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

(11) EP 3 358 535 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.08.2018 Bulletin 2018/32

(51) Int Cl.:
G07C 9/00 *(2006.01)* *G01C 21/36* *(2006.01)*

(21) Application number: **17154715.1**

(22) Date of filing: **03.02.2017**

(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 MD

(71) Applicant: **dormakaba Deutschland GmbH**
58256 Ennepetal (DE)

(72) Inventors:
- **FIEGE, Gero**
  58256 Ennepetal (DE)
- **FANARJI, Alexander**
  58256 Ennepetal (DE)
- **WOLF, Martin**
  58256 Ennepetal (DE)
- **SCHWARZ, Dieter**
  58256 Ennepetal (DE)
- **KRAVCHENKO, Ivan**
  58256 Ennepetal (DE)
- **GIERNICH, Stephan**
  58256 Ennepetal (DE)
- **HIRTSIEFER, Werner**
  58256 Ennepetal (DE)
- **SCHMIDT, Andreas**
  58256 Ennepetal (DE)
- **ESCH, Simone**
  58256 Ennepetal (DE)

(74) Representative: **Balder IP Law, S.L.**
Paseo de la Castellana 93
5a planta
28046 Madrid (ES)

(54) METHOD FOR LOCALISING AN ELECTRONIC LOCK

(57) The application relates to a method for helping a user find the location of an electronic lock 10 which can be opened with the user's data carrier 40. The data carrier 40 can communicate with the electronic lock 10, and the electronic lock 10 can grant access to a physical space upon validation of access rights.
The data carrier 40 is provided with access rights readable by the electronic lock 10 and with a digital image 50 of the electronic lock 10, e.g. of the complete front door 11 in which it is installed. The access rights and the digital image may be sent to the data carrier over the same communications channel. The access rights may be time restricted.

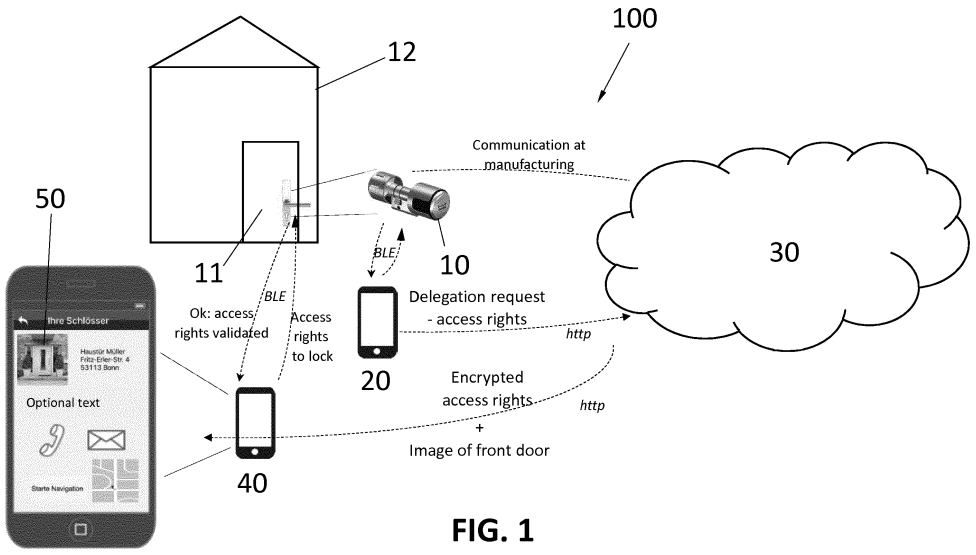

FIG. 1

EP 3 358 535 A1

Description

TECHNICAL FIELD

[0001] The present invention is related to the field of access control systems for controlling access to one or more specific areas in a building.

STATE OF THE ART

[0002] It is known that electronic access control systems are often used to control access to certain areas or physical spaces within the building. These electronic access control systems (which will be also referred to in the following as EAC systems) usually comprise a door lock that gives access to that specific physical space of the building; a user who wants to access this space is in possession of some sort of mobile data carrier with an identification code stored therein. When the user approaches that door lock and the mobile data carrier is in close proximity of a reader in the door, the identification code is read by the reader, and if the read identification code is valid, then access to the space secured by the door lock is given to the holder of the mobile data carrier.

[0003] As a general rule, the identification code stored in the mobile data carrier which upon being determined as valid gives access to the physical space, is provided by a control access server. Indeed, this access control server is the element of the EAC system in charge of establishing these identification codes when setting up the EAC system; the access control server then provides these identification codes to the mobile data carrier. Different identification codes are usually given to every user of the EAC system who requests access that specific space. Each identification code may be valid to gain access to a single space within the building, or it may provide access to several spaces or areas within the building (their office or the cafeteria in a business building), but not to others (the servers area in the IT department or the safe deposit room in the account department). Similarly, the identification code may be valid any time, or its validity may be temporarily restricted (so that an employee has access on weekdays and at certain time slots, but not during the weekend).

[0004] However, it may be the case that the person that has been given rights to access a specific place has not been in that place before, and has difficulties in reaching that place. For example, it might be the case that a parcel has to be delivered at a house by a messenger, the messenger has never been in the house before and is unable to reach it.

[0005] Currently most mobile devices include navigation systems, which might be helpful to solve the above problem. But it is known that sometimes these navigation systems are not very precise, and/or consume too many resources from the mobile device such as big amount of data (which is not always readily available for coverage and/or economic reasons) and also battery; or the address of the owner is not sufficiently detailed. In these occasions, the messenger is unable reach the house where the parcel should be delivered.

DESCRIPTION OF THE INVENTION

[0006] The invention provides a method for facilitating location of an access-based resource.

[0007] According to the present invention, it is possible to provide access rights to a user so that this user can access specific spaces within the system, and also, to facilitate this user to locate the access-based resource.

[0008] A first aspect of the invention relates to a method for facilitating location of an access-based resource to at least one data carrier, the data carrier being able to communicate with the access-based resource, and the access-based resource being configured to grant access to a physical space upon validation of access rights, the method comprising:

- providing the at least one data carrier with access rights readable by the access-based resource;
- providing the at one least data carrier with digital data containing at least one image including the access-based resource.

[0009] This way, a user of the data carrier is provided with access rights to access an access-based resource, and also with at least an image of the access-based resource so as to be able to locate it.

[0010] The digital data can be sent to the at least one data carrier together with the access rights using a same communication channel, usually in a wireless fashion. The digital data need not be encrypted, just the access rights are preferably encrypted, so there is no need for a separate channel.

[0011] In the context of the present invention, the digital data is any one of: an image file of the access-based resource (such as a JPG, JPEG, BMP or any other image file), any file containing the at least one image of the access-based resource (such as a Word or a PDF file, or a video file), or a combination thereof.

[0012] The digital data containing at least one image including the access-based resource can be any geographical or geolocation data of the access-based resource, including picture representations containing the access-based resource, usually of the door or locker where the access-based resource is installed. This representation facilitates the user of the at least data carrier (who is provided with the digital data) to find the access-based resource.

[0013] In some embodiments the access-based resource is an electronic or intelligent lock mounted in a door (or similar) which gives access to the physical space in the building. The electronic lock usually comprises a reader which is able to read access rights provided to the at least one first data carrier; it is also possible that the reader is implemented as an element physically sep-

arate of the electronic lock. The access-based resource is configured to grant access to the physical space upon reading and validating access rights presented to it by the at least one data carrier.

[0014] In the context of the present invention, the at least one data carrier (preferably a mobile data carrier) can be any mobile device or portable electronic device that has processing and communication capabilities, so as to process signals and exchange information with other elements, such as the access-based resource and a server.

[0015] The access rights defined for the at least one data carrier include preferably encrypted data, more preferably in binary form. In this respect, the at least one data carrier may just serve as carrier and storing means for the access rights; the at least one data carrier does not need to be able to process or understand these access rights; the access-based resource is able to read and process these preferably encrypted access rights.

[0016] These access rights can be provided so as to access one or more access-based resources. Also these access rights can be time-limited or not.

[0017] In some embodiments, for security reasons, the access rights defined for the at least one data carrier are directly to the at least one data carrier, preferably via means of an encrypted data package.

[0018] Communication between the at least one data carrier and the access-based resource is preferably done via a short-range communication channel (infrared, NFC, Bluetooth® or BLE, WiFi, etc). Communication between the at least one data carrier and any server is preferably done using any telecommunications network (3G, LTE, etc) or by means of a WiFi network.

[0019] In some embodiments, the method comprises further sending to the at least one data carrier a one-time access to a server storing the digital data containing at least one image including the access-based resource, preferably in the form of a link to the access control server. If the digital data containing at least one image including the access-based resource is too heavy, the user of the at least one data carrier may decide when to access the server where the digital data is stored (for example, when the at least one data carrier is connected to a WiFi).

[0020] Indeed, the step of providing digital data containing at least one image including the access-based resource can comprise the following steps:

- providing the at least one data carrier with an URL or link to a location on a server where the digital data containing at least one image including the access-based resource is;
- establishing a communication channel between the server and the at least one data-carrier;
- retrieving the digital data containing at least one image including the access-based resource from the server to the at least one data carrier.

[0021] In some embodiments, the step of providing the at least one data carrier with access rights readable by the access-based resource comprises:

- receiving a request of delegation of access rights from another data carrier; the request of delegation of access rights from the another data carrier comprising data related to the at least one data carrier or related to a user of the at least one data carrier;
- defining such access rights for the at least one data carrier; and
- sending the access rights defined for the at least one data carrier to the at least one data carrier.

[0022] The request of delegation of access rights comprises data related to the at least one data carrier (IMSI, MSISDN, or any other set of data that uniquely identifies a mobile device) or data related to a user of the at least one data carrier (such as an email address or a username or a social network identity of the user, reachable from the at least one data carrier).

[0023] The above solution makes it possible to delegate access rights to a first user (the owner or user of the at least one data carrier) by a second user (the owner or user of the another data carrier), so that the second user can access a specific space secured by the access-based resource, with a very simple and flexible process. This might be very useful in case that the access-based resource is the electronic lock installed at the front door of the second user, and the first user does not have access rights to the electronic lock, and the first user needs to get into the second user's house (for example, for delivering a package).

[0024] In this above case, the digital data containing at least one image including the access-based resource is preferably uploaded in the server by the user of the another data carrier (the second user).

[0025] The user of the another data carrier may request that the digital data is provided, or is directly sent, or is made available to the at least one data carrier.

[0026] In some embodiments the method further comprises displaying on the at least one data carrier the at least one image of the access-based resource. This way the user of the at least one data carrier need not do anything else with their data carrier: the image of the access-based resource is automatically shown to him/her.

[0027] Thus, according to the invention, access to the physical space secured by the access-based resource is granted upon validation of the access rights stored in the at least one data carrier. Validation of the access rights is preferably done at the access-based resource; this validation is preferably carried out offline, without establishing any communication with any server at the time of validation, thereby saving resources from the access-based resource.

[0028] Validation of the access rights could also be done at a usually remote server.

[0029] In some embodiments, prior to granting access to the physical space by the access-based resource, the

method further comprises validating code provided by the at least one data carrier. This code may need to be provided by the at least one data carrier, usually upon request to carry out some action with the data carrier, may be gesture-based code (such as a shaking gesture with the first or the second data carrier), or it may be a PIN code or similar, previously introduced in the at least one data carrier. This additional step of validating code at the user side, not just at the access-based resource or the server side, enhances the security in case the at least one data carrier is lost by their authentic user.

[0030] In the above embodiments, whenever a server is mentioned, this server is preferably the access control server that will be defined in the following.

[0031] Another aspect of the invention refers to an access control server for facilitating location of an access-based resource, the access-based resource being configured to grant access to a physical space within a building upon validation of access rights, the access control server comprising:

- means for defining access rights for the at least one data carrier, the access rights being readable by the access-based resource;
- means for providing the at least one data carrier with the access rights, so that the access to the physical space can be granted to the at least one data carrier upon validation of the access rights; and
- means for providing the at least one data carrier with digital data containing at least one image containing the access-based resource.

[0032] In the present invention, the access control server is usually a remote access control server managing several access-based resources located within the same building or in different buildings. The access control server is preferably cloud-based, and communication between the access control server with the other elements is carried out via a wireless communication network. But it is also possible that in some EAC systems, the access control server is not remotely located from the access-based resources it controls, and the communication network may be wired.

[0033] In some embodiments, the access control server is part of an access control system also comprising the access-based resource, and in some embodiments it comprises several access-based resources managed by the same access control server or by several access control servers. The access-based resource has communication capabilities to communicate with the access control server and with the at least one data carrier. _The capability of the access-based resource to communicate with the data carrier(s) is ensured at the production process by adding a secret for decrypting the communication with the data carrier, including the encrypted access rights.

[0034] In some embodiments, the access control server further comprises means for receiving a request of delegation of access rights from another data carrier; the request of delegation of access rights from the another data carrier comprising data related to the at least one data carrier or related to a user of the at least one data carrier.

[0035] In the above case, upon receiving a request of delegation of access rights from the another data carrier, the access control server is preferably configured to define access rights for the at least one data carrier, so that access to the physical space can be granted to the at least one data carrier upon the access-based resource validating the access rights of the at least one data carrier, the request of delegation of access rights from the another data carrier comprising data related to the at least one data carrier or related to a user of the at least one data carrier.

[0036] The another data carrier is preferably previously registered before the access control server, and has been granted access rights for the access-based resource and user rights, which enable the user of the another data carrier to access the access control server; these user rights also enable the user of the another data carrier to delegate access rights to other users.

[0037] The present invention also relates to an access control system for facilitating location of an access-based resource for accessing a physical space within a building is provided, the access control system comprising:

- the access control server as defined in the foregoing;
- the access-based resource as previously defined; and,
- the at least one data carrier being able to communicate with the access-based resource and with the access control server.

[0038] The different aspects and embodiments of the invention defined in the foregoing can be combined with one another, as long as they are compatible with each other.

[0039] Additional advantages and features of the invention will become apparent from the detailed description that follows and will be particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0040] To complete the description and in order to provide for a better understanding of the invention, a set of drawings is provided. Said drawings form an integral part of the description and illustrate an embodiment of the invention, which should not be interpreted as restricting the scope of the invention, but just as an example of how the invention can be carried out. The drawings comprise the following figures:

Figure 1 is a schematic block representation of an access control system for facilitating location of an access-based resource to a data carrier according

to the present invention.

DESCRIPTION OF A WAY OF CARRYING OUT THE INVENTION

[0041] The following description is not to be taken in a limiting sense but is given solely for the purpose of describing the broad principles of the invention. Embodiments of the invention will be now described by way of example, with reference to the above-mentioned drawings showing elements and results according to the invention.

[0042] This invention provides a flexible and simple solution to the problem previously posed in the background section for facilitating location of an access-based resource to third party users.

[0043] The example described in the following corresponds to a parcel delivery service, where a customer of the service and owner of a house has granted temporary access to this house to a parcel courier, and the parcel courier may have difficulties in reaching the house. But the access control system provided by the present disclosure is also applicable to and useful in other services such as nursing services or building management (for managing access to doors, locker facilities and IT communications cabinets), where it might also be necessary to rapidly locate the house (or locker or room in a building) where the service is to be delivered.

[0044] In the context of the present invention, data processing units are assumed to include standardized cryptography modules and algorithms.

[0045] Figure 1 shows the main elements of the access control system 100 of the invention, and how they are interrelated.

[0046] A house holder, Mr. Smith, as a customer of the parcel delivery service, has an electronic lock 10 installed at the front door 11 of his home 12. This electronic lock 10 is burglar-proof, for example, an XS-Pro cylinder with a Legic® reader, complemented with Bluetooth or BLE functionality.

[0047] Mr. Smith also has a mobile smartphone 20, where he can download an application (an Android or iOS App) associated with the access control system 100 and therefore become a user of the system by registering (with his mobile phone number and/or email address) and getting one or more administrator usernames and passwords. As a registered user the house holder acquires user rights for accessing an access control server 30 and for setting access rights to the electronic lock 10. It is also possible to become a user of the system via the corresponding webpage.

[0048] The access control server 30 provides a web-based software that is in charge of generating the individual, time-related and lock-specific access rights, and of maintaining these access rights afterwards. These access rights generated by the access control server 30 were provided to Mr. Smith's mobile smartphone 20 once Mr. Smith registered himself in the system. The downloaded application also enables Mr. Smith to open the electronic lock 10 installed at the front door 11 of his house using his smartphone 20, via a Bluetooth communication interface that is established between the electronic lock 10 and the smartphone 20. In order to open the electronic lock 1, the application should be executed and kept on running as a background process. It is then necessary to activate the application and to unlock the screen of the smartphone and activate the door unlocking in the application to open the door. Mr. Smith needs to hold his smartphone in front of the reader in the cylinder and the electronic lock will open upon validation Mr. Smith's access rights at the access control server 30.

[0049] The downloaded application provides other features and capabilities, which will be explained afterwards.

[0050] In the present example Mr. Smith has temporarily given access rights to the parcel courier, so that the parcel courier can deliver a parcel at his house, where there is no one in at the estimated time the courier will deliver the parcel.

[0051] As a user of the system having user rights, Mr. Smith can access the access control server 30, where a list associated to him as a user is stored; this list includes inter alia, the electronic locks he wishes to have controlled and managed by the system, the users he wants to give access to and to which electronic lock(s) each user has access to, and whether the access authorization is time restricted or not. In this specific example Mr. Smith accesses the access control server 30 with the application in his mobile smartphone or via the corresponding webpage, and indicates that he wishes to delegate access rights to the electronic lock 10 to the parcel courier for a time slot around the estimated delivery time. To do so, Mr. Smith includes the parcel courier's mobile phone number and/or email address in his list, associating the parcel courier's data with the electronic lock 10 and during the required time period.

[0052] Upon doing this, the access control server defines encrypted access rights for the parcel courier's mobile phone which are readable by the electronic lock 10, and which will permit the parcel courier to open the electronic door 10 during the time period defined by Mr. Smith, by using his mobile phone 40.

[0053] These encrypted access rights are sent to the parcel courier's mobile phone 40, via an encrypted data package. The parcel courier has already downloaded the application, as a frequent user of the system; and upon receiving the access rights delegated by Mr. Smith, he may open the electronic lock 10 with his mobile phone 40 and leave the parcel inside Mr. Smith's house.

[0054] According to the invention, in addition to the access rights the parcel courier gets in his mobile phone 40 digital data to locate Mr. Smith's house, so as to make it easier for the parcel courier to reach Mr. Smith's house. These digital data include an image of the electronic lock 10, such as a picture 50 of the complete front door.

[0055] Usually, Mr. Smith has previously uploaded the digital data in the access control server 30 making use

of his user rights; if the picture 50 of the front door is too heavy, instead of the picture itself, the parcel courier may receive a link to the URL direction where the picture is stored in the access control server 30.

[0056] These data can also include additional contact details of Mr. Smith, such as Mr. Smith's mobile phone number, so that the parcel courier may contact him if necessary. Or these data may include detailed geolocalisation data or navigation directions to Mr. Smith's front door, so that the parcel courier may reach Mr. Smith's house.

[0057] To provide these additional data may be very helpful to the parcel courier in certain situations, for example, when the parcel courier is unable to find Mr. Smith's house, because Mr. Smith's address is not very precise or fully detailed; for example, Mr. Smith's lives in a group of similar houses, all having the same postal address; by getting the picture of the front door the courier can identify the correct house. Or the person receiving the access rights may be a visitor making use of an accommodation service, who reaches his rental accommodation very late and is having difficulties at reaching the front door of the flat he has rented. If the owner of the building where the rented flat is has previously uploaded detailed information on how to reach the flat, such as pictures of the front door of the building and of the specific flat the user has paid for (in many storey buildings the front doors of all the flats sometimes have no number, but they may be identifiable by some specific feature related to the front door, such as the door mat), the visitor may be able to reach their rented flat without bothering the owner of the flat.

[0058] These digital data containing at least an image including the access-based resource need not be encrypted, and can be sent to the parcel courier's mobile phone 40 together with the access rights using the same channel; there is no need to establish a separate channel.

[0059] If the owner of the mobile device who has been provided access rights (temporary or permanent) is not yet registered in the system, a one-time access to the access control server is sent to the mobile device so as to download the application and be able to open the electronic lock. This way, the owner of the mobile device may also register himself into the access control system; then the encrypted access rights for the electronic lock 10 are sent to the mobile device.

[0060] In the present example, the access rights provided to the parcel courier are time restricted to the time interval chosen by Mr. Smith. The access control server configures these access rights as valid for the specific time interval and then they expire by themselves offline. There is no need to synchronize with the access control server in order to terminate the validity of the access rights. So in case of losing the smartphone, a possible intruder that takes the smartphone will not be able to open the electronic door: since validation is carried out offline and the smartphone is used as an AoC ('access on card') to open the electronic lock 10, the 'AoC' access rights which are time restricted will not open the electronic lock after the time interval chosen by Mr. Smith, which can be made to a single day or even some hours.

[0061] In case the validation of the access rights is done online at the access control server, the access rights presented with the "lost" smartphone will not be validated, since Mr. Smith when detecting the smartphone loss deletes those access rights from the list in the server.

[0062] To make the service more secure and reliable, Mr. Smith may decide that the electronic lock 10 of his front door 11 is only openable if, in addition to presenting access rights validated by the access control server 30, a valid PIN code is entered by the user of the smartphone mobile phone. Or he may also establish that a specific action or gesture has be done with the smartphone. In such case, Mr. Smith with his user rights can do so by executing the application in his smartphone, accessing the access control server, and entering the should specific PIN code or gesture-based action that is needed to additionally input to open the electronic lock of his front door. This two-step validation provides a security feature in case Mr. Smith loses his smartphone 20, since if the PIN or gesture-based action request is activated, the user must know the required PIN or gesture-based action, enter the PIN or do the gesture, and hold the device again in front of the electronic lock to open it.

[0063] Though not detailed, the method for facilitating location of an access-based resource of the present invention includes sequences of messages and commands for reading the access rights, validating the access rights at the access control server, and granting access to the access-based resource; and for establishing the necessary communication channels for uploading and downloading the digital data containing at least an image showing at least the access-based resource.

[0064] In this text, the term "comprises" and its derivations (such as "comprising", etc.) should not be understood in an excluding sense, that is, these terms should not be interpreted as excluding the possibility that what is described and defined may include further elements, steps, etc.

[0065] The invention is obviously not limited to the specific embodiment(s) described herein, but also encompasses any variations that may be considered by any person skilled in the art (for example, as regards the choice of materials, dimensions, components, configuration, etc.), within the general scope of the invention as defined in the claims.

Claims

1. Method for facilitating location of an access-based resource (10) to at least one data carrier (40), the data carrier (40) being able to communicate with the access-based resource (10), and the access-based resource (10) being configured to grant access to a

physical space upon validation of access rights, the method comprising:

- providing the at least one data carrier (40) with access rights readable by the access-based resource (10);
- providing the at one least data carrier (40) with digital data containing at least one image (50) including the access-based resource (10).

2. The method of claim 1, wherein the step of providing digital data containing at least one image (50) including the access-based resource (10) comprises:

- providing the at least one data carrier (40) with an URL or link to a location on a server (30) where the digital data containing at least one image (50) including the access-based resource is;
- establishing a communication channel between the server (30) and the at least one data-carrier (40);
- retrieving the digital data containing at least one image (50) including the access-based resource from the server (30) to the at least one data carrier (40).

3. The method of any of claims 1-2, which further comprises displaying on the at least one data carrier (40) the at least one image (50) of the access-based resource.

4. The method of any of claims 1-3, wherein the digital data is any one of: an image file of the access-based resource, any file containing the at least one image of the access-based resource, or a combination thereof.

5. The method of any of claims 1-4, wherein the digital data is sent to the at least one data carrier (40) together with the access rights using a same communication channel.

6. The method of any of claims 2-5, further comprising sending to the at least one data carrier (40) a one-time access to the server (30).

7. The method of any of claims 1-6, which further comprises encrypting the access rights prior to sending them to the at least one data carrier (40).

8. The method of any of claims 1-7, wherein the access-based resource (10) grants access to the physical space upon validation of the access rights by the access-based resource (10).

9. The method of any of claims 1-8, wherein the step of providing the at least one data carrier (40) with access rights readable by the access-based resource (10) comprises:

- receiving a request of delegation of access rights from another data carrier (20); the request of delegation of access rights from the another data carrier (20) comprising data related to the at least one data carrier (40) or related to a user of the at least one data carrier (40);
- defining such access rights for the at least one data carrier (40); and
- sending the access rights defined for the at least one data carrier to the at least one data carrier (40).

10. The method of claims 2 and 9, wherein the step of providing digital data containing at least one image (50) including the access-based resource (10) comprises the step of uploading at the server (30) the at least one image (50) including the access-based resource (10) by the another data carrier (20).

11. An access control server (30) for facilitating location of an access-based resource (10) to at least one data carrier (40), the access-based resource (10) being configured to grant access to a physical space within a building upon validation of access rights, the access control server (30) comprising:

- means for defining access rights for the at least one data carrier (40), the access rights being readable by the access-based resource (10);
- means for providing the at least one data carrier (40) with the access rights, so that the access to the physical space can be granted to the at least one data carrier (40) upon validation of the access rights; and
- means for providing the at least one data carrier (40) with digital data containing at least one image (50) containing the access-based resource (10).

12. The access control server (30) of claim 11, further comprising:

- means for receiving a request of delegation of access rights from another data carrier (20); the request of delegation of access rights from the another data carrier (20) comprising data related to the at least one data carrier (40) or related to a user of the at least one data carrier (40).

13. The access control server (30) of claim 12, which further comprises communication means with the another data carrier, configured for receiving the at least one image containing the access-based resource (10).

14. The method of any of claims 1-9 or the access control server (30) of any of claims 10-13, wherein the access rights are defined for the at least data carrier (40) for a predetermined period of time.

15. Method of any of claims 1-10 or 14 performed by an access control server of any of claims 11-14.

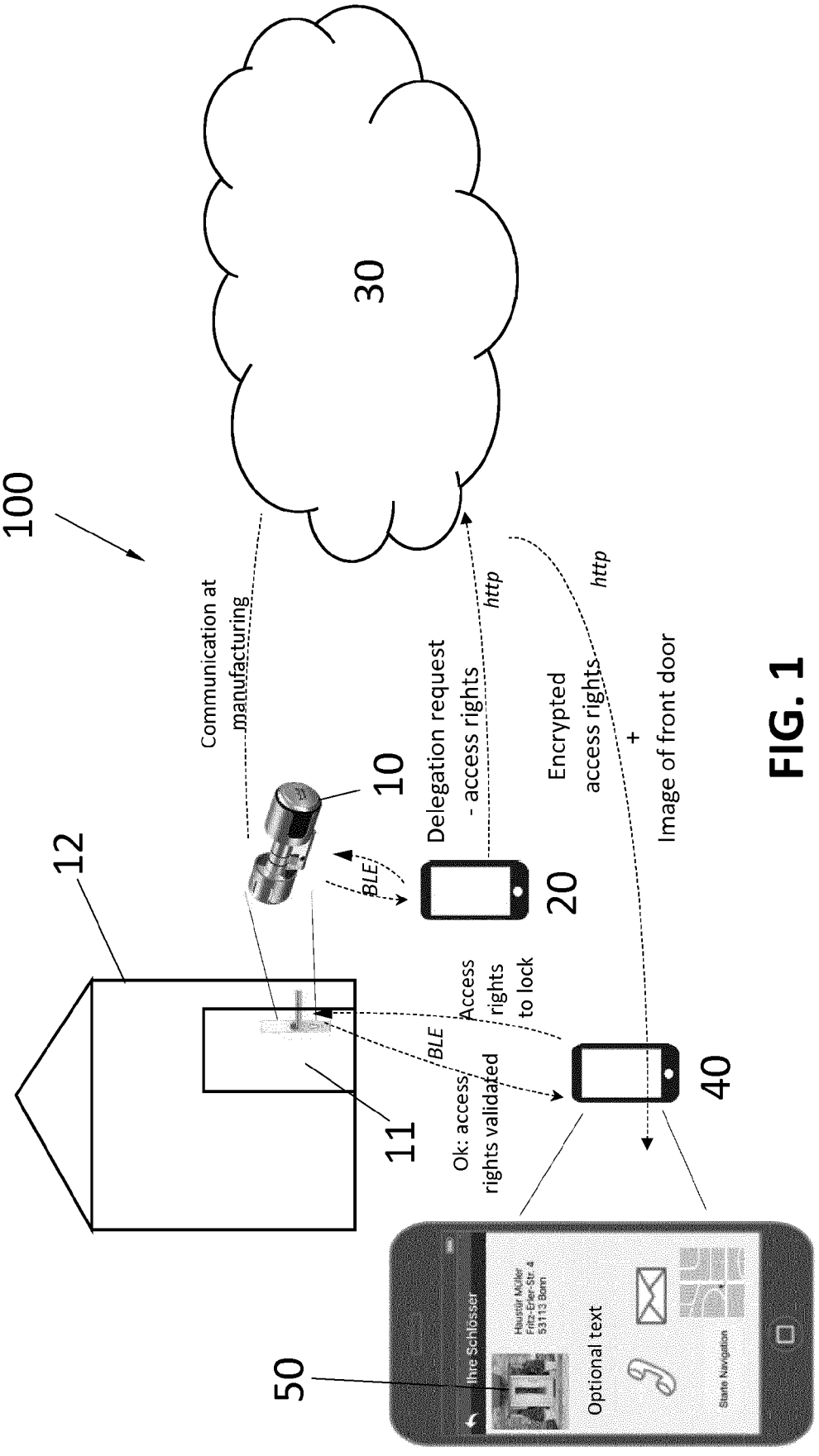
100
30
Communication at manufacturing
http
Delegation request - access rights
http
Encrypted access rights + Image of front door
10
12
BLE
20
Access rights to lock
BLE
Ok: access rights validated
11
40
50
Ihre Schlösser
Optional text
Starte Navigation

FIG. 1

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 17 15 4715

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 2014/239647 A1 (JADALLAH SAMIR [US] ET AL) 28 August 2014 (2014-08-28) * paragraphs [0110], [0117], [0123], [0128] - [0132], [0146], [0156]; figure 14 * * paragraph [0170]; figure 20 * * paragraphs [0097], [0125], [0136] - [0143]; figure 15 *	1-4,6-15	INV. G07C9/00 ADD. G01C21/36
X	US 2016/180618 A1 (HO HARVEY [US] ET AL) 23 June 2016 (2016-06-23) * paragraphs [0093], [0094], [0097], [0098], [0100], [0149] - [0153]; figures 5, 8 *	1-4,6-9, 11,12, 14,15	
A	US 2014/236468 A1 (DAVE SWAPNIL R [US] ET AL) 21 August 2014 (2014-08-21) * paragraphs [0054], [0080] - [0082] *	1-4,6, 10,13	
A	EP 2 085 934 A1 (FORBRUGER KONTAKT DISTRIB AS [DK]; BLADKOMPAGNIET AS [DE]) 5 August 2009 (2009-08-05) * abstract * * paragraphs [0009], [0029], [0030], [0048], [0051], [0052] * * column 10, line 1 - line 6 * * column 17, line 43 - line 49; claim 11 *	1,7-9, 11,12, 14,15	TECHNICAL FIELDS SEARCHED (IPC) G07C G01C E05B G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	13 July 2017	Verhoof, Paul

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 17 15 4715

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.

13-07-2017

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014239647 A1	28-08-2014	AU 2014224065 A1	17-09-2015
		CA 2902446 A1	04-09-2014
		CN 105339573 A	17-02-2016
		EP 2961903 A1	06-01-2016
		US 2014239647 A1	28-08-2014
		WO 2014134563 A1	04-09-2014
US 2016180618 A1	23-06-2016	NONE	
US 2014236468 A1	21-08-2014	NONE	
EP 2085934 A1	05-08-2009	DK 2085934 T3	21-10-2013
		EP 2085934 A1	05-08-2009

EPO FORM P0459

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