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

(11) **EP 4 332 920 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
06.03.2024 Bulletin 2024/10

(21) Application number: **22192916.9**

(22) Date of filing: **30.08.2022**

(51) International Patent Classification (IPC):
G07C 9/00 *(2020.01)*

(52) Cooperative Patent Classification (CPC):
G07C 9/00309; G07C 9/00571; G07C 9/00817; G07C 9/00857; G07C 9/00904; G07C 2209/02; G07C 2209/04

(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:
KH MA MD TN

(71) Applicant: **dormakaba Schweiz AG**
8623 Wetzikon (CH)

(72) Inventors:
- **Kleger, Robert**
  Rümlang (CH)
- **Spoerri, Jacqueline**
  Rümlang (CH)
- **Sumi, Philipp**
  Rümlang (CH)

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

(54) **METHODS AND DEVICES FOR MANAGING ACCESS FOR A MANAGED RESIDENTIAL BUILDING**

(57) The present disclosure relates to a method of managing access for a managed residential building (2; 3) as well as to devices for managing access for a managed residential building (2; 3). Specifically, the present disclosure relates to a computer-implemented method of managing access for a managed residential building (2; 3), having one or more common door(s) (4; 5; 6; 9) including an electronic lock, and at least one private door (7; 8), wherein the common door(s) (4; 5; 6; 9) control(s) access to a common area (10; 11; 12; 13) of the managed residential building (2; 3), and the at least one private door (7; 8) controls access to a private area (14; 15) allocated to a first person (23) according to a rental agreement information, wherein the first person (23) initially, at a starting point in time , does not yet have any electronic access rights for the common area (10; 11; 12; 13) of the managed residential building (2; 3). Moreover, the invention relates to a data processing apparatus (17), and a lock apparatus (16), and a mobile device (19), each configured to at least partially perform said method. Moreover, the present disclosure relates to a computer program product for execution of said method on a data processing apparatus (17).

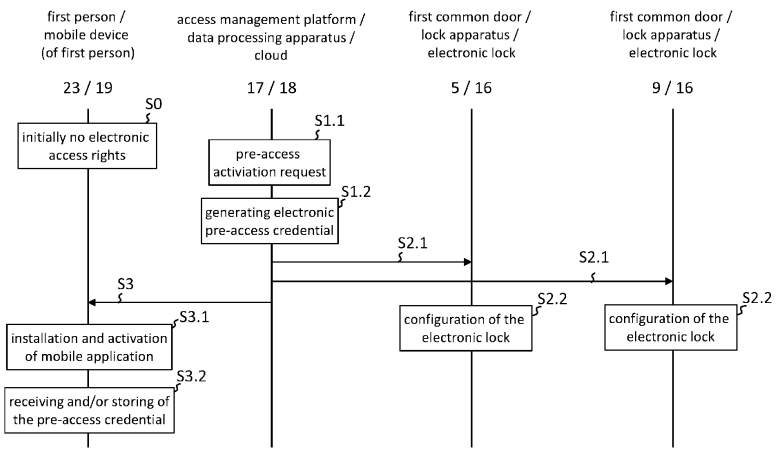

Fig. 3

EP 4 332 920 A1

Description

[0001] The present disclosure relates to a method of managing access for a managed residential building as well as to devices for managing access for a managed residential building. Specifically, the present disclosure relates to a computer-implemented method of managing access for a managed residential building, further to a data processing apparatus, and a lock apparatus, and a mobile device, each configured to at least partially perform said method. Moreover, the present disclosure relates to a computer program product for execution of said method on a data processing apparatus.

[0002] Computer-implemented methods of managing access for a managed residential building, and respective devices, are known with respect to managing electronic locks of private doors and common doors in a managed residential building. For example, a system of the present applicant is known, the system being called Resivo. Within an access management platform, the so-called Resivo Admin Portal, managers or administrators of managed residential buildings can assign access rights to certain persons, for example when a rental agreement of new tenants starts. Thereby, the complexity of change of tenants, for example with respect to apartment handovers, is reduced. No time-consuming key management is necessary since a fully digital access management is possible with no physical keys anymore, but with the help of digital keys using credentials that, when being presented to an electronic lock, allow the entrance through the respective door including the electronic lock.

[0003] However, according to the known system, it is necessary that a person to be granted access to the managed residential building always needs to have a private area (such as an apartment) assigned before a transmission of credentials to the possession of the person can take place. Accordingly, the known system's flexibility is limited in the sense that the person can only be granted access to both, a private door (or several private doors) as well as a common door (or several common doors), at the same time.

[0004] Nevertheless, there are situations when a manager or an administrator would like to give permission to a future tenant to already be able to enter the managed residential building in terms of being able to enter common areas of the managed residential building already, however, without being able to enter the private area (such as the apartment) yet. For example, this is of interest when the official starting date of the rental agreement has not arrived yet but, nevertheless, the tenant should be able to enter already a common area such as a garage or such even before the start of the rental agreement. In these cases, a time-consuming personal meeting between the manager or administrator, or for example a caretaker, usually needs to take place in order to enable the tenant to enter such common area already in advance, prior to the actual start of the rental agreement. Also, the known system is limited regarding managed residential buildings that do not yet have private doors with electronic locks. Then, the use of the described management system is not possible since electronically accessible private doors with respective credentials need to be assigned to a person if it is wished to assign to the person a credential (digital key) for a common door.

[0005] In view of the aforementioned, it is an object of the present invention to provide an improved computer-implemented method of managing access for a managed residential building, as well as to provide an improved respective data processing apparatus, by means of which a more flexible access management of new tenants is made possible. In addition, it is an object of the present invention to provide an improved lock apparatus, as well as an improved mobile device, as well as an improved computer program product, by means of which a more flexible access management of new tenants is supported.

[0006] According to the present disclosure, these objects are achieved through the features of the independent claims. In addition, further advantageous embodiments follow from the dependent claims and the description.

[0007] In detail, the above-mentioned object of a more flexible access management of new tenants is achieved particularly, according to the present disclosure, by a computer-implemented method of managing access for a managed residential building, the managed residential building having at least one or more common door(s) including an electronic lock (each including an electronic lock), and the managed residential building having at least one private door. The suggested computer-implemented method is also applicable for managing access for several managed residential buildings, for example a managed residential area, wherein the managed residential area at least comprises a first managed residential building and a second managed residential building, or even more managed residential buildings. According to the suggested computer-implemented method, the common door controls (or the common doors control) access to a common area of the managed residential building, and the at least one private door controls access to a private area allocated to a first person according to a rental agreement information. In case of several common doors, each common door could provide an entrance to a specific individual common area, for example a first common door to a first common area and a second common door to a different second common area, or several common doors could also provide an entrance to the same common area, such as a shared common area (for example a single room or a single common area that can be entered through the several common doors at two different points). According to the suggested computer-implemented method, the first person initially, at a starting point in time, does not yet have any electronic access rights for the common area of the managed residential building. In particular, the first person initially does not

yet have any electronic access rights for the managed residential buildings, thereby not being able to enter electronically the managed residential buildings at all. Furthermore, it could be the case that, in particular, the first person initially does not yet have any access rights for the managed residential buildings, thereby not being able to enter the managed residential buildings at all. The suggested computer-implemented method is being performed by an access management platform and comprises at least the following steps:

receiving a pre-access activation request to assign an electronic pre-access credential to the first person, wherein the electronic pre-access credential grants the first person, at a pre-access point in time, only the right to open the common door (the common doors) for accessing the common area; and

generating the electronic pre-access credential associated with an identifier of the first person; and

transmitting the electronic pre-access credential to the electronic lock of the common door (of the common doors), thereby, at the pre-access point in time, configuring the electronic lock of the common door (each electronic lock of the common doors) to unlock if the electronic pre-access credential is provided by a mobile device of the first person; and

sending an application-installation invitation to the mobile device of the first person, thereby enabling the first person to install and activate a mobile application through which the electronic pre-access credential is receivable and/or storable.

[0008] With respect to a data processing apparatus, the above-mentioned object is achieved by a suggested data processing apparatus configured to perform the suggested computer-implemented method as described before or hereinafter (for example according to any one of the claims 1 to 11). The suggested data processing apparatus comprises the access management platform or is configured to communicate with the access management platform.

[0009] An essential advantage of the present invention is that a higher flexibility is gained when managing a single or a plurality of managed residential buildings due to a management process being applicable to several different situations. The reason is that a new tenant who shall enter the building according to his rental agreement does not have to be allocated with a private door including an electronic lock anymore in order to receive a permission to enter common doors. Due to the fact that a single access right only with respect to common doors can be granted to the first person, the first person does not have to be given overall permissions (including for example the permission to enter electronically controlled private doors as well) for being able to enter the managed residential building at all. Hence, in a situation where the managed residential building simply has electronic locks in connection with common doors, but no electronic locks (at least no electronic locks according to the same manageable system) in connection with private doors, the access management platform can be used to provide the first person with the exclusive access right of only being able to unlock common doors. Accordingly, the first person as a new tenant can easily be given automatically and from a distance the right to be able to enter the managed residential building. Advantageously, even in the case that private doors and common doors include electronic locks and are manageable via the access management platform, the present invention can facilitate the management process in that a permission to enter, at the pre-access point in time, is only given to the first person with respect to the common doors whereas the private door or doors are not accessible yet. Thereby, the first person could already enter the managed residential building but not yet its private area. This can be of interest during a time after having signed a rental agreement but before the beginning of the contract period, for example even while previous tenants are still living in the later-rented private area.

[0010] The features and advantages described above and below in the context of the suggested computer-implemented method being performed by an access management platform (for example according to any one of the claims 1 to 11) can be transferred in an appropriate manner to the suggested data processing apparatus (for example according to claim 12). In particular, the computer-implemented method can be configured to be performed by the suggested and described data processing apparatus. The suggested and described data processing apparatus is in turn preferably configured to execute the suggested computer-implemented method. In this respect, the features and specific advantages relating to the suggested data processing apparatus or the respective suggested computer-implemented method are regularly described collectively only once. Features described in connection with the computer-implemented method can be included accordingly in an appropriate manner in claims relating to the data processing apparatus and vice versa.

[0011] By way of example, also several private doors either controlling access to one private area, such as several doors providing entrance to one apartment, or controlling access to several private areas (such as for example two different apartments on different floors or to an apartment and a personal garage) can be provided and allocated to the first person according to the rental agreement information. Furthermore, also several common areas might exist, such as the hall of the building with the common door in terms of the main entrance door and additionally a garage with a separate common door and additionally a fitness room with another common door. The access rights might be granted to the first person with respect to all common doors or only with respect

to a selection of common doors, as well as (at the later full-access point in time) with respect to all private doors or only with respect to a selection of private doors.

[0012] In particular, the access management platform is an online web application, moreover in particular not a mobile application. For example, the Resivo Admin Portal of the applicant can be used as access management platform.

[0013] In particular, the pre-access activation request can be entered in the access management platform, for example by a manager managing the relevant rental agreement information.

[0014] In particular, by generating the electronic pre-access credential (and later optionally the electronic full-access credential) associated with an identifier of the first person, an unambiguous allocation of credentials to the identity of a person (the tenants) can be achieved.

[0015] In particular, the application-installation invitation can be sent to the mobile device of the first person via e-mail communication. Particularly, the e-mail then has the invitation link with the help of which the mobile application can be installed by the first person on its mobile device. The mobile application for example can be the Resivo Home App of the applicant. Advantageously, when installing the mobile application, the first person automatically can also have stored the the electronic pre-access credential (and optionally the electronic full-access credential) on its mobile device within said mobile application.

[0016] In an embodiment, the at least one private door includes an electronic lock.

[0017] In an embodiment, the computer-implemented method further comprises at least the following steps:

receiving a full-access activation request to assign an electronic full-access credential to the first person, wherein the electronic full-access credential grants the first person the right to open the common door (doors) for accessing the common area and the right to open the at least one private door for accessing the at least one private area;

generating the electronic full-access credential associated with the identifier of the first person;

transmitting the electronic full-access credential to the electronic lock of the common door (doors) and to the electronic lock of the first person's private door, thereby, at a full-access point in time after the pre-access point in time, configuring the electronic locks (of the common door(s) and the private door(s)) to unlock if the electronic full-access credential is provided by a mobile device of the first person;

sending the electronic full-access credential to the mobile device of the first person using the mobile application installed thereon.

[0018] Advantageously, the first person, after already being able to enter common areas, then can be given the permission to also enter the private area.

[0019] In an embodiment, the computer-implemented method further comprises at least the following step:
transmitting the electronic pre-access credential also to the electronic lock of the first person's private door, thereby, at a full-access point in time after the pre-access point in time, configuring also the electronic lock of the first person's private door to unlock if the electronic pre-access credential is provided by the mobile device of the first person.

[0020] Advantageously, with the use of the same credential, the first person then can be allowed to enter not only the common area but also the private area.

[0021] Preferably, in an embodiment, before the step of transmitting the electronic pre-access credential also to the electronic lock of the first person's private door, the following step is performed:
receiving an extension for full-access request to adapt the electronic pre-access credential for the first person, thereby initiating the granting process of the right to open additionally to the first common door (doors) also the at least one private door.

[0022] Advantageously, within the access management platform, the extension of the access rights for the first person for being able to also enter private areas after already being able to enter common areas needs to be actively performed by, for example, a manager.

[0023] In an embodiment, the computer-implemented method further comprises at least the following step:
predefining the pre-access point in time (and/or predefining the full-access point in time) under a predetermined condition related to the rental agreement information, in particular according to a date of a start of a rental agreement, and/or in particular according to a confirmation of payment, for example a confirmation of payment of a rent and/or of a deposit.

[0024] Advantageously, via the predefinition of the pre-access point in time, the manager can control in advance within the access management platform, from which point of time on an access should be possible. Moreover preferably, an additional point of time, via the predefined full-access point in time, can be determined as to when the first person (tenant) can also additionally enter its private area. Advantageously, these point of times, from which on an access to certain areas is possible, can be made dependent on pre-conditions, such as if the tenant has paid a deposit or as when the actual rental agreement will start. Additionally or alternatively, the definition of point of times can be made within the access management platform already at the beginning.

[0025] In an embodiment, the electronic lock) is (or the electronic locks are) configured to communicate via a communication network with the access management platform, preferably reciprocally.

[0026] In an embodiment, the computer-implemented method further comprises at least the following steps:

storing the electronic pre-access credential and/or storing the electronic full-access credential in an access management platform whitelist; and

verifying if a used electronic pre-access credential, and/or verifying if a used electronic full-access credential, being transmitted from the electronic lock (locks), corresponds (correspond) to the electronic pre-access credential (and/or the electronic full-access credential) stored in the access management platform whitelist;

wherein the step of transmitting the pre-access credential (and/or transmitting the electronic full-access credential) to the electronic lock(s) and configuring the electronic lock(s) only is executed if the step of verification is positive.

[0027] Advantageously, the credential(s) can be stored preferably only online within the access management platform, thereby guaranteeing a high level of security. Credential(s) within the whitelist online, can then be credential(s) who have access to the respective common area (or even private area). In case the credential(s) is (are) not stored within the lock(s), then a fraudulent use in terms of trying to get possession of the credential(s) by accessing the lock(s) can be made relevantly more difficult.

[0028] In an embodiment, the computer-implemented method further comprises at least the following steps:

receiving entrance execution data via the communication network from the electronic lock(s), and/or receiving entrance execution data via a communication network from the mobile application; and

storing the entrance execution data, the entrance execution data comprising:

a time of entrance information about when the electronic lock(s) is or has been opened (are or have been opened); and/or

a user information about which electronic pre-access credential (and/or which electronic full-access credential) is or has been used (are or have been used) to open the electronic lock(s); and/or

a medium information about which mobile device and/or about which mobile application is or has been used (are or have been used) to open the electronic lock(s).

[0029] Advantageously, a control of the uses of the doors, for example as to who is opening doors when and by which medium, can be provided, thereby for example being able to draw conclusion when something extraordinary happened in common areas. For example, a damage in a common area or even with respect of a common door, which possibly could have been caused by a plurality of persons (tenants) could be better analysed with respect to a potential person responsible for the damage. In case a communication network between the mobile application and the access management platform is used, then it could be a different or even the same communication network, as being used between the access management platform and the electronic lock(s).

[0030] In an embodiment, the step of transmitting the pre-access credential and/or the step of transmitting the electronic full-access credential to the electronic lock(s) is executed via a direct communication via the communication network.

[0031] Advantageously, online doors or locks can be provided enabling a communication via the communication network.

[0032] In an embodiment, the step of transmitting the pre-access credential and/or the step of transmitting the electronic full-access credential to the electronic lock(s) is executed via an indirect communication by the step of: transmitting, at a first point in time, the pre-access credential (and/or the electronic full-access credential) to a manager's mobile device, in particular of a caretaker, thereby leading to a necessity of transmitting, at a second point in time after the first point in time, the pre-access credential (and/or the electronic full-access credential) from the manager's mobile device to the electronic lock(s).

[0033] Advantageously, even offline doors or locks can be used according to the suggested method. In particular, the manager or caretaker could use a management app, such as a so-called utility app, which is not available for the tenants (first person). The manager or caretaker then could provide the credential(s) to the lock(s) so that no direct online connection between the access management platform and the respective lock(s) would be needed for this step.

[0034] In an embodiment, the pre-access credential and/or the electronic full-access credential is (are) encrypted, preferably using asymmetric encryption.

[0035] An example for the asymmetric encryption is the Elliptic Curve Cryptography. Advantageously, the credential(s) is (are) configured as being not readable by the mobile device (or the mobile application) of the first person, but being only readable by the electronic lock(s) and/or the access management platform. In particular, especially with respect to the suggested systems and methods, the credential(s) is (are) transmitted in encrypted form from the access management platform to the mobile device (in particular the mobile application). The credential(s) also remain(s) stored in an encrypted manner on the mobile device. The credential(s) is (are) then also transmitted in encrypted form to the electronic lock at the moment of intention of access. Only at the electronic look, the credential(s) then is (are) decrypted in order to make the access decision by the verifying step.

[0036] In an embodiment, the computer-implemented

method further comprises the step of deactivating the right to open the common door(s) and/or to open the at least one private door, preferably by:

deleting the electronic pre-access credential and/or the electronic full-access credential from a whitelist; and/or

storing the electronic pre-access credential and/or the electronic full-access credential on a blacklist, wherein the blacklist is assigned with priority in comparison to the whitelist; and/or

transmitting the electronic pre-access credential and/or the electronic full-access credential to the electronic lock of the common door(s) and/or of the at least one private door, thereby configuring the electronic lock(s) not to unlock anymore if the electronic pre-access credential and/or the electronic full-access credential is provided by the mobile device of the first person.

[0037] Advantageously, in case of a lost or stolen mobile device of the first person with the credential(s) being stored thereon or in case of wishing not to grant access anymore to the first person, the suggested method guarantees a simple and fast way of adapting the access rights by invalidating previous access right.

[0038] With respect to a lock apparatus, the above-mentioned object is achieved by a suggested lock apparatus configured to at least partially perform the suggested computer-implemented method as described before or hereinafter (for example according to any one of the claims 1 to 11), when interacting with the access management platform or when interacting with the suggested data processing apparatus. The suggested lock apparatus comprises the electronic lock and is configured to lock and unlock the common door.

[0039] In addition, according to an independent aspect of the invention, a method of managing access for a managed residential building is suggested, the managed residential building having at least a common door including an electronic lock or having several common doors each including an electronic lock, and the managed residential building having at least one private door, the common door controls (or, respectively, the common doors control) access to a common area of the managed residential building, and the at least one private door controls access to a private area allocated to a first person according to a rental agreement information, wherein the first person initially, at a starting point in time, does not yet have any electronic access rights for the common area of the managed residential building, the method being performed by a lock apparatus and comprising at least the following steps:

receiving an electronic pre-access credential of the first person, wherein the electronic pre-access credential grants the first person, at a pre-access point in time, only the right to open the common door(s) for accessing the common area;

configuring the electronic lock of the common door(s) to unlock if the electronic pre-access credential is provided by a mobile device of the first person.

[0040] In addition, according to an independent aspect of the invention, a lock apparatus is suggested, configured to at least partially perform the suggested method of managing access for a managed residential building being performed by a lock apparatus as described before or hereinafter, wherein the lock apparatus comprises the electronic lock and is configured to lock and unlock the common door.

[0041] The features and advantages described above and below in the context of the suggested method being performed by a lock apparatus can be transferred in an appropriate manner to the suggested lock apparatus. In particular, the method can be configured to be performed by the suggested and described lock apparatus. The suggested and described lock apparatus is in turn preferably configured to execute the suggested method. In this respect, the features and specific advantages relating to the suggested lock apparatus or the respective suggested method are regularly described collectively only once. Features described in connection with the method can be included accordingly in an appropriate manner in claims relating to the lock apparatus and vice versa.

[0042] In an embodiment, the lock apparatus comprises a whitelist for storing the electronic pre-access credential and/or the electronic full-access credential. In an embodiment of the method being performed by a lock apparatus, the method further comprises the step of storing the electronic pre-access credential and/or the electronic full-access credential in a whitelist.

[0043] Advantageously, the credential(s) can be stored, after being transmitted to the electronic lock, in said whitelist, thereby the whitelist being responsible for keeping all the credential(s) granting persons the right to open the respective door(s). Storing can advantageously take place offline.

[0044] In addition, according to an independent aspect of the invention, a system is suggested, comprising the suggested data processing apparatus as described before or hereinafter (for example according to claim 12), and the suggested lock apparatus as described before or hereinafter, the data processing apparatus and the lock apparatus being in interactive connection with each other, preferably thereby performing the suggested computer-implemented method being performed by a access management platform as described before or hereinafter (for example according to any one of the claims 1 to 11), and/or preferably thereby performing the suggested method being performed by a lock apparatus as described before or hereinafter.

[0045] With respect to a mobile device, the above-

mentioned object is achieved by a suggested mobile device configured to at least partially perform the suggested computer-implemented method as described before or hereinafter (for example according to any one of the claims 1 to 11), when interacting with the access management platform or when interacting with the suggested data processing apparatus. The suggested mobile device comprises the mobile application having stored the electronic pre-access credential.

[0046] In addition, according to an independent aspect of the invention, a computer-implemented method of managing access for a managed residential building is suggested, the managed residential building having at least a common door including an electronic lock or having several common doors each including an electronic lock, and the managed residential building having at least one private door, the common door controls (or, respectively, the common doors control) access to a common area of the managed residential building, and the at least one private door controls access to a private area allocated to a first person according to a rental agreement information, wherein the first person initially, at a starting point in time, does not yet have any electronic access rights for the common area of the managed residential building, the method being performed by a mobile device and comprising at least the following steps:

receiving an application-installation invitation;

installing and activating a mobile application;

receiving and/or storing, through the mobile application, an electronic pre-access credential for the first person, wherein the electronic pre-access credential grants the first person, at a pre-access point in time, only the right to open the common door(s) for accessing the common area when being provided to the electronic lock of the common door(s).

[0047] In addition, according to an independent aspect of the invention, a mobile device is suggested, configured to at least partially perform the suggested computer-implemented method of managing access for a managed residential building being performed by a mobile device as described before or hereinafter, wherein the mobile device comprises the mobile application having stored the electronic pre-access credential.

[0048] The features and advantages described above and below in the context of the suggested computer-implemented method being performed by a mobile device can be transferred in an appropriate manner to the suggested mobile device. In particular, the computer-implemented method can be configured to be performed by the suggested and described mobile device. The suggested and described mobile device is in turn preferably configured to execute the suggested computer-implemented method. In this respect, the features and specific advantages relating to the suggested mobile device or the respective suggested computer-implemented method are regularly described collectively only once. Features described in connection with the computer-implemented method can be included accordingly in an appropriate manner in claims relating to the mobile device and vice versa.

[0049] In an embodiment of the mobile device and/or of the lock apparatus, the mobile device and/or the lock apparatus comprise a wireless communication interface, preferably a short range communication interface, the wireless communication interface of the lock apparatus being configured to receive the electronic pre-access credential and/or the electronic full-access credential, preferably being sent from the mobile application; the wireless communication interface of the mobile device being configured to send the electronic pre-access credential and/or the electronic full-access credential, preferably to the lock apparatus or the electronic lock. In an embodiment of the method being performed by a lock apparatus or of the computer-implemented method being performed mobile device, the method, correspondingly, further comprises the step of receiving or sending the electronic pre-access credential and/or the electronic full-access credential via a wireless communication interface, preferably a short range communication interface. In particular, the wireless communication interface performs steps of sending and/or receiving the personal access right identifier via bluetooth low energy (BLE) technology. Advantageously, common mobile devices of the tenants, with bluetooth technology, can be used to unlock and lock door(s), preferably with the help of the mobile application. Preferably. the wireless communication interface of the lock apparatus is configured to process a via bluetooth low energy (BLE) technology received signal further in a following verifying step only if a predetermined threshold value of a signal strength, in particular of a received signal strength indicator (RSSI), is reached. Further preferably, the predetermined threshold value of a signal strength can be adapted, in particular via the access management platform. Advantageously, bluetooth technology can be used for the entrance into respective doors. However, due to the fact that different mobile devices (or even the same type of mobile devices) generate bluetooth signals of different strengths, a threshold value can be used to adapt the proximity of the used mobile device to the electronic lock, thereby avoiding opening unwished doors if any what so low signal strength were sufficient to initiate a verifying step of the transmitted credential(s) in the electronic lock. Advantageously, the threshold value can be even made dependent on the type of mobile device used and can be adapted, for example in the access management platform.

[0050] In addition, according to an independent aspect of the invention, a system is suggested, comprising the suggested data processing apparatus as described before or hereinafter (for example according to claim 12), and the suggested mobile device as described before or hereinafter, the data processing apparatus and the mo-

bile device being in interactive connection with each other, preferably thereby performing the suggested computer-implemented method being performed by a access management platform as described before or hereinafter (for example according to any one of the claims 1 to 11), and/or preferably thereby performing the suggested computer-implemented method being performed by a mobile device as described before or hereinafter.

[0051] In addition, according to an independent aspect of the invention, a system is suggested, comprising the suggested mobile device as described before or hereinafter, and the suggested lock apparatus as described before or hereinafter, the mobile device and the lock apparatus being in interactive connection with each other, preferably thereby performing the suggested computer-implemented method being performed by a mobile device as described before or hereinafter, and/or preferably thereby performing the suggested method being performed by a lock apparatus as described before or hereinafter.

[0052] With respect to a computer program product, the above-mentioned object is achieved by a suggested computer program product comprising commands which, when the computer program product is executed by a processor of a data processing apparatus, preferably of the suggested data processing apparatus, cause the data processing apparatus to perform the steps of the suggested computer-implemented method performed by the access management platform as described before or hereinafter (for example according to any one of the claims 1 to 11).

[0053] In addition, according to an independent aspect of the invention, a computer-readable medium is suggested, on which the suggested computer program product as described before or hereinafter is stored.

[0054] In addition, according to an independent aspect of the invention, a system is suggested, comprising the suggested data processing apparatus as described before or hereinafter, the suggested lock apparatus as described before or hereinafter, and the suggested mobile device as described before or hereinafter, the data processing apparatus, the lock apparatus, and the mobile device being in interactive connection with each other, preferably thereby performing the suggested computer-implemented method being performed by a access management platform as described before or hereinafter (for example according to any one of the claims 1 to 11), and/or preferably thereby performing the suggested method being performed by a lock apparatus as described before or hereinafter, and/or preferably thereby performing the suggested computer-implemented method being performed by a mobile device as described before or hereinafter.

[0055] In an embodiment, the data processing apparatus or the lock apparatus comprise a blacklist for storing the electronic pre-access credential and/or the electronic full-access credential. In an embodiment of the computer-implemented method being performed by the access management platform or of the method being performed by a lock apparatus, the method further comprises the step of storing the electronic pre-access credential and/or the electronic full-access credential in a blacklist. Advantageously, a blacklist can be used to overrule the entries within a whitelist, thereby causing that a credential (credentials) listed in the blacklist does not have the access right to open the respective lock anymore. Writing a credential (credentials) into a blacklist can be a way of the before-described deactivating of a credential.

[0056] In general, the suggested methods for managing access for a managed residential building are also applicable for managing access for several managed residential buildings, for example a managed residential area, as described with respect to the suggested computer-implemented method being performed by an access management platform. Furthermore, the explanations with respect to said suggested computer-implemented method being performed by an access management platform which explanations deal with the use of several common doors or, respectively, deal with initially non-existing access rights of the first person also apply to the further presented suggested methods for managing access for a managed residential building.

[0057] The present disclosure will be explained in more detail, by way of an example, with reference to the drawings in which:

Figure 1: shows a schematic view of a managed residential area, including managed residential buildings;

Figure 2: shows a block diagram illustrating schematically a system of managing access for the managed residential building;

Figure 3: shows a block diagram illustrating schematically an exemplary sequence of steps for managing the access for the managed residential building;

Figure 4: shows a block diagram illustrating schematically an exemplary sequence of the steps of additionally assigning a full-access;

Figure 5: shows a block diagram illustrating schematically an exemplary sequence of the steps of additionally assigning a full-access, as an alternative to Fig. 4; and

Figure 6: shows a block diagram illustrating schematically several exemplary steps of the suggested methods.

[0058] Figure 1 schematically shows a managed residential area 1. The managed residential area 1 comprises in this example two managed residential buildings 2 and 3. The managed residential area 1 may be a private

site on which the two managed residential buildings 2 and 3 are located, the private site having an entrance in the form of a common door 4, for example an access gate to the private site. The managed residential buildings 2 and 3 are managed for example by an owner or an administrator and the managed residential buildings 2 and 3 for example have apartments for being rented to private persons.

[0059] In addition to the common door 4 for entering the general area of the private site, there are two further common doors 5 and 6 as main entrance doors to the respective managed residential buildings 2 or 3. Moreover, in the depicted scenery, there are also two private doors 7 and 8, which are the entrances to private rooms such as apartments of tenants indicated by dashed lines and being located within the managed residential building 2. Furthermore, within the managed residential building 2, another common door 9 is present, which is the entrance to another general room represented by the dashed lines below and being accessible not only for one person (tenant) but for different persons (different tenants) within the managed residential building 2. In general, the common doors 4, 5, 6, and 9 control access to common areas 10, 11, 12, and 13 whereas the private doors 7 and 8 control access to private areas 14 and 15.

[0060] In the depicted scenery, by way of an example, it is assumed that all the doors include electronic locks. However, for the suggested method, it could be the case that only one or several common door(s) 4, 5, 6, and/or 9 include(s) (an) electronic lock(s) wherein the private door(s) does (do) not have (an) electronic lock(s).

[0061] By way of an example, the common area 10 could be the private site, such as a secured area, of the owner of the managed residential area 1, and the common area 10 should accordingly be accessible to all tenants. The first managed residential building 2 could have the common area 11 in terms of the entry hall of the building, as well as an additional common area 13 in terms a fitness room. Furthermore, the second managed residential building 3 could have the common area 12, being the entire building itself, in terms of a garage. Additionally, the two private rooms 14 and 15 could be two different private apartments, one for a first person in terms of a first tenant and the other one for another tenant. In the described scenery, both tenants should receive access rights to the common areas 10 and 11 whereas the common areas 12 and 13 could be individually allocated according to the rental agreements as well as the private area 14 is allocated to one tenant and the private area 15 to the other tenant. In such a scenery, the suggested methods, devices and systems could apply for only the managed residential building 2, which at least has a common area 11 or 13 and a private area 14 or 15. Also, the suggested methods, devices and systems could apply for both managed residential buildings 2 and 3 together (as common doors 5, 6, and 9, as well as private doors 7, and 8 are present as well). Also, the suggested methods, devices and systems could apply for the entire managed residential are 1, including managed residential buildings 2 and 3.

[0062] The suggested methods, devices and systems provide advantages for example when a change of tenant takes place and is to be managed with regard to giving the tenants the permission from a distance to enter common areas 10, 11, 12, 13 and/or private areas 14, 15. In particular, with the help of the suggested methods, devices and systems, it is possible to give an access right to a first person, at least initially, only with respect to one or several common door(s) 4, 5, 6, 9, even if the private area 14 and/or 15 remains non-accessible for the first person yet. This could be of interest in cases when a new tenant should be given permission to enter common areas 10, 11, 12, or 13 already even if the official start of the rental agreement has not started yet, resulting in the fact that the owner does not want to give to the first person access rights with regard to the rented private area 14 and/or 15. It could be also the case that the official date of the rental agreement has started already but the deposit has not been paid yet by the first person or another requirement has not fulfilled yet, and, accordingly, the owner does not want to give a permission to the first person yet to enter the private area 14 and/or 15. Another use case is that the managed residential building 2 itself only comprises electronic locks with respect to the common doors 5 and/or 9, but not with respect to at least the rented private area 14 or 15 and its respective private door 7 or 8.

[0063] Figure 2 schematically shows a system of managing access for the managed residential building 2. For the sake of a better view, the private door 8 is left out in the illustration according to Figure 2. However, within the depicted managed residential building 2 (depicted with the help of a dashed box), the three doors in terms of the common doors 5 and 9, as well as the private door 7 are depicted, each door 5, 7 and 9 comprising a lock apparatus 16 including an electronic lock. The suggested system and especially the suggested computer-implemented method could also work and has the described advantages if the private door 7 did not have an electronic lock but a solely mechanic lock.

[0064] The managed residential building 2 is in the possession of the owner and might be managed by the owner or for example by an administrator. Said possession is schematically depicted with the help of the outer dash-dotted box. Furthermore, according to the depicted system, the owner or administrator is in control of a data processing apparatus 17, forming part of or being in interactive communication with the cloud 18. The cloud 18 or the data processing apparatus 17 comprises an access management platform, with the help of which platform the computer-implemented method of managing access for the managed residential building 2 can be performed. An example for such access management platform is the -called Resivo Admin Portal as a web application of the recent applicant dormakaba.

[0065] Within the possession of a first person, herein-

after also referred to a new tenant, a mobile device 19 is depicted as well. With the help of the mobile device 19, in particular with a mobile application installed thereon, the new tenant is able to open the common doors 5 and 9, and, at a later point of time, the private door 7 to his/her apartment as well, when given the respective permission. An example for such mobile application is the so-called Resivo Home App of the recent applicant dormakaba.

[0066] The data processing apparatus 17 is configured to communicate via a communication network 20 with the lock apparatuses 16 of the common doors 5 and 9 (indicated by the double arrow), and furthermore optionally with the lock apparatus 16 of the private door 7 (indicated by the dashed double arrow) by another communication network or, as depicted, by the same communication network 20. Moreover, the data processing apparatus 17 is configured to communicate via a communication network 21 (which could also be the same communication network 20 as mentioned before) with the mobile device 19 of the new tenant. The connection between the data processing apparatus 17 and the mobile device 19 usually is unidirectional as depicted with the help of the single arrow, thereby allowing the data processing apparatus 21 to send information to the mobile device 19 but not allowing the mobile device 19 to initiate a communication directly with the data processing apparatus 17. Furthermore, a communication connection, namely a short range communication connection, exists between the mobile device 19 of the new tenant as well as the lock apparatuses at least of a common door 5, in the recent case, also of the common door 9 (indicated by the single arrows) and the private door 7 (indicated by the single dashed arrow).

[0067] The short range communication connections 22 are realised via bluetooth low energy technology, with the help of a bluetooth low energy transmitter module, which is integrated in the mobile device 19 of the new tenant, as well as with the help of bluetooth low energy receiver modules integrated in the lock apparatuses 16.

[0068] Accordingly, the mobile device 19 and/or the lock apparatuses 16 can comprise a wireless communication interface, preferably a short range communication interface, the wireless communication interface of the lock apparatus being configured to receive the electronic pre-access credential and/or the electronic full-access credential, preferably being sent from the mobile application; the wireless communication interface of the mobile device 19 being configured to send the electronic pre-access credential and/or the electronic full-access credential, preferably to the lock apparatuses 16 or the electronic lock. In particular, the wireless communication interface performs steps of sending and/or receiving the personal access right identifier via bluetooth low energy (BLE) technology. Advantageously, common mobile devices 19 of the tenants, with bluetooth technology, can be used to unlock and lock door(s), preferably with the help of the mobile application. Preferably. the wireless communication interface of the lock apparatus is configured to process a via bluetooth low energy (BLE) technology received signal further in a following verifying step only if a predetermined threshold value of a signal strength, in particular of a received signal strength indicator (RSSI), is reached. Further preferably, the predetermined threshold value of a signal strength can be adapted, in particular via the access management platform. Advantageously, bluetooth technology can be used for the entrance into respective doors. However, due to the fact that different mobile devices 19 (or even the same type of mobile devices) generate bluetooth signals of different strengths, a threshold value can be used to adapt the proximity of the used mobile device to the electronic lock, thereby avoiding opening unwished doors if any what so low signal strength were sufficient to initiate a verifying step of the transmitted credential(s) in the electronic lock. Advantageously, the threshold value can be even made dependent on the type of mobile device 19 used and can be adapted, for example in the access management platform.

[0069] The shown lock apparatuses 16 are configured as so-called connected or on-line devices due to the arrangement of the communication network 20, with the help of which an on-line communication, for example with the data processing apparatus 17, can take place. However, it is also possible according to the present disclosure, to realise the lock apparatuses 16 as so-called off-line or stand-alone devices. Then the necessary communication, for example, of the data processing apparatus 16 with the lock apparatuses 16 could be realised also as short range communication connection, preferably still wireless, as for example by bluetooth low energy technology as mentioned with respect to the short range communication connections 22. Then, the owner or administrator or a delegated person such as a caretaker could conduct the necessary communication between the data processing apparatus 17 and the lock apparatuses 16 in an indirect manner, for example with the help of an administrator's mobile device being able to communicate with the data processing apparatus 17, preferably on-line, as well as with the lock apparatuses 16 off-line as described. The administrator or caretaker could therefore use a different mobile application, such as the so-called Utility App of the recent applicant dormakaba (cf. Figure 6 and steps S12.1 and S12.2 later).

[0070] In general, the communication networks 20 could comprise a mobile radio network, such as GSM (Global System for Mobile Communication), UMTS (Universal Mobile Telephone System), WLAN (Wireless Local Area Network) or the like. Optionally, the communication networks 20 could also comprise a wire based network, such as provided by LAN (Local Area Network), an Ethernet connection or an USB connection or the like, and/or the Internet as preferred on-line connection medium. In general, as an alternative to the described bluetooth communication connection as the short range communication connections 22, the short range communication connections 22 could also be implemented as a ra-

dio-based communication interface, such as RFID communication interfaces (Radio Frequency Identifier), so-called NFC interfaces (Near Field Communication), optical interfaces like infrared or visual communication interfaces. Preferred however is the interface arranged as bluetooth low energy interface.

[0071] In the following paragraphs, described with more specific reference to Figures 3 to 6, possible sequences of steps performed within the methods in order to manage access rights according to the present disclosure are depicted.

[0072] Figure 3 shows a timing diagram illustrating an exemplary sequence of steps for managing the access for the managed residential building 2 for the new tenant (the first person 23). The first person initially at a starting point in time (as indicated by reference S0) does not yet have any electronic access rights for the common area 11 or 13. Then, in the access management platform, for example by an entry of an administrator, a pre-access activation request is received within step S1.1.

[0073] The pre-access activation request is done in order to assign an electronic pre-access credential to the first person 23. The electronic pre-access credential, therefore, is configured to grant the first person 23, at a pre-access point in time, only the right to open the common doors 5 and 9 for accessing the common areas 11 and 13. At a later point in time, for example the so-called full-access point in time, furthermore, an access right can be assigned to the first person 23 also being able to open the private door 7 or 8.

[0074] In step 1.2, the electronic pre-access credential associated is generated in the access management platform (or, respectively, in the data processing apparatus 17 or, respectively, in the cloud 18) with an identifier of the first person 23, thereby resulting in an unambiguous credential and electronic key for the first person 23.

[0075] In step S2.1, the electronic pre-access credential is transmitted to the electronic locks of both common doors 5 and 9. The transmitting could take place at the same time and is, according to the example depicted in Figure 2, conducted via the communication network 20. By transmitting the electronic pre-access credential, the electronic locks of the lock apparatuses 16 of the common doors 5 and 9 are configured, at the pre-access point in time, to unlock if the electronic pre-access credential is provided by the mobile device 19 of the first person 23, which configuration step is depicted by the reference S2.2.

[0076] In step S3, the access management platform (or, respectively, in the data processing apparatus 17 or, respectively, in the cloud 18) send an application-installation invitation to the mobile device 19 of the first person 23. The sending is preferably made via the communication network 20 on-line, for example via an e-mail sent to the first person 23. Within the e-mail, a link can be included, enabling the first person 23 to, by following the link, download the mobile application, such as the Reviso Home App. Thereby, the first person 23 is enabled to then install and activate within step S3.1 the mobile application. Through this mobile application, the electronic pre-access credential is receivable and storable within step S3.2. For example, the individual version of the mobile application could permit the first person 23 to automatically download and store the personal electronic pre-access credential which has before been generated in the access management platform (step S1.2).

[0077] Figure 4 shows a timing diagram illustrating an exemplary sequence of the steps of additionally giving the first person 23 a full-access, also to the private area 14 by enabling the first person 23 to be able to unlock the private door 7. The sequence of steps is practically the same as the before described with respect to the diagram of Figure 3, only with additional method steps. Accordingly, hereinafter, said additional steps will only be described.

[0078] In the depicted embodiment, after the steps S3.1 and S3.2 which lead to possession of the electronic pre-access credential for the first person 23 and, accordingly, the respective access right to enter the common areas 11 and 13 accessible via the common doors 5 and 9, the step S4.1 is performed by the suggested computer-implemented method. Thereby, a full-access activation request to assign an electronic full-access credential to the first person 23 is received. The electronic full-access credential finally can grant the first person 23 the right to open the common doors 5 and 9 for accessing the common area 11 and 13, but additionally also the right to open the first private door 7 for accessing the private area 14, such as the new tenant's apartment.

[0079] In step S4.2, the electronic full-access credential associated is generated with the (before-already-used) identifier of the first person 23.

[0080] Thereafter, the electronic full-access credential is transmitted to the electronic locks of the common doors 5 and 9 and also to the electronic lock of the first person's private door 7, thereby, at a full-access point in time after the pre-access point in time, configuring (step S5.2) the electronic locks to unlock if the electronic full-access credential is provided by the mobile device 19 of the first person 23.

[0081] It is also possible that the electronic full-access credential would only be transmitted to the first person's private door 7, since the common doors 5 and 9, or, respectively, their corresponding electronic locks or lock apparatuses 16 already have the electronic pre-access credential which still could guarantee the possibility to enter the respective common doors 5 and 9.

[0082] It is also possible, that the steps S4.1, S4.2, S5.1, and S5.2 (only some of them or even all) are already performed before, for example also already with the generation and transmission of the electronic pre-access credential. However, according to the present disclosure, the full-access credential at least is not sent or at least cannot be used by the first person 23 to open private doors 7 or 8 at the beginning already. First, solely any of the common doors 5, 9, or 4, or 6 can be opened by the

first person 23, and then, afterwards, the permission to open also private doors 7 and/or 8 might be given to the first person 23. Despite of generating or even transmitting the electronic full-access credential already, the ability to open said private doors 7 or 8 could be still hold back, for example, by not yet sending the electronic full-access credential to the first person 23. Accordingly, the full-access point in time could also be the moment when the electronic full-access credential is sent to the first person 23.

[0083] However, according to the method depicted in Figure 4, the electronic full-access credential is sent in step S6 to the mobile device 19 of the first person 23 using the mobile application installed thereon. Thereby, the electronic full-access credential is received and stored (step S6.1) in the mobile application, enabling the first person 23 to open also the private door 7 when presenting the electronic full-access credential to the private door's electronic lock (lock apparatus 16).

[0084] Figure 5 shows a timing diagram illustrating an exemplary sequence of the steps of additionally giving the first person 23 a full-access, also to the private area 14 by enabling the first person 23 to be able to unlock the private door 7, as an alternative to the sequence of steps as shown in Figure 4. The sequence of steps is practically the same as the before described with respect to the diagram of Figure 3, only with additional method steps. Accordingly, hereinafter, said additional steps will only be described.

[0085] In the depicted embodiment, after the steps S3.1 and S3.2 which lead to possession of the electronic pre-access credential for the first person 23 and, accordingly, the respective access right to enter the common areas 11 and 13 accessible via the common doors 5 and 9, the step S7.1 is performed by the suggested computer-implemented method. In step 7.1, the electronic pre-access credential before generated and already transmitted to the first person 23 is also transmitted to the electronic lock of the first person's private door 7, thereby, at a respective full-access point in time after the pre-access point in time, configuring (step S7.2) also the electronic lock of the first person's private door 7 to unlock if the electronic pre-access credential is provided by the mobile device 19 of the first person 23. Accordingly, the first person 23 then also has the right to open the private door 7 for accessing the private area 14, such as the new tenant's apartment.

[0086] Preferably, in an embodiment not depicted, before the step S7.1 of transmitting the electronic pre-access credential also to the electronic lock of the first person's private door 7, the following step could be performed: receiving an extension for full-access request to adapt the electronic pre-access credential for the first person 23, thereby initiating the granting process of the right to open additionally to the common door(s) 5, 9 also the at least one private door 7.

[0087] Figure 6 shows a timing diagram illustrating several exemplary steps which can be part of the suggested sequences of steps for managing access to the managed residential building 2. Hereinafter, only the additional steps in comparison to the before described sequences are described. The steps can be combined with the before described embodiments. Moreover, the steps newly described with respect to Figure 6 do not need to be all combined. Also, single steps can be provided or combined with respect to the suggested embodiments. In the embodiment according to Figure 6, in comparison to the before described embodiment, the first person 23 is only to be allowed to open the common door 5 (and not anymore the common door 9), only by way of an example.

[0088] In step S8, the pre-access point in time and/or the full-access point in time can be predefined within the access management platform. The predefinition results in a predetermined condition related to the rental agreement information, in particular according to a date of a start of a rental agreement and/or according to a confirmation of payment, such as a payment of a rent and/or a deposit. Then, the first person 23 could be given the permission to access either the common area 11 or even the private are 7, according to the depicted embodiment, under said condition that a deposit has been paid for example. Advantageously, the first person 23 can be given via only one entry within the access management platform the access right from a first date on to common area 11 and from a second date on to the private area 7.

[0089] In step S9, the electronic pre-access credential (and/or according to another embodiment the electronic full-access credential) is stored in an access management platform whitelist. Furthermore, in step S10, it is verified if a used electronic pre-access credential (and/or a used electronic full-access credential) being transmitted from the electronic lock(s), corresponds to the electronic pre-access credential (and/or the electronic full-access credential) stored in the access management platform whitelist. Then, the step of transmitting (step S2.1, or S5.1, or S7.1) the pre-access credential (and/or the electronic full-access credential) to the electronic lock(s) and configuring (S2.1; S5.1; S6.1) the electronic lock(s) only is executed if the step of verification (step S10) is positive. Correspondingly, the steps depending on a positive verification have been depicted with dashed arrows and boxes in Figure 6. Accordingly, a storage of the credentials in the electronic locks does not have to take place. However, a online lock apparatus 16 needs to be provided or at least a lock apparatus 16 being able to permanently connect to the access management platform under a request of a person to enter the respective door.

[0090] In step 11.1, by way of an example, entrance execution data is received via the communication network 20 from the electronic lock(s) and/or via a communication network 21 from the mobile application. Then, the entrance execution data is stored (step 11.2.) in the access management platform. The entrance execution data can comprise a time of entrance information about when the electronic lock(s) is or has (are or have) been

opened; and/or a user information about which electronic pre-access credential and/or which electronic full-access credential is or has been used to open the electronic lock(s); and/or a medium information about which mobile device 23 and/or which mobile application is or has been used to open the electronic lock(s).

[0091] In general, the credential could also be added to a blacklist (not depicted) of the access management platform or of the electronic locks, wherein credentials entered in the blacklist have priority in comparison to credentials listed in the whitelist in a manner that a credential being in the blacklist cannot lead to opening the respective door. Thereby, even if the first person 23 lost his mobile device 19, an abuse of the lost credentials can be avoided.

[0092] In general, the presented steps S2.1, S5.1 and/or S7.1 in terms of transmitting the pre-access credential and/or the electronic full-access credential to the electronic lock(s) can be executed via a direct communication via the communication network 20. Nevertheless, another option is that the steps S2.1, S5.1 and/or S7.1 in terms of transmitting the pre-access credential and/or the electronic full-access credential to the electronic lock(s) can be executed via an indirect communication by the step of: transmitting (step S12.1), at a first point in time, the pre-access credential (and/or the electronic full-access credential) to a manager's mobile device, in the particular example the mobile device 24 of the caretaker 25, thereby leading to a necessity of transmitting (in step S12.2), at a second point in time after the first point in time, the pre-access credential (and/or the electronic full-access credential) from the manager's mobile device 24 to the electronic lock(s). This alternative of an indirect transfer of the credentials is depicted in Figure 6 with the help of dotted arrows. For the indirect transmission, the so-called Utility App of the recent applicant can for example be used on the mobile device 24 of the caretaker 25.

[0093] In general, the pre-access credential and/or the electronic full-access credential can be encrypted, preferably using asymmetric encryption. An example for the asymmetric encryption is the Elliptic Curve Cryptography. Advantageously, the credential(s) is (are) configured as being not readable by the mobile device 19 (or the mobile application) of the first person 23, but being only readable by the electronic lock(s) and/or the access management platform. In particular, especially with respect to the suggested systems and methods, the credential(s) can be transmitted in encrypted form from the access management platform to the mobile device 19 (in particular the mobile application). The credential(s) also remain(s) stored in an encrypted manner on the mobile device 19. The credential(s) can then be also transmitted in encrypted form to the electronic lock at the moment of intention of access. Only at the electronic look, the credential(s) then is (are) decrypted in order to make the access decision by the verifying step.

[0094] In an embodiment, not depicted, the computer-implemented method further comprises the step of deactivating the right to open the common door(s) 4, 5, 6, and/or 9 and/or to open the private doors 7 and/or 8, preferably by:

- deleting the electronic pre-access credential and/or the electronic full-access credential from the whitelist; and/or
- storing the electronic pre-access credential and/or the electronic full-access credential on the blacklist, wherein the blacklist is assigned with priority in comparison to the whitelist; and/or
- transmitting the electronic pre-access credential and/or the electronic full-access credential to the electronic lock of the common door(s) 4, 5, 6, and/or 9 and/or of the private door 7 and(or 8, thereby configuring the electronic lock(s) not to unlock anymore if the electronic pre-access credential and/or the electronic full-access credential is provided by the mobile device 19 of the first person 23.

[0095] It should be noted that, in the description, the sequence of the steps has been presented in a specific order, one skilled in the art will understand, however, that the order of at least some of the steps could be altered, without deviating from the scope of the disclosure.

Reference numerals:

[0096]

1	managed residential area
2, 3	managed residential buildings
4, 5, 6, 9	common door
7, 8	private door
10, 11, 12, 13	common area
14, 15	private area
16	lock apparatus
17	data processing apparatus
18	cloud
19	mobile device
20, 21	communication network
22	short range communication connection
23	first person
24	mobile device (of caretaker)
25	caretaker

Claims

1. A computer-implemented method of managing access for a managed residential building (2; 3), the managed residential building (2; 3) having one or more common door(s) (4; 5; 6; 9) including an electronic lock, and at least one private door (7; 8),

wherein the common door(s) (4; 5; 6; 9) control(s) access to a common area (10; 11; 12; 13) of the managed residential building (2; 3), and the at least one private door (7; 8) controls access to a private area (14; 15) allocated to a first person (23) according to a rental agreement information,
wherein the first person (23) initially, at a starting point in time, does not yet have any electronic access rights for the common area (10; 11; 12; 13) of the managed residential building (2; 3),
the method being performed by an access management platform and comprising at least the following steps:

receiving (S1.1) a pre-access activation request to assign an electronic pre-access credential to the first person (23), wherein the electronic pre-access credential grants the first person (23), at a pre-access point in time, only the right to open the common door(s) (4; 5; 6; 9) for accessing the common area (10; 11; 12; 13);
generating (S1.2) the electronic pre-access credential associated with an identifier of the first person (23);
transmitting (S2.1) the electronic pre-access credential to the electronic lock(s) of the common door(s) (4; 5; 6; 9), thereby, at the pre-access point in time, configuring (S2.2) the electronic lock(s) of the common door(s) (4; 5; 6; 9) to unlock if the electronic pre-access credential is provided by a mobile device (19) of the first person (23);
sending (S3) an application-installation invitation to the mobile device (19) of the first person (23), thereby enabling the first person (23) to install and activate (S3.1) a mobile application through which the electronic pre-access credential is receivable and/or storable (S3.2).

2. The computer-implemented method according to claim 1, wherein the at least one private door (7; 8) includes an electronic lock.

3. The computer-implemented method according to claim 2, further comprising at least the following steps:

receiving (S4.1) a full-access activation request to assign an electronic full-access credential to the first person (23), wherein the electronic full-access credential grants the first person (23) the right to open the common door(s) (4; 5; 6; 9) for accessing the common area (10; 11; 12; 13) and the right to open the at least one private door (7; 8) for accessing the at least one private area (14; 15);
generating (S4.2) the electronic full-access credential associated with the identifier of the first person (23);
transmitting (S5.1) the electronic full-access credential to the electronic lock(s) of the common door(s) (4; 5; 6; 9) and to the electronic lock of the first person's private door (7; 8), thereby, at a full-access point in time after the pre-access point in time, configuring (S5.2) the electronic locks to unlock if the electronic full-access credential is provided by a mobile device (19) of the first person (23);
sending (S6) the electronic full-access credential to the mobile device (19) of the first person (23) using the mobile application installed thereon.

4. The computer-implemented method according to claim 2, further comprising at least the following step:
transmitting (S7.1) the electronic pre-access credential also to the electronic lock of the first person's private door (7; 8), thereby, at a full-access point in time after the pre-access point in time, configuring (S7.2) also the electronic lock of the first person's private door (7; 8) to unlock if the electronic pre-access credential is provided by the mobile device (19) of the first person (23).

5. The computer-implemented method according to any one of the preceding claims, further comprising at least the following step:
predefining (S8) the pre-access point in time, and/or the full-access point in time, under a predetermined condition related to the rental agreement information, in particular according to a date of a start of a rental agreement and/or according to a confirmation of payment, in particular of a rent and/or a deposit.

6. The computer-implemented method according to any one of the preceding claims, wherein the electronic lock(s) is (are) configured to communicate via a communication network (20) with the access management platform, preferably reciprocally.

7. The computer-implemented method according to claim 6, further comprising at least the following steps:

storing (S9) the electronic pre-access credential and/or the electronic full-access credential in an access management platform whitelist; and
verifying (S10) if a used electronic pre-access credential and/or a used electronic full-access credential, being transmitted from the electronic lock(s), corresponds to the electronic pre-access credential and/or the electronic full-access credential stored in the access management

platform whitelist;

wherein the step of transmitting (S2.1; S5.1; S7.1) the pre-access credential and/or the electronic full-access credential to the electronic lock(s) and configuring (S2.2; S5.2; S7.2) the electronic lock(s) only is executed if the step of verification (S10) is positive.

8. The computer-implemented method according to any one of the preceding claims, further comprising at least the following steps:

receiving (S11.1) entrance execution data via the communication network (20) from the electronic lock(s) and/or via a communication network (21) from the mobile application; and
storing (S11.2) the entrance execution data, the entrance execution data comprising:

a time of entrance information about when the electronic lock(s) is or has (are or have) been opened; and/or
a user information about which electronic pre-access credential and/or which electronic full-access credential is or has been used to open the electronic lock(s); and/or
a medium information about which mobile device (19) and/or which mobile application is or has been used to open the electronic lock(s).

9. The computer-implemented method according to any one of the claims 6 to 8, wherein the step of transmitting (S2.1; S5.1; S7.1) the pre-access credential and/or the electronic full-access credential to the electronic lock(s) is executed via a direct communication via the communication network (20).

10. The computer-implemented method according to any one of the claims 1 to 8, wherein the step of transmitting (S2.1; S5.1; S7.1) the pre-access credential and/or the electronic full-access credential to the electronic lock(s) is executed via an indirect communication by the step of:
transmitting (S12.1), at a first point in time, the pre-access credential and/or the electronic full-access credential to a manager's mobile device (24), in particular caretaker's (25), thereby leading to a necessity of transmitting (S12.2), at a second point in time after the first point in time, the pre-access credential and/or the electronic full-access credential from the manager's mobile device (24) to the electronic lock(s).

11. The computer-implemented method according to any one of the preceding claims, wherein the pre-access credential and/or the electronic full-access credential is encrypted, preferably using asymmetric encryption.

12. A data processing apparatus (17) configured to perform a computer-implemented method according to any one of the preceding claims, the data processing apparatus (17) comprising the access management platform or configured to communicate with the access management platform.

13. A lock apparatus (16) configured to at least partially perform a computer-implemented method according to any one of the preceding claims, when interacting with the access management platform or when interacting with the data processing apparatus (17) according to claim 12, the lock apparatus (16) comprising the electronic lock and configured to lock and unlock the common door (4; 5; 6; 9).

14. A mobile device (19) configured to at least partially perform a computer-implemented method according to any one of the preceding claims, when interacting with the access management platform or when interacting with the data processing apparatus (17) according to claim 12, the mobile device (19) comprising the mobile application having stored the electronic pre-access credential.

15. A computer program product comprising commands which, when the computer program product is executed by a processor of a data processing apparatus (17), preferably according to claim 12, cause the data processing apparatus (17) to perform the steps of the computer-implemented method according to any one of the preceding claims.

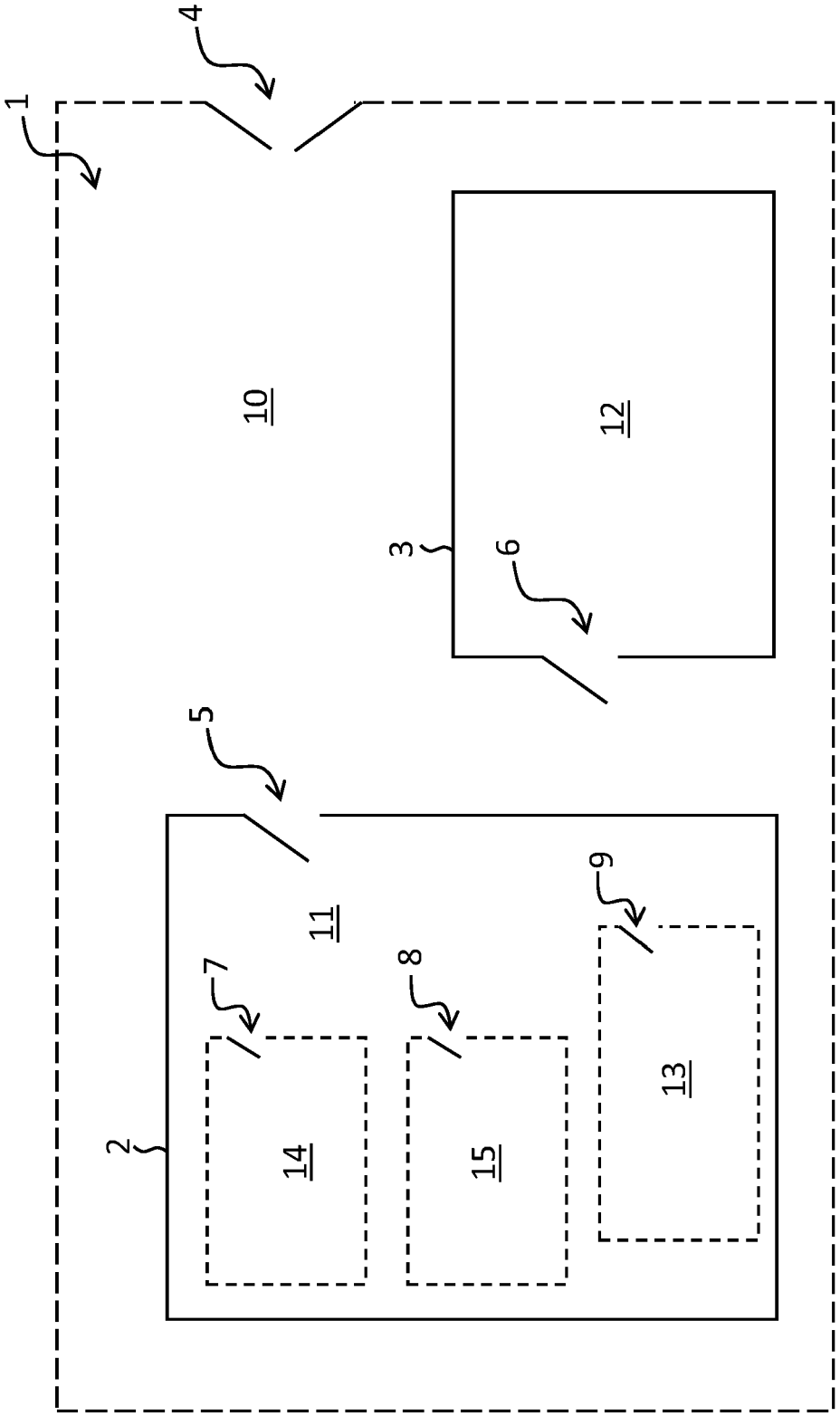

Fig. 1

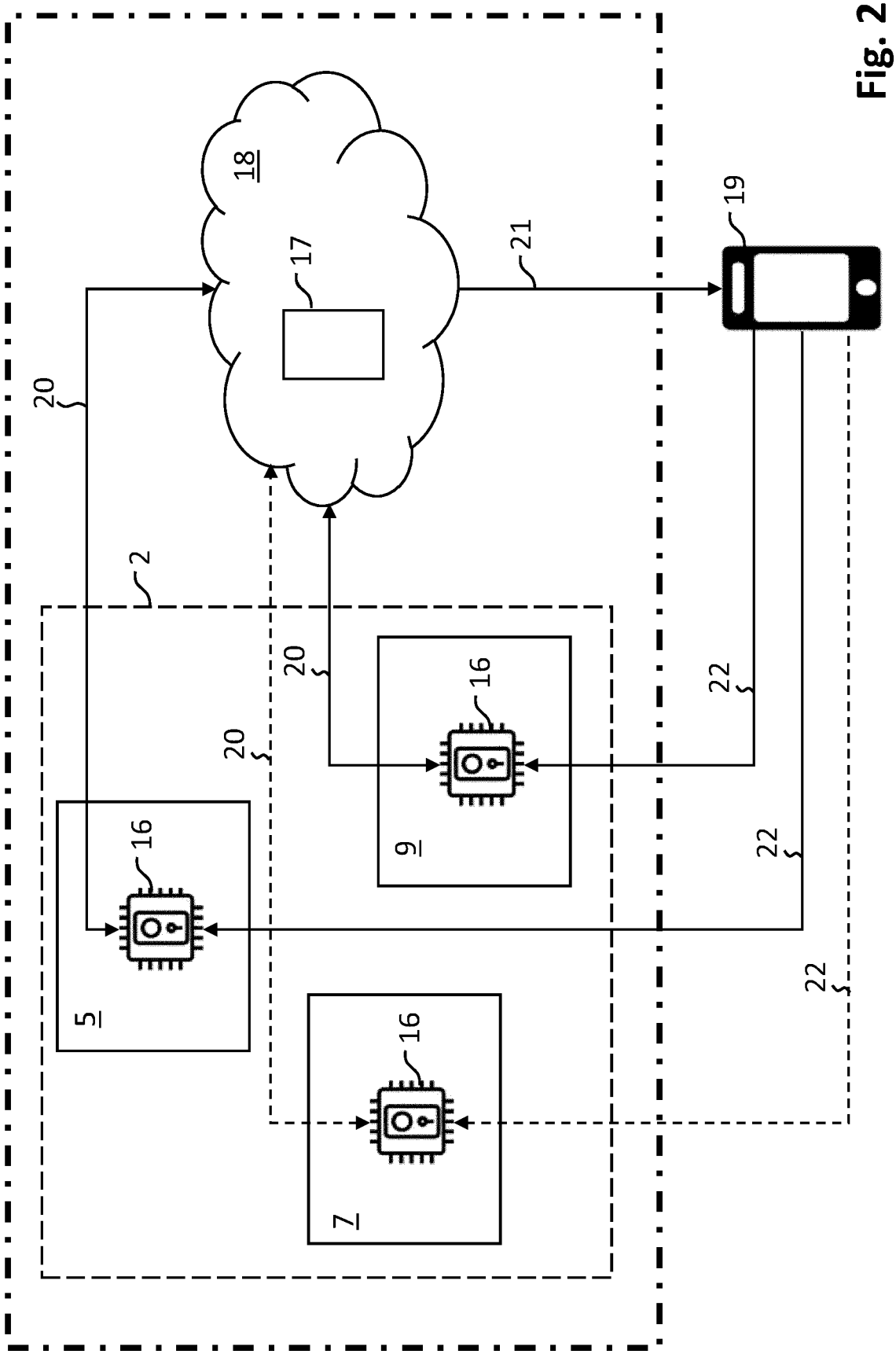

Fig. 2

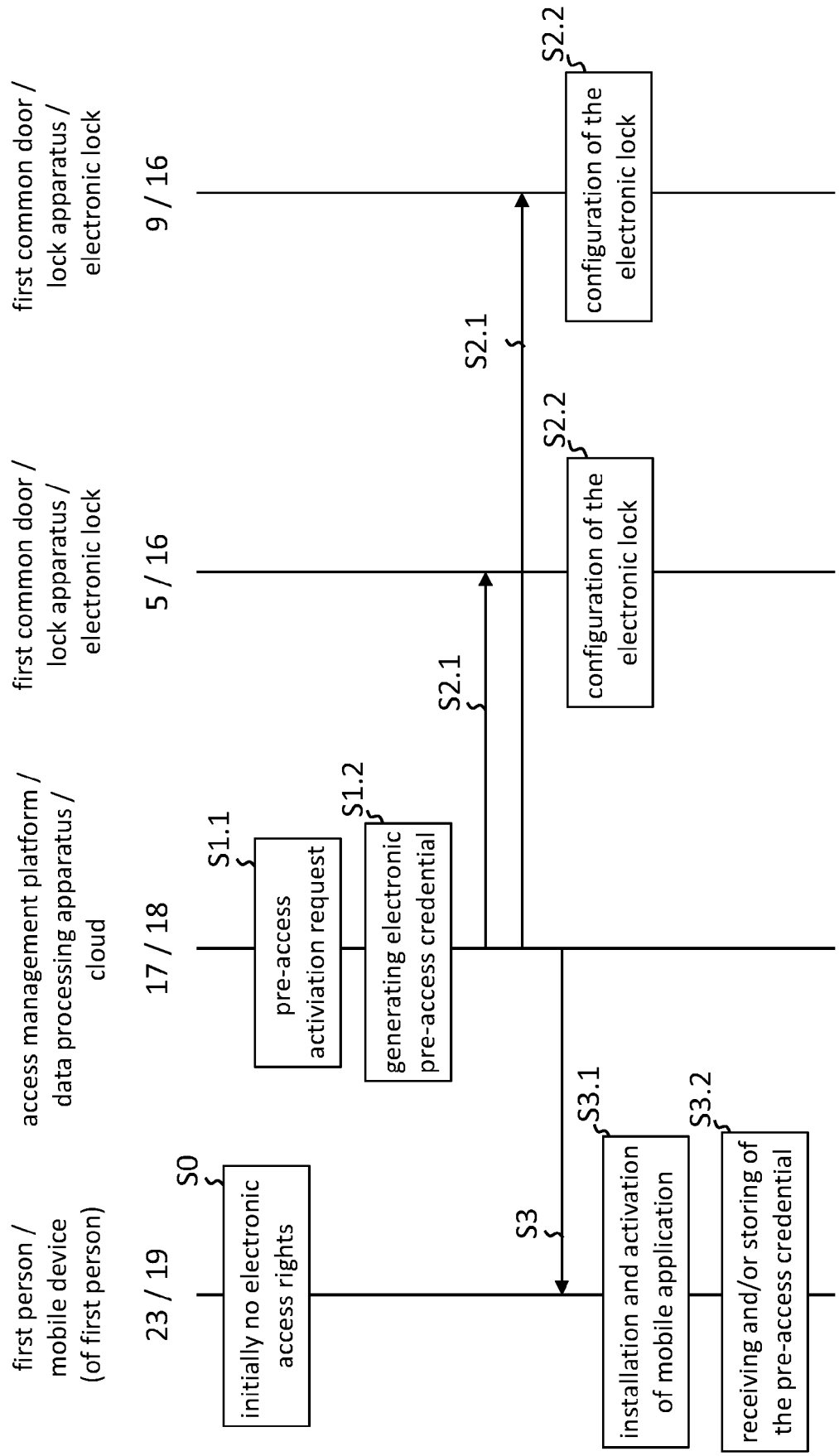
first person / mobile device (of first person)
23 / 19
access management platform / data processing apparatus / cloud
17 / 18
first common door / lock apparatus / electronic lock
5 / 16
first common door / lock apparatus / electronic lock
9 / 16
S0
initially no electronic access rights
S1.1
pre-access activiation request
S1.2
generating electronic pre-access credential
S2.1
S2.1
S2.2
configuration of the electronic lock
S2.2
configuration of the electronic lock
S3
S3.1
installation and activation of mobile application
S3.2
receiving and/or storing of the pre-access credential

Fig. 3

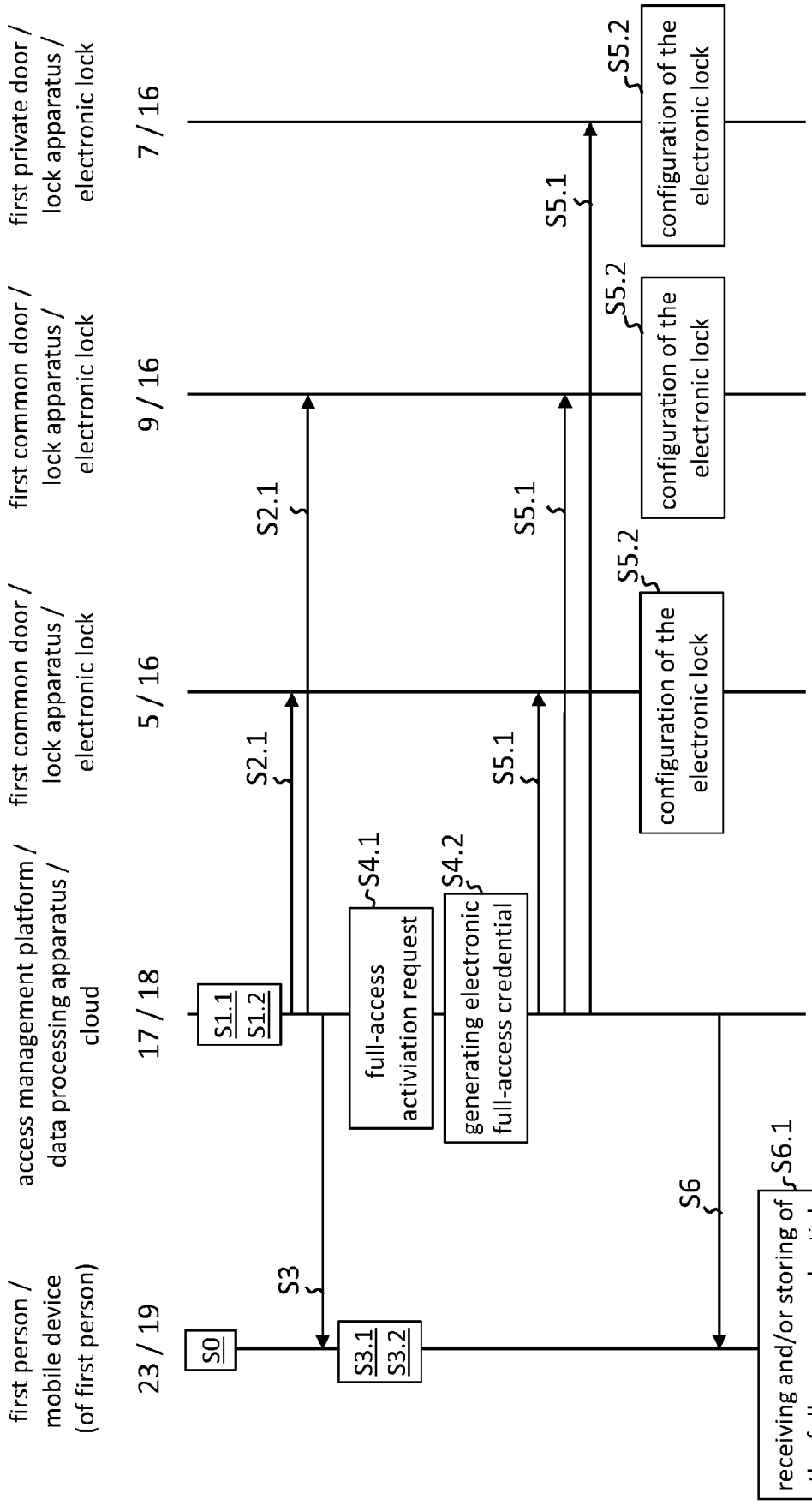
first person / mobile device (of first person)
23 / 19
access management platform / data processing apparatus / cloud
17 / 18
first common door / lock apparatus / electronic lock
5 / 16
first common door / lock apparatus / electronic lock
9 / 16
first private door / lock apparatus / electronic lock
7 / 16
S0
S1.1
S1.2
S2.1
S2.1
S3
S3.1
S3.2
S4.1
full-access activiation request
S4.2
generating electronic full-access credential
S5.1
S5.1
S5.1
S5.2
configuration of the electronic lock
S5.2
configuration of the electronic lock
S5.2
configuration of the electronic lock
S6
S6.1
receiving and/or storing of the full-access credential

Fig. 4

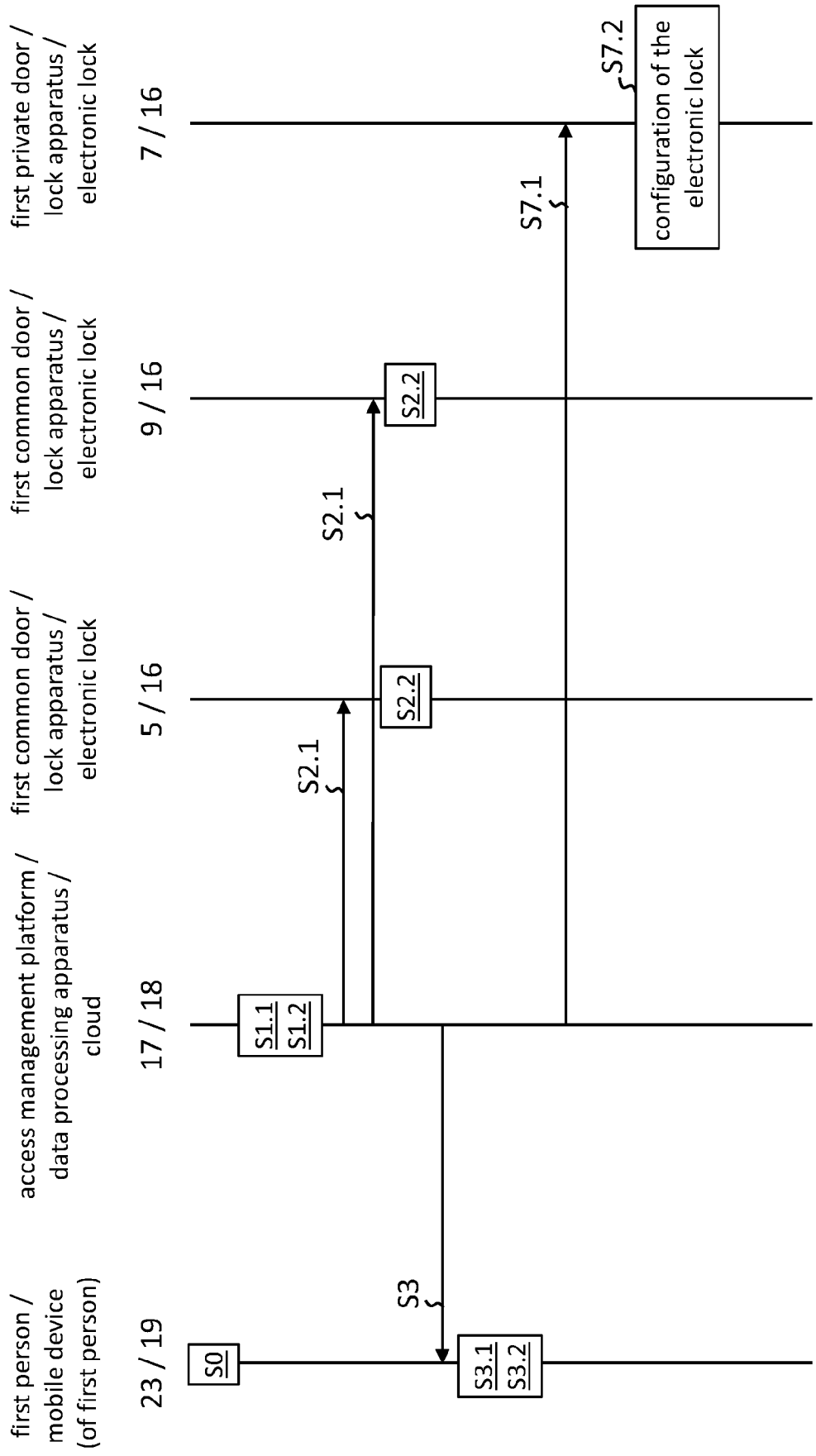
first person / mobile device (of first person)
23 / 19
access management platform / data processing apparatus / cloud
17 / 18
first common door / lock apparatus / electronic lock
5 / 16
first common door / lock apparatus / electronic lock
9 / 16
first private door / lock apparatus / electronic lock
7 / 16
S0
S1.1
S1.2
S2.1
S2.2
S2.1
S2.2
S3
S3.1
S3.2
S7.1
S7.2
configuration of the electronic lock

Fig. 5

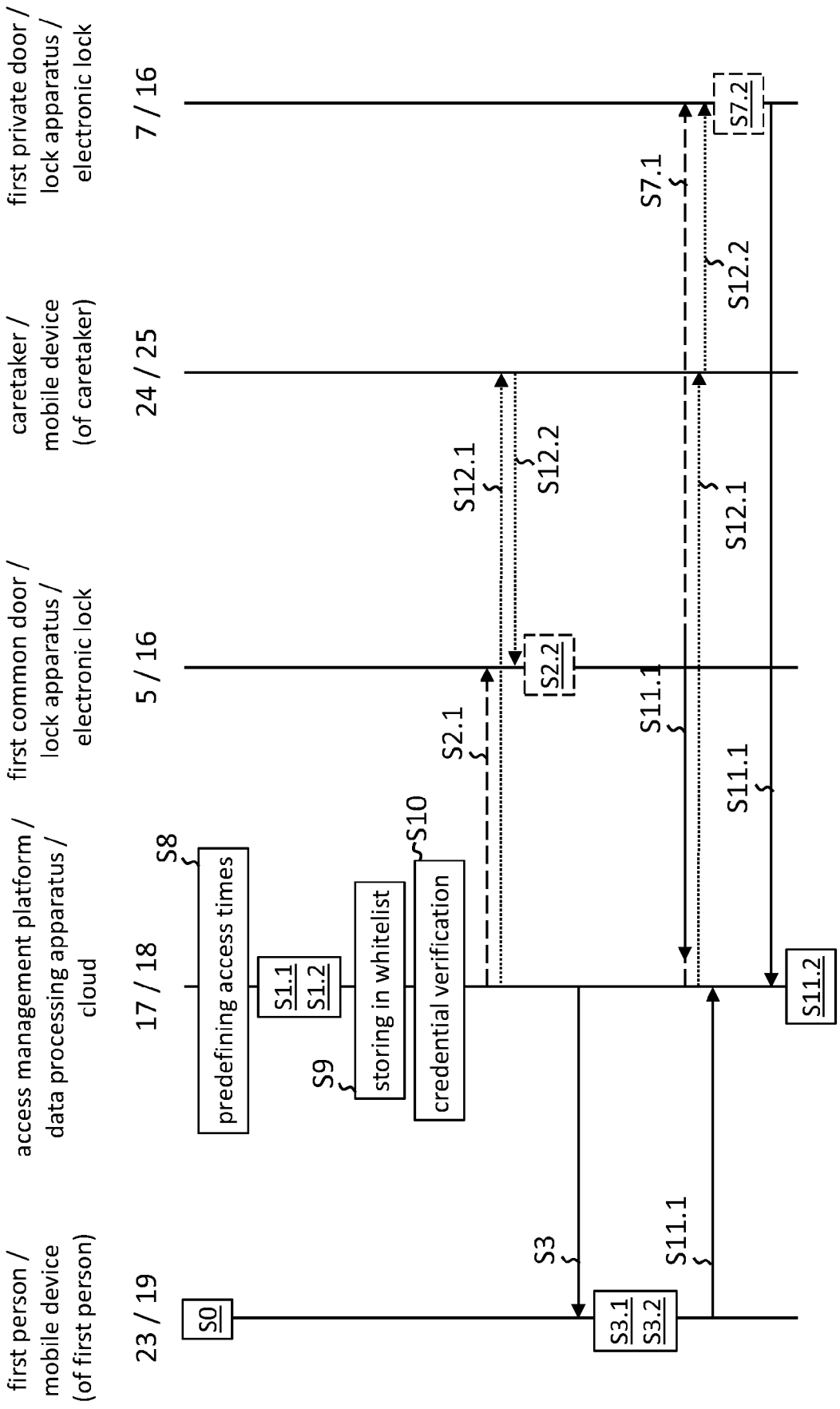
first person / mobile device (of first person)
23 / 19
access management platform / data processing apparatus / cloud
17 / 18
first common door / lock apparatus / electronic lock
5 / 16
caretaker / mobile device (of caretaker)
24 / 25
first private door / lock apparatus / electronic lock
7 / 16
S0
S8
predefining access times
S1.1
S1.2
S9
storing in whitelist
S10
credential verification
S2.1
S2.2
S12.1
S12.2
S3
S3.1
S3.2
S11.1
S11.2
S7.1
S7.2

Fig. 6

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 22 19 2916

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 Y A	US 2021/142601 A1 (SCHOENFELDER LUKE A [US] ET AL) 13 May 2021 (2021-05-13) * abstract; figures 1A-3D * * paragraph [0020] - paragraph [0123] *	1-6,8,9, 11-15 10 7	INV. G07C9/00
Y A	EP 1 024 239 A1 (IBM [US]) 2 August 2000 (2000-08-02) * paragraph [0017] * * paragraph [0022] - paragraph [0024] *	10 1-9, 11-15	
A	US 2018/005143 A1 (CAMARGO FABIAN EMILIO PHILIPE [US] ET AL) 4 January 2018 (2018-01-04) * paragraph [0004] - paragraph [0008] * * paragraph [0032] - paragraph [0037] *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)
G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	30 January 2023	Holzmann, Wolf

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 22 19 2916

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.

30-01-2023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021142601 A1	13-05-2021	CA 3118110 A1	30-04-2022
		CN 114530008 A	24-05-2022
		EP 3992931 A1	04-05-2022
		JP 2022073909 A	17-05-2022
		KR 20220058376 A	09-05-2022
		TW 202217607 A	01-05-2022
		US 2021142601 A1	13-05-2021
		US 2021407229 A1	30-12-2021
EP 1024239 A1	02-08-2000	AU 1793400 A	18-08-2000
		CA 2323146 A1	03-08-2000
		DE 69924349 T2	09-02-2006
		EP 1024239 A1	02-08-2000
		ES 2236973 T3	16-07-2005
		JP 3485254 B2	13-01-2004
		JP 2000224163 A	11-08-2000
		MY 125905 A	30-08-2006
		TW 462173 B	01-11-2001
		US 6981142 B1	27-12-2005
		WO 0045016 A1	03-08-2000
US 2018005143 A1	04-01-2018	AU 2017286911 A1	24-01-2019
		CA 3029585 A1	04-01-2018
		EP 3479307 A1	08-05-2019
		US 2018005143 A1	04-01-2018
		US 2021232983 A1	29-07-2021
		WO 2018005976 A1	04-01-2018

EPO FORM P0459

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