access control system and to an interception unit for use in such an access control system or an upgrade of such an access control system.

PRIOR ART

[0002] Many buildings requiring controlled access are equipped with access control systems which do not provide for all the functionality as well as all the security levels as would be desired, however installing a completely new access control system is too costly or even technically impossible.

SUMMARY OF THE INVENTION

[0003] Therefore the need exists for easy upgrade possibilities for existing access control systems as well as for methods of operating such upgraded access control systems and elements for upgrading such access control systems.

[0004] The present invention proposes such a method for upgrading an existing access control system, a method for operating such an upgraded access control system, as well as elements for such an upgraded access control systems or elements to be used for the upgrade of such access control systems.

[0005] More specifically, the present invention in a 1st aspect thereof relates to a method for upgrading an existing access control system. Such an existing access control system comprises at least one access point (e.g. a door) which is controlled by a reader unit for reading authorization information from a portable token (a batch, a key or the like) and a corresponding unlocking device (typically a physical device physically locking and unlocking the door). The reader unit is in wired connection via at least one 1st control line (a physical wired line, can be a single line, two or more wired lines) communicatively connected to an access controller, and said access controller is in wired connection via at least one 2nd control line (again a physical wired line, can be a single line, two or more wired lines) communicatively connected to said unlocking device, and said access controller controls the locking state of said unlocking device via said 2nd control line by verifying identification information transmitted via 1st control line from said reader unit. Typically such an access control system comprises one central access control unit and, depending on the access points, a corresponding number of reader units and unlocking units, but it is also possible that for each access point in individual reader unit, access unit and unlocking unit are pre-existing, in both cases the proposed upgrade is possible.

[0006] Such a pre-existing access control system, which typically works with data exchange by the 1st control line on the basis of serial, Wiegand or clock and data, the proposal is to upgrade as follows:

> the method comprises the steps of interposing into the at least one 1st control line an interception unit. Said interception unit is adapted to and allowing for receiving and, if needed after temporarily withholding said identification information received from said reader unit, and only transmitting it to the access control unit once said interception unit has verified permission to access independently via a 2nd communication with a holder of said token (i.e. a person carrying the token).

[0007] In other words the upgrade is realized in that a 2nd identification retrieval mechanism is embedded into the pre-existing access control system. This identification information retrieval mechanism is brought in by an additional interception unit. This interception unit, which can simply be inserted into the communication channel between the reader and the access controller, has the functionality of independently establishing a connection to either the same or another token of the holder desiring to access through the access point. Preferably the idea is to have as a 1st token the batch of the holder, and the 2nd token of the holder is the personal mobile handheld device. The interception unit is adapted for establishing a communication link to the personal mobile handheld device in order to retrieve information there from to allow for increased security access granting. Due to the fact that nowadays basically everyone carries a mobile handheld device with a huge range of functionality, which actually can be used for holder identification information purposes, this is probably the most simple upgrade possibility for an access control system. The idea is to use the functionality of the mobile handheld device for identification purposes, in other words only an app needs to be installed on the mobile handheld device (tablet, smart phone, mobile phone, etc.) and then the interception device uses a communication channel available (Bluetooth, WLAN, smart Bluetooth) for establishing a connection to the mobile handheld device. So basically the function of the interception device is to intercept the data transfer between the reader and the access controller until, after having established a connection between the interception device and the mobile handheld device and after having established further identification information by using the mobile handheld device, only forwarding the data transfer further to the access controller once identification has been verified. For further increased security it's possible to use the telecommunication functionalities of the mobile handheld devices of the holders in order to further verify the input information (pin, fingerprint, etc.) input by the holder into the mobile handheld device by contacting a corresponding central authority (e.g. via cloud-based). Preferably all this data communication is encrypted, and it is possible to basically store the token information using the interception unit and the handheld device the 1st time, on the mobile handheld device so as to avoid to have to use the token (key, batch) each time an access point needs to be released and passed.

[0008] According to a 1st preferred embodiment of this method, the interception unit comprises at least one radiofrequency interface for establishing a wireless communication channel between said interception unit and a mobile handheld devic of said holder, and said verification by the interception unit involves retrieving information about access permission of said holder via said mobile handheld device.

[0009] Preferably the radiofrequency interface is a wireless local area network (WLAN) interface, a Bluetooth interface, Bluetooth smart, preferably a low-energy Bluetooth or Bluetooth smart interface.

[0010] According to yet another preferred embodiment, retrieving information about access permission of said holder via said mobile handheld device includes the steps of identifying said holder and/or said mobile handheld device by means of input given by said holder into said mobile handheld device, and/or by means of readout of an unambiguous identification information from said mobile handheld device. Such identification information can for example be input into the mobile handheld device in a 1st contact with the upgraded access control system, and can be the identification information associated with the personal token of the holder of the personal mobile handheld device, see further description below. Preferably, said input is at least one of: a pin code, a biometric information collected by said mobile device, such as fingerprint, picture, in particular face and/or skin picture, eyepicture, positional information, or a combination thereof.

[0011] According to a further preferred embodiment further increasing the security level of the upgrade retrieving information about access permission of said holder via said mobile handheld device includes the step of establishing an external wireless communication using a WLAN or telecommunication channel by said mobile handheld device to an overall control authority (i.e. the central data control unit, e.g. established cloud-based) which verifies access permission independently and transmits, provided access granted, a corresponding permission back to said mobile handheld device and directly and/or in directly via said radiofrequency interface to the interception unit.

[0012] The interception unit, after having verified permission to access, preferentially transmits said identification information from said reader unit identical to the one as initially received from said reader unit. However it's also possible to transmit specifically modified data to the access controller.

[0013] Verifying permission to access is possible either by the interception unit autonomously and/or by an overall control authority via communication therewith by means of the mobile handheld device and may involve authorizing at least one of: access time, access frequency, access number, access permission status of holder, trust status of holder, compliance of data about or from holder retrieved by said mobile handheld device with an internal database, or a combination thereof.

[0014] According to yet another preferred embodiment, the radio frequency interface automatically establishes a radiofrequency connection to said mobile handheld device once it is in sufficient proximity to the interception unit , and, if needed, once connection established, increases the power level from low level stand by to high-level.

[0015] The interception unit can be provided with means for determining the distance between the interception unit and the mobile handheld device, and this distance can also be taken into account as a parameter for granting access.

[0016] Further preferably, the interception unit comprises an independent CPU, RAM, ROM, volatile and/or non-volatile data storage elements, an encryption unit, standalone and/or grid based power supply. If need be also a real-time clock element, and optionally a secondary CPU, RAM/ROM, data storage element can be present.

[0017] Although the interception unit can be put into the same housing as the reader, and the access controller, it's however also possible to put the interception unit only into a housing of the reader or into a separate housing.

[0018] According to yet another preferred embodiment, the data transmitted via said 1st communication line is serial, Wiegand (3 wires, one common ground and D0 and D1) or clock and data. The 2nd communication line is often just a power line.

[0019] Further preferably communication via at least one of said 1st control line, said 2nd control line, between the interception unit and the mobile handheld device, between the mobile handheld device and the overall control, is encrypted.

[0020] Once authorized by at least one of token or handheld mobile device, independent verification by overall control or a combination thereof access can be granted without need of the token in each case and only by said handheld mobile device. Like that it's for example possible to only require the holder to show the token the 1st time he/she is accessing the corresponding building or area, and after that the mobile phone will automatically allow to authorize and unlock the corresponding access point. If however for example the usual working hours have passed, this non-token-based authorization can be revoked so as to increase security.

[0021] According to a 2nd aspect of the present invention, it relates further to an access control system upgraded using a method as detailed above and comprising the structural elements as outlined above.

[0022] According to yet another aspect of the present invention, it relates to a method of operating an upgraded access control system as detailed in the preceding paragraph including the steps of:

- keeping the interception unit at low energy and/or range level for broadcast only;
- establishing an encrypted communication between the interception unit and the mobile handheld device by said radiofrequency interface, if need be after verifying distance information between the 2 units;
- requesting input information from the holder on said mobile handheld device by corresponding optical and/or acoustic signal emitted by said mobile handheld device ;
- collecting input by said mobile handheld device , wherein preferably said input is a pin code, and/or a biometric information;
- transmitting said input information, either directly in an encrypted way or after a verification in said mobile handheld device and/or after a verification of the input information by establishment of a communication between said mobile handheld device and the overall control and permission of the overall control, to the interception unit;
- forwarding of permission information received by the interception unit from the reader unit via the 2nd control line to the access controller for unlocking the unlocking device.

[0023] According to yet another aspect of the present invention, it relates to a method of setting up a holder in an upgraded access control system as outlined above including the steps of:

- a new holder installs a respective app on the personal mobile handheld device ;
- for a 1st time approaches the access point;
- the app connects to the interception unit in learning mode;
- the holder uses the personal token on the reader unit;
- token information transmitted from the reader to the interception unit is transmitted to the mobile handheld device and is stored therein in an encrypted and unreadable for the holder way.

[0024] Last but not least the present invention relates to a particularly tailored interception unit for a method as outlined above or to be part of or used in an access control system as outlined above and preferably comprising at least one radiofrequency interface for establishing a wireless communication channel between said interception unit and a mobile handheld device of said holder, and wherein said verification by the interception unit involves retrieving information about access permission of said holder via said mobile handheld device, wherein preferably the radiofrequency interface is a wireless local area network (WLAN) interface, a Bluetooth interface, Bluetooth smart, preferably a low-energy Bluetooth interface.

[0025] Further embodiments of the invention are laid down in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026] Preferred embodiments of the invention are described in the following with reference to the drawings, which are for the purpose of illustrating the present preferred embodiments of the invention and not for the purpose of limiting the same. In the drawings,

Fig. 1 shows a schematic representation of a pre-existing access control system including one central access controller and to exemplary access points with reader and unlocking unit;

Fig. 2 shows a schematic representation of such an access control system upgraded in accordance with the present invention; and

Fig. 3 shows a schematic representation of an interception unit according to the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

[0027] As illustrated in figure 1, a pre-existing access control system typically involves, at each access point, a reader unit 1 and an unlocking device 3, the latter normally being an electric motor controlled to withdraw or bring forward a locking pin or the like. As illustrated in this figure, there is one central access controller 2 in case of several, in this case two different access points each with reader unit 1 and unlocking device 3.

[0028] Such a pre-existing access control system furthermore typically includes a management unit 7, e.g. a central computer or server, which is also linked to the access controller 2, and which can be used to manage and control the access permissions in the access controller 2. Access is controlled in this case by a personal token 6, which can be a batch, or a key, which would then be a combination of a mechanical and an electrical/electronic access device, which can be used for accessing a certain access point. As illustrated on the left side of figure 1, the token 6 is approached to the reader unit 1 for access, and the reader unit typically communicates via radiofrequency with the token, which basically then acts as an RFID. Typically this communication is encrypted. The corresponding token information, typically in encrypted form, is subsequently transferred via a 1st physical control line 4 from the reader unit 1 to the access controller 2. In the access controller 2 the token information, is compared with corresponding authorization codes, or databases, and if there the required access permission can be established by this comparison, an unlocking signal is transmitted from the access controller 2 to the unlocking device 3 for unlocking the door of the access point.

[0029] Typically these access control systems date back into the 80s and 90s and have a certain security standard, which is certainly good, but very often not sufficient for nowadays standards. However upgrading such an access control system involves uninstalling the existing structure and building in a new structure, which is costly, time-consuming and sometimes even essentially impossible.

[0030] This is where the present invention provides for an unexpectedly simple but very efficient and at the same time very safe upgrade as shall be outlined herein below.

[0031] All that needs to be done for upgrading such an access control system is one basically inserts an interception unit 9 into the 1st control line 4 between the reader and the access controller 2. So basically this 1st line 4 is split into a 1st part line 4' between the reader unit 1 and the interception unit 9, and a 2nd part line 4" between the interception unit 9 and the access controller.

[0032] In a nutshell, the interception unit acts to intercept the data transfer and only forward the data received from the reader if corresponding access granting or identification is established in the interception unit 9.

[0033] To this end the interception unit 9 is provided with communication means to communicate with a portable handheld device 10 carried by the person also carrying the token 6 and desiring to pass the access point. Once the handheld device 10 is in sufficient proximity to the interception unit 9, a preferably encrypted data connection is established between the interception unit 9 and the mobile handheld device 10. An app installed on the mobile handheld device 10 after establishment of this data connection for example request the user to input a pin, to present the finger to a fingerprint sensor on the handheld device, to make a picture of the face or of the eye or the like, in the sense of biometric data, and only if this data is then verified to be correct, the interception unit 9 forwards the data, initially received from the reader unit via line 4', for which via line 4" to the access controller 2, which will then, without having to be modified at all basically, trigger the corresponding unlocking signal for the unlocking device 3. In order to increase identification verification what can and preferably is done is that the information retrieved by the mobile handheld device is further verified by establishment of a mobile data connection of the mobile handheld device 10 to the Internet, where on the Internet then, by corresponding communication between the app on the handheld device and the corresponding Internet site, preferably using an encrypted protocol, the information is verified, and if positively verified the corresponding access granting approval is transmitted to the app on the handheld device, the handheld device will transmit the approval to the interception unit 9, and in turn the interception unit 9 will then basically release the signal to the access controller 2.

[0034] The essential elements of the interception unit 9 required for actually carrying out this function are schematically illustrated in figure 3. The interception unit 9, which can be in a separate housing, which however can also be put into the housing of the reader for example, comprises a reader interface 14 for communicating with the reader by line 4' , and a controller interface 15 for communicating with the access controller 2 by line 4". There is a central processing unit with RAM and ROM as well as volatile and/or non-volatile additional memory, and an additional power supply 12, typically grid based and in case of grid failure, including a battery or the like for backup. Furthermore the interception device 9 comprises a radiofrequency interface for communication with the mobile handheld device 10. This is preferably a low-energy Bluetooth interface, so as to save energy and to avoid unnecessary radiofrequency emission.

[0035] More specifically, the main electronics of the interception unit shall be outlined as follows: there is provided a usual intelligent controller, often SoC or single chip, like, comprising CPU, ROM to hold program storage, RAM for temporary data storage (volatile) and stack, data storage nonvolatile, an encryption unit, typically in the hardware, supports accelerated Advanced Encryption Standard (AES) calculation, RTC - Realtime clock to maintain time in case of power outage (battery powered), RF interface 13 - here: Bluetooth low energy (BLE, bluetooth smart) protocol engine, radio, HF amplifiers etc.

[0036] In the hardware, one can for example use the CC2540 TI specialized microcontroller which contains all above (no RTC, but a counter).

[0037] Connected to such a main controller is

the eader interface 14, which behaves like the usual "controller side" interfaces a reader is connected to. In case of "wiegand", there are min. 2 inputs for "D0" and D1" data lines, typically a reader block or LED indication output, a buzzer control output (optional). Alternative versions can use different interfaces like Omron Magstripe (clock&Data) interface, serial RS-485 or other interfaces

a controller-side interface 15, which behaves like the usual "wiegand" or other access reader. In case "wiegand", there are min. 2 outputs for D0 and D1 data lines, typically reader block or LED indication INPUTS, buzzer control input.

[0038] Alternative versions might have other outputs or interfaces.

[0039] A key is that 14 and 15 are "inverse function" interfaces, so while a reader can be connected to 14, 15 actually SIMULATES a reader to the controller.

[0040] Other components might include a higher level application CPU with more memory, encryption, decision making capabilities.

[0041] Power supply circuitry will generally be needed also, as illustrated by reference numeral 12.

[0042] Another important part of the solution is a smart phone 10, which can communicate with the main electronics via Bluetooth or Bluetooth Smart or Wifi.

[0043] A cloud based service can be used also to enhance functionality in the communication 19. The invention can be used as a standard BLE based ID reader.

[0044] In this mode of operation, the device 9 can receive credentials from a smart phone and deliver these to the controller, effectively emulating a Wiegand Reader.

[0045] However, the invention offers currently unknown possibilities due to the additional interfaces and software.

[0046] Some of the following functions can be used independently and work well together.

[0047] The two main functions the invention can provide are

- increasing the level of security of an existing, installed access control system with minimal changes to the system;
- increasing the usability and convenience of an existing, installed access control system.

[0048] In addition, use of the invention can also provide online reporting and even decision making for currently offline, installed access control systems, which generally also results in higher security and monitorability.

[0049] One key idea of the invention is that it can "intercept" the credentials coming from a reader 1, and only forwarding these to the controller 2 after certain additional security checks, logging or validation of personal security credentials (pin, password, fingerprint, face contour etc) have been conducted.

[0050] Only once these checks are finished, the original (or modified credentials are released to the controller.

[0051] Possibilities include time or other criteria based additional checks (for example, if an employee comes in the morning, he also needs to do a face recognition check on his mobile, but later he does not need to do this).

[0052] One other key idea is that the intercepted credentials can be stored into the memory of the RF connected mobile phone, so that the user has no access, the data is safely encrypted, and can be released at the next reader (door).

[0053] As an example, an employee arriving in the morning to the premises of a military or industrial location will "badge" to open the door, with all other security steps involved. The credentials of his card can be captured into the memory of the mobile phone, and for any further access within the premises, no ID card or batch is needed any more ("hands free" operations) because the ID of the employee has now entered the memory of the smart phone, potentially has been online validated, and can be transmitted through the inventions port 15 to door controllers 9 as if the employee would use his hands and his ID/batch manually (which he still may do).

[0054] Such intercepted credentials need to be kept secure. So one aspect of the invention can be that by use of location data, the ID information can be erased from the mobile phone once it leaves the perimeter of the location (geo fencing), so a lost phone outside of the area can not be used for entry.

[0055] It is also possible to go completely "badge free" in that the mobile phone 10 connects to a server to get the ID credentials (userid/password can be used to secure that data, and the phone can then get a local copy of the ID data), and instead of presenting a badge, carrying the mobile phone will be enough to be identified.

[0056] Range reading: The BLE standard preferably used in the present device includes the possibility to transmit at different RF levels, and also include the actual transmit energy level in announcements.

[0057] On the other side, standard mobile phone, bluetooth BLE stack implementations, API and libraries support "ranging" by reading the RSSI level from the RF receivers, and calculating, based on that information PLUS the transmitted RSSI level, the approximate distance.

[0058] Using this functionality, it can be assured that a user with a mobile phone is only recognized when within a certain defined distance (20cm, 50cm etc).

[0059] For example - this functionality can be used to make sure the above mentioned "copy ID into local memory" function can only be used if the mobile is within very close proximity of the device 9, however, later, for the "hands free" solution (sending back the ID for entry), a larger distance is allowed.

[0060] The following functions can be added, individually or in any combination, to already installed, legacy access control systems without the need to update these with anything else but the interception unit according to the invention:

- increase security by adding pin functionality (using the mobile phone as the pin pad)
- pin requirement may be time schedule controlled
- alternatively, fingerprint can be required (on mobile phones which have a fingerprint id mechanism)

- alternatively, face recognition, voice recognition, or any other way to identify the user can be used
- increase security by just checking for the availability of the mobile with the user
- increase security by automatically going online and checking that the mobile (identified by MAC, user name or whatever) matches the ID card in the pocket of the user
- increase security by checking that the user has the right at this time, date, to enter the site (important for remote infrastructure maintenance, train, truck use etc)
- logging of the access attempts to the central website can be enabled by using the mobile phone as an internet access device for the invention
- online validation of the credentials/access attempts can be added before the ID is forwarded
- a new ID management system can be built up online, where the system has a different set of credentials/IDs, and only if the user's presented ID is authorized by

the online system, a "simple" ID to unlock the system is provided to the controller The system can even be used as a modern "immobilizer" or locking system for trucks, machines etc. A "driver" can safely go to a coffee break, because without his mobile phone, the truck will not start.

[0061] When he returns to his car, the mobile phone will "see" the truck, and go online to request an authorization key that the user may operate the truck, which then, upon approval, is encrypted with the car's security credentials and sent via the invention into the truck to unlock it.

[0062] Same can be used for loading decks etc an electronic lock in addition to any mechanical locks on which any access attempt can be monitored, logged and prohibited in case there is no rights.

[0063] However, main use of the invention is the upgrade of current access control installations using readers, to increase security or usability, by adding the mobile phone component with its readers and interfaces, and the possibility to go online for recording and decision making at a central location.

[0064] The invention enables legacy access control systems to be part of the "internet of things" without the central controllers to be touched.

[0065] It can also be used to monitor the "door enable" relay/ door strike power, so that the effective "entry ok" signal can be locked in addition.

LIST OF REFERENCE SIGNS

1	reader unit
2	access controller
3	unlocking device
4	1st control line between reader unit and access controller
5	2nd control line between access controller and unlocking device
6	token (batch, key)
7	management unit
8	communication between access controller and management unit
9	interception unit
10	mobile handheld device
11	wireless communication between interception unit and mobile handheld device
12	power supply unit
13	radiofrequency interface, Bluetooth low energy
14	reader interface
15	controller interface
16	housing
17	central control unit
18	wireless communication between interception unit and mobile handheld device
19	wireless communication between mobile handheld device and overall control

Claims

1. Method for upgrading an existing access control system, said existing access control system comprising at least one access point which is controlled by a reader unit (1) for reading authorization information from a portable token (6) and a corresponding unlocking device (3), wherein the reader unit (1) is in wired connection via at least one 1st control line (4) communicatively connected to an access controller (2), wherein said access controller (2) is in wired connection via at least one 2nd control line (5) communicatively connected to said unlocking device (3), and wherein said access controller (2) controls the locking state of said unlocking device (3) via said 2nd control line (5) by verifying identification information transmitted via 1st control line (4) from said reader unit (1),
wherein the method comprises the steps of interposing into the at least one 1st control line (4) an interception unit (9), said interception unit (9) adapted to and allowing for receiving and, if needed after temporarily withholding said

identification information from said reader unit (1), only transmitting it to the access control unit (2) once said interception unit (9) has verified permission to access independently via a 2nd communication with a holder of said token (6).

2. Method according to claim 1, wherein the interception unit (9) comprises at least one radiofrequency interface (13) for establishing a wireless communication channel (18) between said interception unit (9) and a mobile handheld device (10) of said holder, and wherein said verification by the interception unit (9) involves retrieving information about access permission of said holder via said mobile handheld device (10), wherein preferably the radiofrequency interface (13) is a wireless local area network (WLAN) interface, a Bluetooth interface, Bluetooth smart, preferably a low-energy Bluetooth interface.

3. Method according to claim 2, wherein retrieving information about access permission of said holder via said mobile handheld device (10) includes the steps of identifying said holder and/or said mobile handheld device (10) by means of input given by said holder into said mobile handheld device (10), and/or by means of readout of an unambiguous identification number from said mobile handheld device (10), wherein said input is preferably at least one of: a pin code, a biometric information collected by said mobile device, such as fingerprint, picture, in particular face picture, positional information, or a combination thereof.

4. Method according to claim 2 or 3, wherein retrieving information about access permission of said holder via said mobile handheld device (10) includes the step of establishing an external wireless communication (19) using a WLAN or telecommunication channel by said mobile handheld device (10) to an overall control authority which verifies access permission independently and transmits, if access granted, a corresponding permission back to said mobile handheld device (10) and directly and/or in directly via said radiofrequency interface (13) to the interception unit.

5. Method according to any of the preceding claims, wherein the interception unit (9), after having verified permission to access, transmits said identification information from said reader unit (1) identical to the one as initially received from said reader unit (1) or in a modified way.

6. Method according to any of the preceding claims, wherein verifying permission to access either by the interception unit (9) autonomously and/or by an overall control authority via communication there with by means of the mobile handheld device (10) involves authorizing and/or determining at least one of: access time, access frequency, access number, access permission status of holder, trust status of holder, compliance of data about or from holder retrieved by said mobile handheld device (10) with an internal database, location of the mobile handheld device determined via GPS (geo-fencing) or a combination thereof.

7. Method according to any of the preceding claims, wherein the radio frequency interface (13) automatically establishes a radiofrequency connection to said mobile handheld device (10) once it is in sufficient proximity to the interception unit (9), and, if needed, once connection established, increases the power level from low level stand by to high-level.

8. Method according to any of the preceding claims, wherein the interception unit (9) is provided with means for determining the distance between the interception unit (9) and the mobile handheld device (10), and wherein this distance is taken into account as a parameter for granting access.

9. Method according to any of the preceding claims, wherein the interception unit (9) comprises an independent CPU, RAM, ROM, volatile and/or non-volatile data storage elements, an encryption unit, standalone and/or grid based power supply, if need be a real-time clock element, and optionally a secondary CPU, RAM/ROM, data storage element.

10. Method according to any of the preceding claims, wherein the transmission via said 1 st communication line (4) is serial, Wiegand or clock and data, and/or wherein communication via said 1st control line (4), and/or via said 2nd control line (5), and/or between (18) the interception unit (9) and the mobile handheld device (10) and/or between (19) the mobile handheld device (10) and the overall control is encrypted.

11. Method according to any of the preceding claims, wherein once authorized by at least one of token (9), handheld mobile device (10), independent verification by overall control or a combination thereof access can be granted without need of the token (9) and only by said handheld mobile device (10).

12. Access control system upgraded using a method according to any of the preceding claims.

13. Method of operating an access control system according to claim 12 including the steps of:

keeping the interception unit (9) at low energy and/or range level for broadcast only;
establishing an encrypted communication between the interception unit (9) and the mobile handheld device (10) by said radiofrequency interface (13), if need be after verifying distance information between the 2 units;
requesting input information from the holder on said mobile handheld device (10) by corresponding optical and/or acoustic signal emitted by said mobile handheld device (10);
collecting input by said mobile handheld device (10), wherein preferably said input is a pin code, and/or a biometric information;
transmitting said input information, either directly in an encrypted way or after a verification in said mobile handheld device (10) and/or after a verification of the input information by establishment of a communication between said mobile handheld device (10) and the overall control and permission of the overall control, to the interception unit (9);
forwarding of permission information received by the interception unit (9) from the reader unit (1) via the 2nd control line (5) to the access controller for unlocking the unlocking device (3).

14. Method of setting up a holder in an access control system according to claim 12 including the steps of:

a new holder installs a respective app on the personal mobile handheld device (10);
for a 1 st time approaches the access point;
the app connects to the interception unit (9) in learning mode;
the holder uses the personal token (6) on the reader unit (1);
token information transmitted from the reader to the interception unit (9) is transmitted to the mobile handheld device (10) and is stored therein in an encrypted and unreadable for the holder way.

15. Interception unit (9) for a method according to any of the preceding claims or for an access control system according to claim 12 comprising at least one radiofrequency interface (13) for establishing a wireless communication channel (18) between said interception unit (9) and a mobile handheld device (10) of said holder, and wherein said verification by the interception unit (9) involves retrieving information about access permission of said holder via said mobile handheld device (10), wherein preferably the radiofrequency interface (13) is a wireless local area network (WLAN) interface, a Bluetooth interface, Bluetooth smart, preferably a low-energy Bluetooth interface.

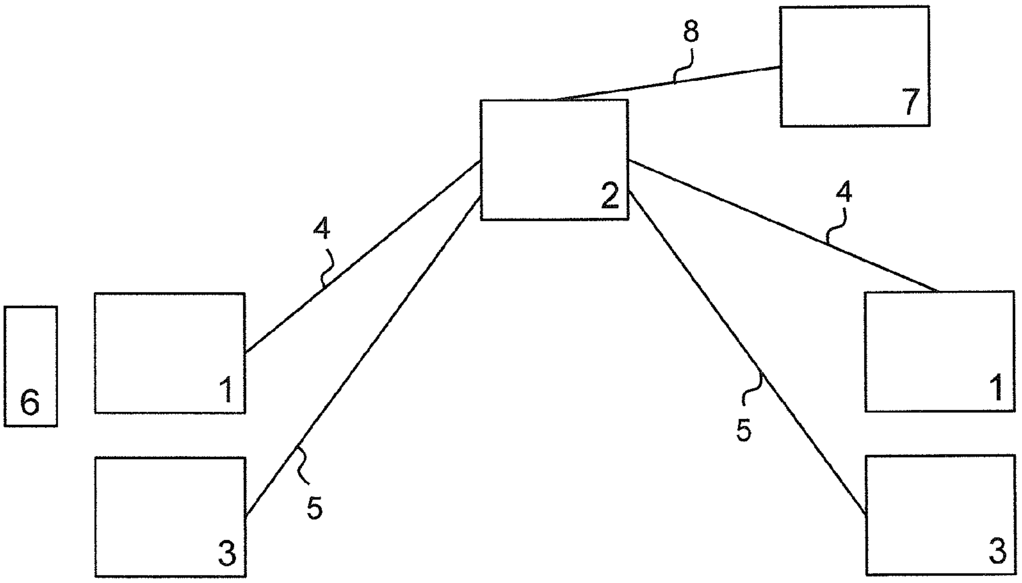

FIG. 1

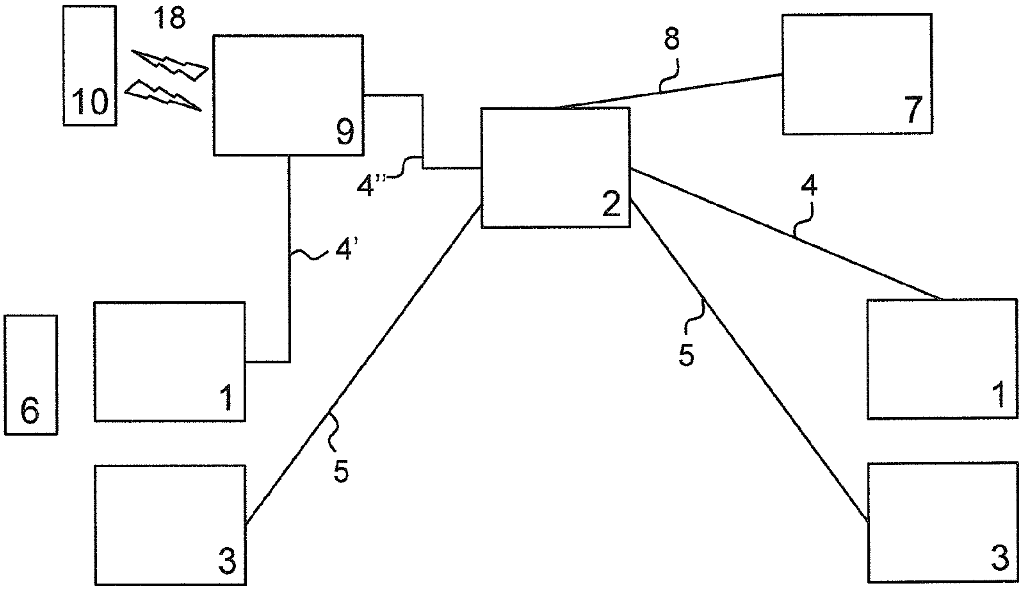

FIG. 2

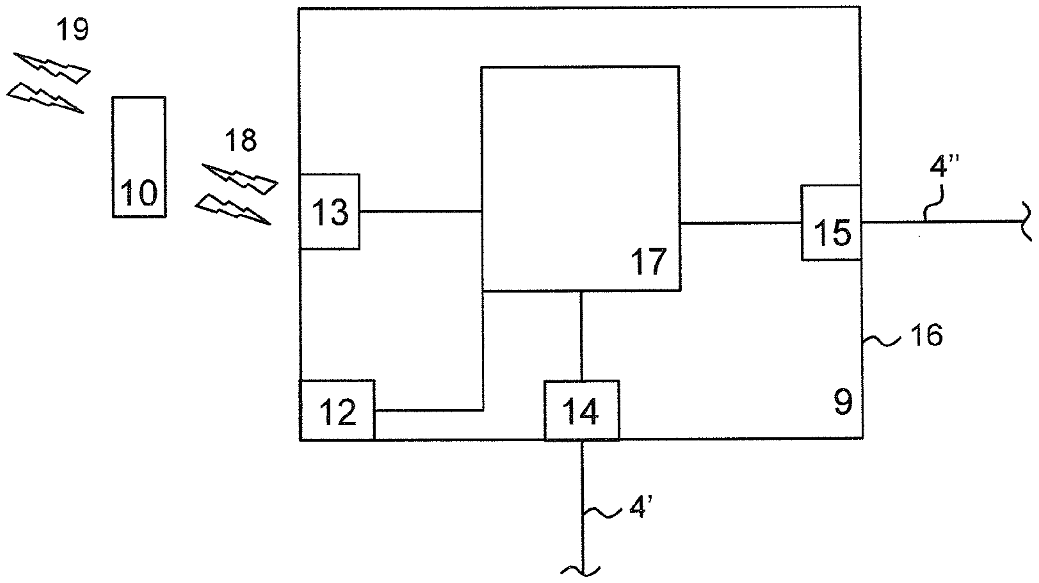

FIG. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 15 15 6996

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	US 2004/041019 A1 (ULTRA SCAN CORP [US]) 4 March 2004 (2004-03-04) * abstract; figure 1 * * paragraphs [0001] - [0019] * -----	1-12	INV. G07C9/00
X A	US 2003/200446 A1 (SIEGEL WILLIAM G [US] ET AL) 23 October 2003 (2003-10-23) * abstract; figure 1 * * paragraphs [0007] - [0028] * -----	1,12 2-11	
X A	EP 2 738 707 A1 (HID GLOBAL GMBH [DE]) 4 June 2014 (2014-06-04) * abstract; figures 1,2 * * paragraphs [0006] - [0037] * -----	1,12 2-11	
A	US 2012/280783 A1 (GERHARDT PAUL MICHAEL [US] ET AL) 8 November 2012 (2012-11-08) * abstract; figure 30 * * paragraphs [0154] - [0158] * -----	1-12	
A	US 2003/197593 A1 (SIEGEL WILLIAM G [US] ET AL) 23 October 2003 (2003-10-23) * abstract; figures 3,4 * * paragraphs [0007] - [0013] * * paragraphs [0038] - [0059] * -----	1-12	TECHNICAL FIELDS SEARCHED (IPC) G07C
A	US 5 679 945 A (RENNER G FRED [US] ET AL) 21 October 1997 (1997-10-21) * abstract; figures 4,5 * * column 2, lines 30-43 * * column 5, line 30 - column 6, line 52 * * column 9, line 8 - column 10, line 58 * -----	1-12	
A	WO 2005/001777 A1 (SCM MICROSYSTEMS GMBH [DE]; MERKERT ROBERT J SR [US]) 6 January 2005 (2005-01-06) * abstract; figures 2,3 * * page 1 - page 4 * -----	1-12	

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
The Hague	8 September 2015	Pfyffer, Gregor

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

Europäisches Patentamt
European Patent Office
Office européen des brevets

Application Number

EP 15 15 6996

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing claims for which payment was due.

□ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due and for those claims for which claims fees have been paid, namely claim(s):

□ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

□ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

□ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

□ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1-12

□ The present supplementary European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims (Rule 164 (1) EPC).

Europäisches Patentamt
European Patent Office
Office européen des brevets

LACK OF UNITY OF INVENTION SHEET B

Application Number

EP 15 15 6996

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-12

   Method for upgrading an existing access control system

   ---

2. claim: 13

   Method for operating an access control system

   ---

3. claim: 14

   Method for setting up a new user in an access control system

   ---

4. claim: 15

   Interception unit for an access control system

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

EP 15 15 6996

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.

08-09-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004041019 A1	04-03-2004	AU 2003260092 A1	19-03-2004
		BR 0313802 A	05-07-2005
		CA 2496669 A1	11-03-2004
		CN 1689021 A	26-10-2005
		EP 1540567 A2	15-06-2005
		US 2004041019 A1	04-03-2004
		WO 2004021253 A2	11-03-2004
US 2003200446 A1	23-10-2003	AU 2003222673 A1	03-11-2003
		US 2003200446 A1	23-10-2003
		WO 03090403 A1	30-10-2003
EP 2738707 A1	04-06-2014	EP 2738707 A1	04-06-2014
		US 2014144985 A1	29-05-2014
US 2012280783 A1	08-11-2012	CA 2834964 A1	08-11-2012
		CN 103635940 A	12-03-2014
		EP 2710562 A1	26-03-2014
		US 2012280783 A1	08-11-2012
		US 2012280789 A1	08-11-2012
		US 2012280790 A1	08-11-2012
		US 2014365773 A1	11-12-2014
		US 2015102906 A1	16-04-2015
		US 2015181014 A1	25-06-2015
		WO 2012151290 A1	08-11-2012
US 2003197593 A1	23-10-2003	AU 2003234149 A1	03-11-2003
		US 2003197593 A1	23-10-2003
		US 2005264398 A1	01-12-2005
		WO 03090154 A1	30-10-2003
US 5679945 A	21-10-1997	AU 5313896 A	16-10-1996
		CA 2217052 A1	03-10-1996
		US 5679945 A	21-10-1997
		US 6223984 B1	01-05-2001
		WO 9630857 A1	03-10-1996
WO 2005001777 A1	06-01-2005	DE 20309254 U1	06-11-2003
		EP 1634250 A1	15-03-2006
		US 2005082365 A1	21-04-2005
		WO 2005001777 A1	06-01-2005

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