(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 April 2015 (23.04.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/055812 A1

(51) International Patent Classification:
G07C 9/00 (2006.01)

(21) International Application Number:
PCT/EP2014/072311

(22) International Filing Date:
17 October 2014 (17.10.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/057,271 18 October 2013 (18.10.2013) US

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; P.O. Box 70340, S-107 23 Stockholm (SE).

(72) Inventor: **SINGH, Sona**; Rinds Gränd 5, S-187 73 Täby (SE).

(74) Agent: **KRANSELL & WENNBORG KB**; P.O. Box 27834, S-115 93 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: COMMUNICATION AND PROCESSING OF CREDENTIAL DATA

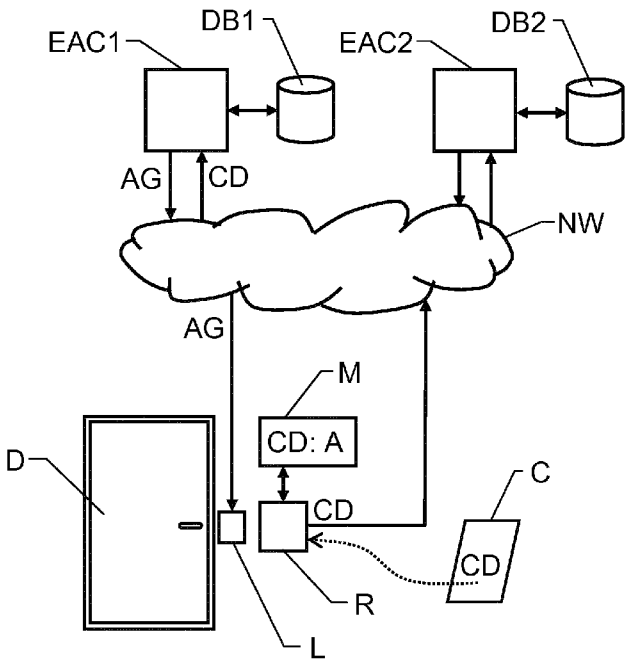

Fig. 2

(57) Abstract: A reader unit (R) registers credential data (CD) representing users seeking access to a well-defined space. The reader unit (R) is associated with an access control related building component (e.g. a lockable door). Each piece of credential data (CD) is further associated with a linked address (A) identifying one of a first credential data receiver (EAC1) and at least one second credential data receiver (EAC2). The linked address (A) Is stored in a memory module (M, M1, M2) associated with the reader unit (R, R1, R2) or on a portable carrier (C) holding the piece of credential data (CD). If the linked address (A) identifies the first credential data receiver (EAC1), the reader unit (R) forwards the registered credential data (CD) to a first credential data receiver (EAC1), and if the linked address (A) identifies a particular one of the at least one second credential data receiver (EAC2), the reader unit (R) forwards the registered credential data (CD) to the particular one of the at least one second credential data receiver (EAC2). In response to the credential data (CD), the first credential data receiver (EAC1) is configured to effect at least one decision (AG) in respect of the well-defined space independently of the at least one second credential data receiver (EAC2) (e.g. opening a door), and vice versa.

WO 2015/055812 A1

Communication and Processing of Credential Data

THE BACKGROUND OF THE INVENTION AND PRIOR ART

The present invention relates generally to solutions for handling credential data in an efficient manner, for example in connection with access control. More particularly the invention relates to a reader unit according to the preamble of claim 1, a data communication system according to the preamble of claim 2 and a method according to the preamble of claim 8. The invention also relates to a computer program product according to claim 13 and a computer readable medium according to claim 14.

In modern buildings, especially in business premises, electronic access control (EAC) systems are often used to control entries to and exits from various facilities. Here, personal so-called credential data are normally used as a basis to define which subjects who are authorized to enter a certain area during a given interval of time. The credential data may be embodied in a key fob, a smartcard, a proximity card or other appropriate carrier, e.g. a subscriber identity module (SIM) card of a mobile telephone or a personal digital assistant (PDA).

A reader unit, for instance of short-range radio communication type, can be employed to register the credential data and forward the data to an access control node. In this context, the short-range radio communication type of interface is understood to adhere a known wireless protocol, e.g. the NFC (Near Field Communication) protocol, Bluetooth, ZigBee or WiFi. Provided that the credential data are found to represent an authorized subject, the access control node causes an access message to be sent to a control mechanism of a door associated with the reader, for instance via a UART protocol (UART = Universal Asynchronous Receiver/ Transmitter), resulting in that the door opens.

US 2008/0163361 describes a solution, for providing a secure access network. Here, access decisions are made by a portable credential using data and algorithms stored on the credential. Since access decisions are made by the portable credential non-networked hosts or local hosts can be employed that do not necessarily need to be connected to a central access controller or database thereby reducing the cost of building and maintaining the secure access network.

US 2011/0187493 discloses a system, wherein access is controlled within a multi- room facility. A guest of the multi-room facility is here allowed to remotely confirm reservations to the facility as well as bypass the front desk of the multi-room for check-in purposes. At a location within the facility, the guests are allowed to confirm their arrival, check-in, and have their access credential written with personalized access data that may be useable for the duration of the guest's stay.

PROBLEMS ASSOCIATED WITH THE PRIOR ART

Consequently flexible access solutions are known. However, there is yet no efficient system enabling different enterprises/organizations to share one or more automatic doors (or other access related components) of a building without requiring a central control function for said one or more doors/components, which is common for all organizations.

SUMMARY OF THE INVENTION

The object of the present invention is therefore to solve the above problem, and thus offer flexible and efficient solution that enables different enterprises/organizations to conveniently share one or more automatic doors (or other access related components).

According to one aspect of the invention, the object is achieved by the initially described reader unit, wherein the reader unit is

configured to communicate with at least one second credential data receiver for causing at least one access decision in respect of the well-defined space to be effected. The reader unit is further configured to forward each registered piece of credential data to either the first credential data receiver or to a particular one of the at least one second credential data receiver based on an address linked to the piece of credential data. The linked address identifies the first credential data receiver or the particular one of the at least one second credential data receiver. The linked address (preferably of Internet-Protocol type), in turn, is stored in either a memory module associated with the reader unit; or on a carrier (e.g. a card) holding the piece of credential data, which carrier is configured to be presented to the reader unit for registering the piece of credential data.

This reader unit is advantageous because it renders it possible for different enterprises and organizations to control various access-related components independently of one another while sharing a common reader unit.

According to another aspect of the invention, the object is achieved by the data communication system described initially, wherein the data communication system includes at least one second credential data receiver configured to receive credential data registered by the reader unit, and in response thereto cause at least one access decision in respect of the well-defined space to be effected. Moreover, the reader unit is communicatively connected to the first credential data receiver and the at least one second credential data receiver. The reader unit is further configured to forward a registered piece of credential data to either the first credential data receiver or a particular one of the at least one second credential data receiver based on an address linked to the piece of credential data, which address identifies the first credential data receiver or the particular one of the at least one second credential data receiver. The linked address, in turn, is stored in a memory module associated with the reader unit, or on a carrier holding the piece of credential

data, which carrier is configured to be presented to the reader unit for registering the piece of credential data. The advantages of this system are the same as those associated with the above-proposed reader unit.

According to one preferred embodiment of this aspect of the invention, the at least one access decision involves granting or refusing access to the well-defined space. Here, the access-control-related building component includes a lock mechanism configured to selectively enable or prevent access to the well-defined space via a door associated with the reader unit. In response to a received piece of credential data, each of the first and the at least one second credential data receiver is configured to check the piece of credential data against a database defining a set of users' access rights to the well-defined space. If the piece of credential data is found to designate an authorized user, the credential data receivers are configured to cause an access grant message to be sent to the lock mechanism, which access grant message orders the lock mechanism to open the door. Otherwise, i.e. if the user is found not to be authorized, the credential data receivers are configured to refrain from causing the access grant message to be sent to the lock mechanism. Hence, the access to a building, or part thereof, can be controlled in a very convenient and efficient manner.

According to another preferred embodiment of this aspect of the invention, the at least one access decision involves registering an entry to or exit from the well-defined space. Here, in response to a received piece of credential data, each of the first and the at least one second credential data receiver is configured to: register an entry if the piece of credential data is received via a first scanner of the reader unit, and register an exit if the piece of credential data is received via a second scanner of the reader unit. Thus, a digital puncher / time-clock can be conveniently implemented.

According to a further preferred embodiment of this aspect of

the invention, the data communication system includes a control node that is communicatively connected to the reader unit and each of the first and the at least one second credential data receiver. The control node is configured to receive credential data from the reader unit, and forward the received credential data to a credential data receiver identified by the address linked to the credential data. The control node is also configured to receive access grant messages from the first and the at least one second credential data receiver; and forward the received access grant messages to the lock mechanism. Each access grant message is here configured to order the lock mechanism to be opened during a predetermined interval, for example to allow a person to pass through a door. This enables a highly efficient implementation of an automatic door or similar function.

According to yet another preferred embodiment of this aspect of the invention, the control node is communicatively connected to at least one reader unit in addition to said reader unit. The control node is further configured to receive credential data from the additional reader unit, forward the received credential data to a credential data receiver identified by the address linked to the credential data, receive access grant messages from the first and the at least one second credential data receiver, and forward the received access grant messages to a lock mechanism in addition to said lock mechanism. Also here each access grant message is configured to order the additional lock mechanism to be opened during a predetermined interval. Thus, the control node can control multiple lock mechanisms in a straightforward and efficient manner.

Preferably, the linked addresses identifying the first and the at least one second credential data receivers are Internet Protocol addresses.

According to another aspect of the invention, the object is achieved by the method described initially, wherein it is presumed that the network includes a first credential data receiver and at

least one second credential data receiver. The method involves forwarding each registered piece of credential data to either the first credential data receiver, or a particular one of the at least one second credential data receiver based on an address linked to the piece of credential data, which address identifies the first credential data receiver or the particular one of the at least one second credential data receiver. The linked address, in turn, is stored in a memory module associated with the reader unit, or on a carrier holding the piece of credential data, which carrier is configured to be presented to the reader unit for registering the piece of credential data. The advantages of this method, as well as the preferred embodiments thereof, are apparent from the discussion above with reference to the proposed reader unit and data communication system.

According to a further aspect of the invention the object is achieved by a computer program product, which is loadable into the memory of a computer, and includes software for performing the steps of the above proposed method when executed on a computer.

According to another aspect of the invention the object is achieved by a computer readable medium, having a program recorded thereon, where the program causes a computer to perform the method proposed above when the program is loaded into the computer.

Further advantages, beneficial features and applications of the present invention will be apparent from the following description and the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is now to be explained more closely by means of preferred embodiments, which are disclosed as examples, and with reference to the attached drawings.

Figure 1 shows a block diagram over a prior-art access

control system;

Figures 2-6 show block diagrams over data communication systems according to various embodiments of the invention; and

Figure 7 illustrates, by means of a flow diagram, the general method according to the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Initially, we refer to Figure 1 showing a block diagram over a prior-art access control system. Here, first and second readers, 110 and 120, are connected to a first and a second control panel 130 and 160 respectively. Each reader 110 and 120 is arranged to control entries via a door 115 based on communication with the control panels 130 and 160.

The first control panel 130, in turn, is controlled by a first EAC node 140 and based on entries in a first database 150 associated with the first control panel 130. More precisely, when a first user approaches the door 115 and presents a credential data carrier C (e.g. in the form of a proximity card, a key fob, a smartcard, or other appropriate carrier, such as a subscriber identity module (SIM) card of a mobile telephone or a personal digital assistant (PDA)) to a given reader, say a first reader 110, this reader 110 reads out the credential data CD from the data carrier C and forwards the credential data CD to the first control panel 130. Then, the first control panel 130 checks the first database 150 for any entries matching the credential data CD. If a match is found, the first control panel 130 queries the first EAC node 140 to determine whether or not the first user (i.e. the person being associated with the credential data CD) shall be allowed to enter through the door 115. Given that the first user is found to be authorized, the first control panel 130 sends a first access grant message AG1 (for instance via a UART protocol) to a lock control mechanism 105 at the door 115. In res-

ponse to the first access grant message AG1 the lock control mechanism 105 unlocks the door 115, so that the first user can enter.

We can assume that each of a first and second organization controls the door 115, and that the above-mentioned first user belongs to the first organization. When a second user belonging to the second organization approaches the door 115 in order to enter, he/she presents his/her credential data carrier C to the second reader 120. The second reader 120 reads out the credential data CD from the data carrier C and forwards this data to the second control panel 160. Then, the second control panel 160 checks a second database 180 for any entries matching the second user's credential data CD. If a match is found, the second control panel 160 queries a second EAC node 170 to determine whether or not the second user shall be allowed to enter through the door 115. Given that the second user is found to be authorized, the second control panel 160 sends a second access grant message AG2 to the lock control mechanism 105, which in response thereto, unlocks the door 115, so that the second user can enter.

As can be seen in Figure 1, each organization that wishes to control entries (and/or exits) via a given door needs to arrange a respective reader unit at this door and build up an entire communication structure of its own to control the door's lock mechanism. Consequently, if many organizations are involved, a large amount of hardware is required, for instance in the form of reader units at the door. Moreover, sharing control panels, EAC nodes and/or databases between organizations is undesired for many reasons, for example referring to security/integrity risks and administration.

Such problems, however, can be avoided by the present invention. Figure 2 shows a block diagram over a data communication system according to a first embodiment of the invention.

Here, a reader unit R is associated with a door D through which users may gain access to a well-defined space. The reader unit R is configured to register user credential data CD, which may be stored on a personal carrier C embodied in a key fob, a smartcard, a proximity card or any other appropriate carrier, e.g. a SIM card of a mobile telephone or a PDA.

The system includes a first credential data receiver EAC1 and at least one second credential data receiver EAC2, where the first credential data receiver EAC1 may be controlled by a first organization and the at least one second credential data receiver EAC2 may be controlled by a respective organization different from the first organization. For clarity reasons, however, in the following description, we will only refer to one second credential data receiver EAC2.

Analogous to the above example, a user seeking access to the well-defined space is expected present his/her carrier C for the reader unit R, and in response thereto, the reader unit R is configured to register the credential data CD on the carrier C. Here, since there are more than one control node, the reader unit R is configured to communicate with both the first and the second credential data receiver EAC1 and EAC2, preferably via a general communication network NW, such as the Internet. In each individual case, however, the reader unit R is configured to forward the registered credential data CD to exactly one of the first credential data receiver EAC1 or the second credential data receiver EAC2.

According to the invention, each piece of credential data CD is linked to an address A, which identifies either the first credential data receiver EAC1 or the second credential data receiver EAC2 (or in the general case, a particular one of the at least one second credential data receiver EAC2). The linked address A, preferably an Internet Protocol address, is stored either in a memory module M associated with the reader unit R (as shown in Figure 1), or on the carrier C holding the piece of credential data

CD (as will be described below with reference to Figures 3a, 3b and 6).

In the example illustrated in Figure 2, we assume that access decisions generated by the system involve granting or refusing access to the well-defined space, i.e. that an access-control-related building component comprises a lock mechanism L configured to selectively enable or prevent access to a well-defined space via a door D that is associated with a reader unit R. In the specific example shown in Figure 2, it is further assumed that the address A linked to the credential data CD identifies the first credential data receiver EAC1. Therefore, the credential data CD are sent, via the communication network NW, to the first credential data receiver EAC1. Here, the credential data CD are checked against a first database DB1 to determine whether or not the user associated with the credential data CD is authorized to enter the door D at the current point in time. If so, the first credential data receiver EAC1 forwards an access grant message AG to a lock control mechanism L, which in response thereto, unlocks the door D, so that the user can enter the door D.

Similarly, if a carrier C is presented for the reader unit R, which carrier C contains credential data CD linked to an address A identifying the second credential data receiver EAC2, the credential data CD are forwarded to the second credential data receiver EAC2 for verification against a second database DB2.

Figure 3a shows a block diagram over a data communication system according to a second embodiment of the invention. Here, all units, components, signals and messages that also occur in Figure 2 represent the same units, components, signals and messages as described above with reference to Figure 2. As can be seen, in Figure 3a, there is no memory module M associated with the reader unit R. Instead, each carrier C contains the address A being linked to the credential data CD. Thus, upon presentation of the carrier C for the reader unit R, the reader

unit R is configured to read out the credential data CD as well as the address A linked thereto. Based on this address A, in turn, the reader unit R is configured to send the credential data CD to the credential data receiver identified by the address A, which in this example likewise is the first credential receiver EAC1. Then, the first credential receiver EAC1 executes the above-described verification procedure, and if the credential data CD are found to correspond to an authorized user, an access grant message AG is issued in response to which the lock L is caused to be unlocked. Otherwise, i.e. if the piece of credential data CD are found not to designate an authorized user, the first credential receiver EAC1 refrains from causing the access grant message AG to be sent to the lock mechanism L, and the lock mechanism L remains locked.

Figure 3b shows an example of how the data content of the carrier C in Figure 3a may be organized according one embodiment of the invention. Here, a storage area 310 contains a general encryption key K, which is required in the reader unit R to gain access to the contents of the carrier C. The address A, in turn, contains a first address field 310, which includes an address Adr_{EAC1} to the first credential receiver EAC1; and a second address field 320 which includes another address Adr_X. This address may specify a different credential receiver being responsible for controlling another door. However, the second address field 320 may equally well be used for purposes completely unrelated to locking/unlocking of a door, e.g. registering the presence of a user. Each of the overall address A and the individual address fields 310 and 320 is preferably protected by a respective encryption key, such that only authorized entities can gain access to the data therein.

Figure 4 shows a block diagram over a data communication system according to a third embodiment of the invention. Here, all units, components, signals and messages that also occur in either of Figures 2 or 3 represent the same units, components, signals and messages as described above with reference to Fi-

gure 2 or 3.

In the data communication system of Figure 4, the access decisions involve registering entries to or exits from a well-defined space. I.e. the system may implement a digital puncher / time-clock. To this aim, the reader unit R contains a first scanner R-IN and a second scanner R-OUT, which are arranged on the inside and the outside respectively of the door D.

Moreover, each of the first and second credential data receivers EAC1 and EAC2 is configured to register an entry into the well-defined space in respect of a user associated with a given piece of credential data CD if the piece of credential data CD is received via a first scanner R-IN of the reader unit R, and register an exit out from the well-defined space in respect of the user if the piece of credential data CD is received via a second scanner R-OUT. Analogous to the above, in response to a received piece of credential data CD, the reader unit R is configured to send the piece of credential data CD to the first credential data receiver EAC1 if the address A linked thereto identifies the first credential data receiver EAC1, and to the second credential data receiver EAC2 if the linked address A identifies the second credential data receiver EAC2.

Figures 5 and 6 show block diagrams over data communication systems according to a fourth and fifth embodiment respectively of the invention, both in which the access decisions involve granting or refusing access to well-defined spaces via doors D1 and D2 controllable via lock mechanisms L1 and L2 to which a respective reader unit R1 and R2 is associated.

Again, all units, components, signals and messages that also occur in either of Figures 2 to 4 represent the same units, components, signals and messages as described above with reference to Figure 2 to 4.

In the system of Figure 5, the addresses A linked to the credential data CD are stored in a memory module M (analogous to Fi-

gures 2 and 4), whereas in the system of Figure 6 the linked addresses are stored on the carriers C (analogous to Figure 3), otherwise the systems in Figures 5 and 6 are identical.

Inter alia, both systems contain a control node N, which is communicatively connected to a first reader unit R1 associated with a first door D1. The control node N is also communicatively connected to a second reader unit R2 associated with a second door D2 and, via a communication network NW, communicatively connected to each of a first and second credential data receiver EAC1 and EAC2 respectively. The control node N is configured to receive credential data CD from the reader units R1 and R2, and forward the received credential data CD to the credential data receiver EAC1 or EAC2 identified by the address A linked to the credential data CD.

The control node N is further configured to receive access grant messages AG from the first and second credential data receiver EAC1 and EAC2, and forward the received access grant messages AG to either a first lock mechanism L1 associated with the first door D1 or a second lock mechanism L2 associated with the second door D2 depending on from which reader unit R1 or R2 the credential data CD originated. As mentioned above, each access grant message AG is configured to order the lock mechanism L1 or L2 to be opened during a predetermined interval.

Naturally, according to the invention, the control node N may be configured to handle any other number of well-defined spaces and credential data receivers than two, i.e. from one and up. It should also be noted that the number of well-defined spaces (doors) and the number of credential data receivers need not be identical. On the contrary, it may very well be the case that the number of well-defined spaces (doors) is relatively large while the number of the credential data receivers is relatively small, say two; or vice versa, that the number of the credential data receivers is relatively large while the number of well-defined spaces is just one or two.

In any case, upon presentation of a piece of credential data CD to one of the reader units R1 or R2, this reader unit is configured to forward the piece of credential data CD to the credential data receiver EAC1 or EAC2 identified by the address A linked to the piece of credential data CD. Then, in response to a received piece of credential data CD, each of the first and the at least one second credential data receiver EAC1 and EAC2 is configured to check the piece of credential data CD against a database DB1 or DB2 respectively defining a set of users' access rights to the well-defined space behind the door D1 or D2 to which the reader unit R1 or R2 is associated by which the piece of credential data CD was registered. If the piece of credential data CD is found to designate an authorized user, the credential data receiver EAC1 or EAC2 is configured to cause an access grant message AG to be sent to the lock mechanism L1 or L2 ordering the lock mechanism L1 or L2 to open the door D1 or D2.

If, however, the piece of credential data CD is found not to designate an authorized user, the credential data receiver EAC1 or EAC2 is configured to refrain from causing an access grant message AG to be sent to any of the lock mechanisms L1 or L2.

Preferably, the reader units R, R1 and R2, the credential data receivers EAC, EAC1 and EAC2 and the control node N include, or are in communicative connection with at least one memory unit storing at least one computer program product, which contains software for performing the above-described actions when the computer program product is run on a processor of the reader units R, R1 and R2, the credential data receivers EAC, EAC1 and EAC2 and the control node N respectively.

In order to sum up, we will now describe the general method executed by the proposed reader unit according to the invention with reference to the flow diagram in Figure 7.

A first step 710 checks if credential data have been received,

and if so a step 720 follows. Otherwise, the procedure loops back and stays in step 710.

Step 720 reads out the address linked to the credential data, either from a memory module associated with the reader unit or from a carrier for the credential data. Preferably, to maintain adequate security and reduce the risk of fraudulent manipulation, reading out the credential data from the carrier requires access to a first encryption key in the reader unit.

After having read out the credential data, a step 730 forwards the registered credential data to the credential data receiver identified by the address linked to the registered credential data. Again, for security reasons and to reduce the risk of fraudulent manipulation, access to a second encryption key (identical to or different from the first key) is preferably required in the reader unit to enable this transmission.

A subsequent step 740 determines whether or not the user associated with the credential data is authorized. From the reader unit's point-of-view this means waiting for an access decision from the credential data receiver. If such a decision arrives within a predefined time, for instance in the form of an access grant message, a step 750 follows. Analogous to the above, sending the access decision preferably also requires access to a third encryption key, such that the reader unit can be certain that a received access decision was issued by an authorized source, e.g. one of its associated credential data receivers.

If no access decision arrives within the predefined time, the procedure loops back to step 710.

In step 750, at least one access decision is effected in response to the access decision with respect to a well-defined space and the user being associated with the registered credential data. The access decision may involve granting access to the well-defined space, registering an entry to the well-defined space or registering an exit from the well-defined space.

After step 750, the procedure loops back to step 710.

It is worth noting that, although steps 710, 720 and 730 all mention "credential data", this does not mean that an exact copy of these specific data must be received, read out and forwarded respectively. Instead, various forms of data *derived from* the credential data may be received, read out and forwarded in and from the reader unit. Thus, the term "credential data" should here be regarded as a token being passed on from the carrier.

All of the process steps, as well as any sub-sequence of steps, described with reference to Figure 7 above may be controlled by means of a programmed computer apparatus. Moreover, although the embodiments of the invention described above with reference to the drawings comprise a computer apparatus and processes performed in a computer apparatus, the invention thus also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The program may be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the process according to the invention. The program may either be a part of an operating system, or be a separate application. The carrier may be any entity or device capable of carrying the program. For example, the carrier may comprise a storage medium, such as a Flash memory, a ROM (Read Only Memory), for example a DVD (Digital Video/ Versatile Disk), a CD (Compact Disc) or a semiconductor ROM, an EPROM (Erasable Programmable Read-Only Memory), an EEPROM (Electrically Erasable Programmable Read-Only Memory), or a magnetic recording medium, for example a floppy disc or hard disc. Further, the carrier may be a transmissible carrier such as an electrical or optical signal which may be conveyed via electrical or optical cable or by radio or by other means. When the program is embodied in a signal which may be conveyed directly by a cable or other device or means, the carrier may be constituted by such cable or device or means.

Alternatively, the carrier may be an integrated circuit in which the program is embedded, the integrated circuit being adapted for performing, or for use in the performance of, the relevant processes.

The term “comprises/comprising” when used in this specification is taken to specify the presence of stated features, integers, steps or components. However, the term does not preclude the presence or addition of one or more additional features, integers, steps or components or groups thereof.

The invention is not restricted to the described embodiments in the figures, but may be varied freely within the scope of the claims.

Claims

1. A reader unit (R, R1, R2) configured to:

register credential data (CD) in respect of users seeking access to a well-defined space,

communicate with an access-control-related building component (L, L1, L2) associated with the well-defined space, and

communicate with a first credential data receiver (EAC1) for causing at least one access decision (AG) in respect of the well-defined space to be effected,

characterized in that the reader unit (R, R1, R2) is further configured to:

communicate with at least one second credential data receiver (EAC2) for causing at least one access decision (AG) in respect of the well-defined space to be effected, and

forward each registered piece of credential data (CD) to either the first credential data receiver (EAC1) or a particular one of the at least one second credential data receiver (EAC2) based on an address (A) linked to the piece of credential data (CD) which address (A) identifies the first credential data receiver (EAC1) or the particular one of the at least one second credential data receiver (EAC2), the linked address (A) being stored in:

a memory module (M, M1, M2) associated with the reader unit (R, R1, R2) or

on a carrier (C) holding the piece of credential data (CD) which carrier (C) is configured to be presented to the reader unit (R, R1, R2) for registering the piece of credential data (CD).

2. A data communication system comprising:

a reader unit (R, R1, R2) configured to register credential data (CD) in respect of users seeking access to a well-defined space,

an access-control-related building component (L, L1, L2) associated with the reader unit (R, R1, R2) and the well-defined space, and

a first credential data receiver (EAC1) configured to receive credential data (CD) registered by the reader unit (R, R1, R2) and in response thereto cause at least one access decision (AG) in respect of the well-defined space to be effected,

characterized in that

the data communication system comprises at least one second credential data receiver (EAC2) configured to receive credential data (CD) registered by the reader unit (R, R1, R2) and in response thereto cause at least one access decision (AG) in respect of the well-defined space to be effected, the reader unit (R, R1, R2) is communicatively connected to the first credential data receiver (EAC1) and the at least one second credential data receiver (EAC2), and the reader unit (R, R1, R2) is further configured to forward a registered piece of credential data (CD) to either the first credential data receiver (EAC1) or a particular one of the at least one second credential data receiver (EAC2) based on an address (A) linked to the piece of credential data (CD) which address (A) identifies the first credential data receiver (EAC1) or the particular one of the at least one second credential data receiver (EAC2), the linked address (A) being stored in:

a memory module (M, M1, M2) associated with the reader unit (R, R1, R2) or

on a carrier (C) holding the piece of credential data (CD) which carrier (C) is configured to be presented to the reader unit (R, R1, R2) for registering the piece of credential data (CD).

3. The reader unit (R, R1, R2) according to claim 1 or the data communication system according to claim 2, wherein the at least one access decision (AG) involves granting or refusing access to the well-defined space, the access-control-related building component comprises a lock mechanism (L, L1, L2) configured to selectively enable or prevent access to the well-defined space via a door (D) associated with the reader unit (R, R1, R2), and in response to a received piece of credential data

(CD), each of the first and the at least one second credential data receiver (EAC1; EAC2) is configured to:

check the piece of credential data (CD) against a database (DB1; DB2) defining a set of users' access rights to the well-defined space,

if the piece of credential data (CD) is found to designate an authorized user, causing an access grant message (AG) to be sent to the lock mechanism (L, L1, L2) ordering the lock mechanism (L, L1, L2) to open the door (D), and otherwise

refrain from causing the access grant message (AG) to be sent to the lock mechanism (L, L1, L2).

4. The reader unit (R) according to claim 1 or the data communication system according to claim 2, wherein the at least one access decision involves registering an entry to or exit from the well-defined space, and in response to a received piece of credential data (CD), each of the first and the at least one second credential data receiver (EAC1; EAC2) is configured to:

register an entry if the piece of credential data (CD) is received via a first scanner (R-IN) of the reader unit (R), and

register an exit the piece of credential data (CD) is received via a second scanner (R-OUT) of the reader unit (R).

5. The data communication system according to claim 2, comprising a control node (N) communicatively connected to the reader unit (R1) and each of the first and the at least one second credential data receiver (EAC1; EAC2), the control node (N) being configured to:

receive credential data (CD) from the reader unit (R1),

forward the received credential data (CD) to a credential data receiver (EAC1; EAC2) identified by the address (A) linked to the credential data (CD),

receive access grant messages (AG) from the first and the at least one second credential data receiver (EAC1; EAC2), and

forward the received access grant messages (AG) to the lock mechanism (L1), each access grant message (AG) being

configured to order the lock mechanism (L1) to be opened during a predetermined interval.

6. The data communication system according claim 4, wherein the control node (N) is communicatively connected to at least one reader unit (R2) in addition to said reader unit (R1), the control node (N) being further configured to

receive credential data (CD) from said additional reader unit (R2),

forward the received credential data (CD) to a credential data receiver (EAC1; EAC2) identified by the address (A) linked to the credential data (CD),

receive access grant messages (AG) from the first and the at least one second credential data receiver (EAC1; EAC2), and

forward the received access grant messages (AG) to a lock mechanism (L2) in addition to said lock mechanism (L1), each access grant message (AG) being configured to order the additional lock mechanism (L2) to be opened during a predetermined interval.

7. The data communication system according to any one of claims 5 or 6, wherein the linked addresses (A) identifying the first and the at least one second credential data receivers (EAC1; EAC2) are Internet Protocol addresses.

8. A method of communicating data in a network comprising:

registering credential data (CD) in a reader unit (R, R1, R2), the credential data (CD) representing users seeking access to a well-defined space associated to the reader unit (R, R1, R2),

forwarding any registered credential data (CD) to a credential data receiver (EAC1; EAC2) and in response thereto

effecting at least one access decision (AG) in respect of the well-defined space,

characterized by the network comprising a first credential data receiver (EAC1) and at least one second credential data

receiver (EAC2), and the method comprising

forwarding each registered piece of credential data (CD) to either the first credential data receiver (EAC1) or a particular one of the at least one second credential data receiver (EAC2) based on an address (A) linked to the piece of credential data (CD) which address (A) identifies the first credential data receiver (EAC1) or the particular one of the at least one second credential data receiver (EAC2), the linked address (A) being stored in:

a memory module (M, M1, M2) associated with the reader unit (R, R1, R2) or

on a carrier (C) holding the piece of credential data (CD) which carrier (C) is configured to be presented to the reader unit (R, R1, R2) for registering the piece of credential data (CD).

9. The method according to claim 8, wherein in response to a received piece of credential data (CD), in each of the first and the at least one second credential data receiver (EAC1; EAC2), the method comprising:

checking the piece of credential data (CD) against a database (DB1; DB2) defining a set of users' access rights to the well-defined space, if the piece of credential data (CD) is found to designate an authorized user,

causing an access grant message (AG) to be sent to a lock mechanism (L, L1, L2) configured to selectively enable or prevent access to the well-defined space via a door (D, D1, D2) associated with the reader unit (R, R1, R2), the access grant message (AG) being configured to order the lock mechanism (L, L1, L2) to open the door (D, D1, D2), and otherwise

refraining from causing the access grant message (AG) to be sent to the lock mechanism (L, L1, L2).

10. The method according to claim 8, wherein in response to a received piece of credential data (CD), in each of the first and the at least one second credential data receiver (EAC1; EAC2), the method comprising:

registering an entry to the well-defined space if the piece of credential data (CD) is received via a first scanner (R-IN) of the reader unit (R), and

registering an exit from the well-defined space the piece of credential data (CD) is received via a second scanner (R-OUT) of the reader unit (R).

11. The method according to any one of claims 8 to 10, comprising:

receiving credential data (CD) from the reader unit (R1) in a control node (N),

forwarding the received credential data (CD) from the control node (N) to a credential data receiver (EAC1; EAC2) identified by the address (A) linked to the credential data (CD),

receiving, in the control node (N), access grant messages (AG) from the first and the at least one second credential data receiver (EAC1; EAC2), and

forwarding the received access grant messages (AG) from the control node (N) to the lock mechanism (L1), each access grant message (AG) ordering the lock mechanism (L1) to be opened during a predetermined interval.

12. The method according to any one of claims 8 to 11, wherein the linked addresses (A) identifying the first and second credential data receivers (EAC1; EAC2) are Internet Protocol addresses.

13. A computer program product loadable into the memory of a computer, the computer program product comprising software, which when executed on a computer:

registers credential data in a reader unit, the credential data representing users seeking access to a well-defined space associated to the reader unit,

forwards each registered piece of credential data to either a first credential data receiver or a particular one of at least one second credential data receiver based on an address linked to

the piece of credential data which address identifies the first credential data receiver or the particular one of the at least one second credential data receiver, the linked address being stored in a memory module associated with the reader unit or on a carrier holding the piece of credential data which carrier is configured to be presented to the reader unit for registering the piece of credential data,
wherein each of said credential data receivers is configured to, in response to a piece of credential data, effect at least one access decision in respect of the well-defined space

14. A computer readable medium, containing the computer program product according to claim 13.

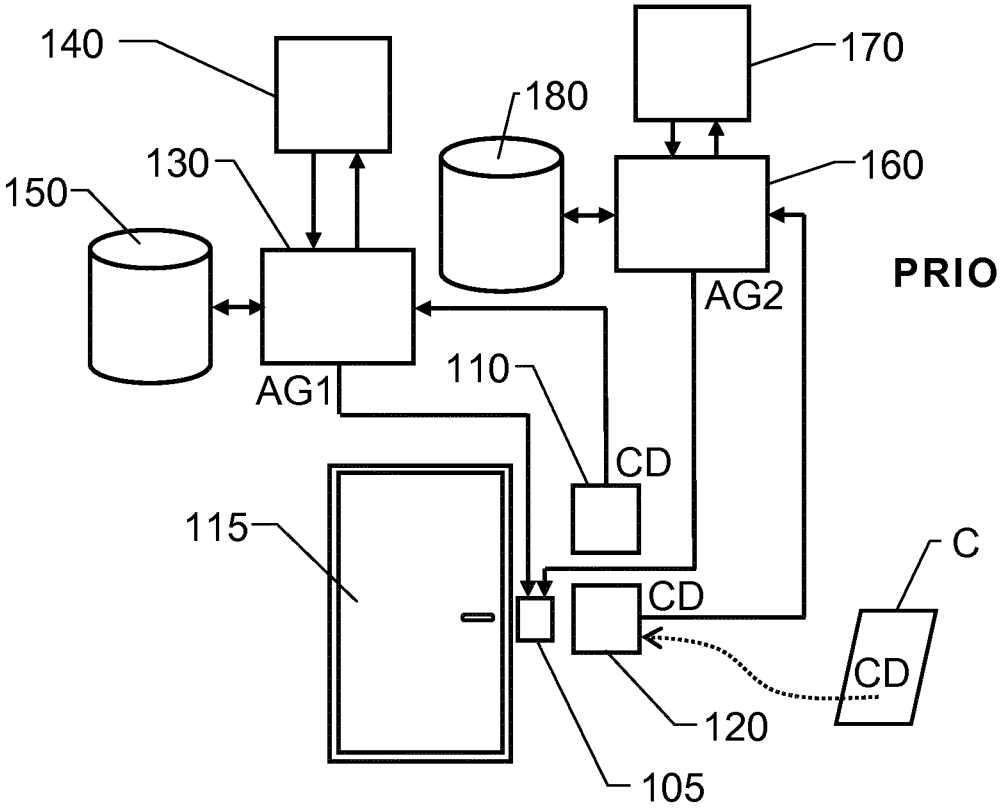
140
170
180
130
160
150
AG2
PRIOR ART
AG1
110
CD
115
C
CD
CD
120
105

Fig. 1

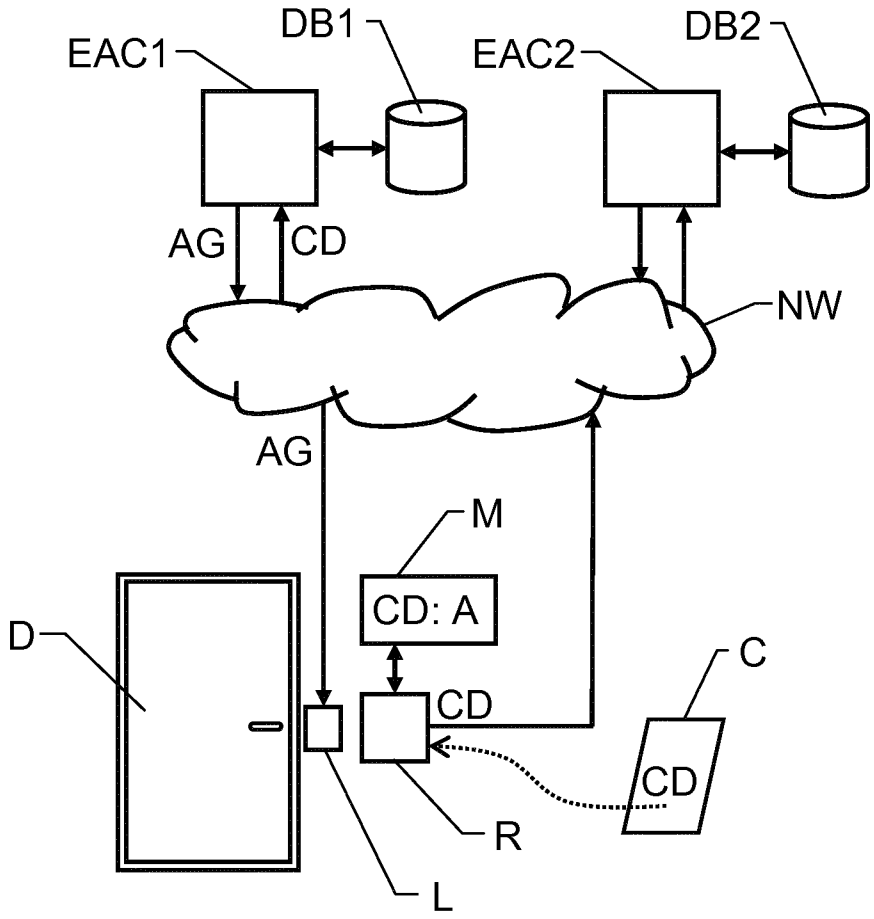
DB1
EAC1
EAC2
DB2
AG
CD
NW
AG
M
CD: A
D
C
CD
CD
R
L

Fig. 2

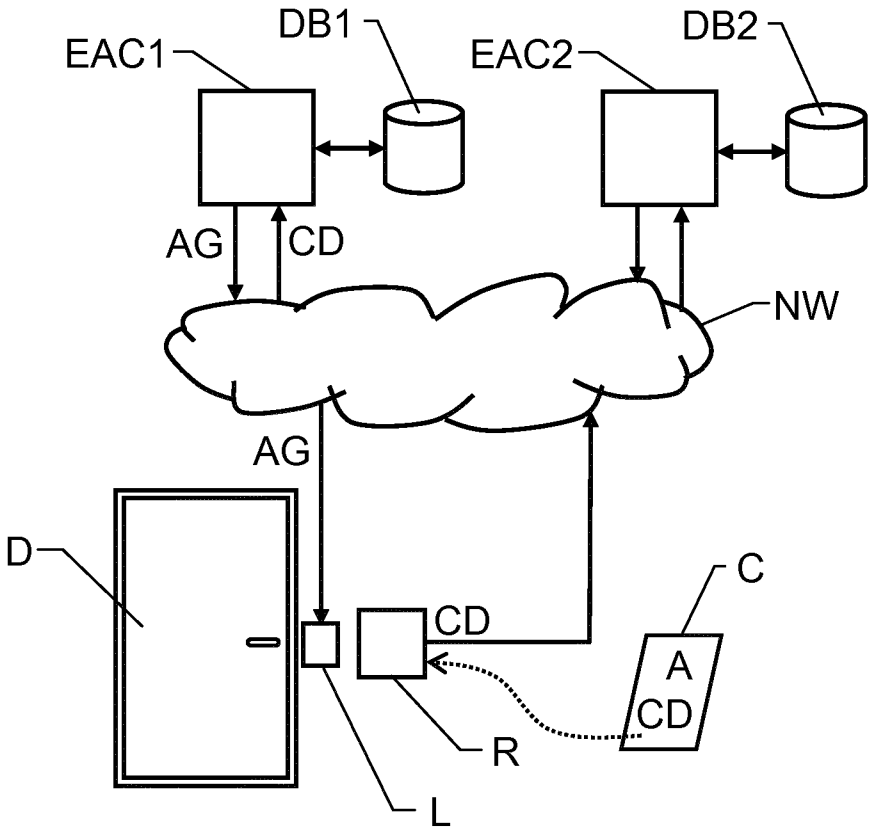

Fig. 3a

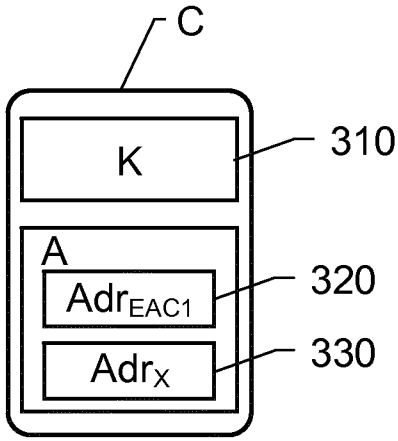

Fig. 3b

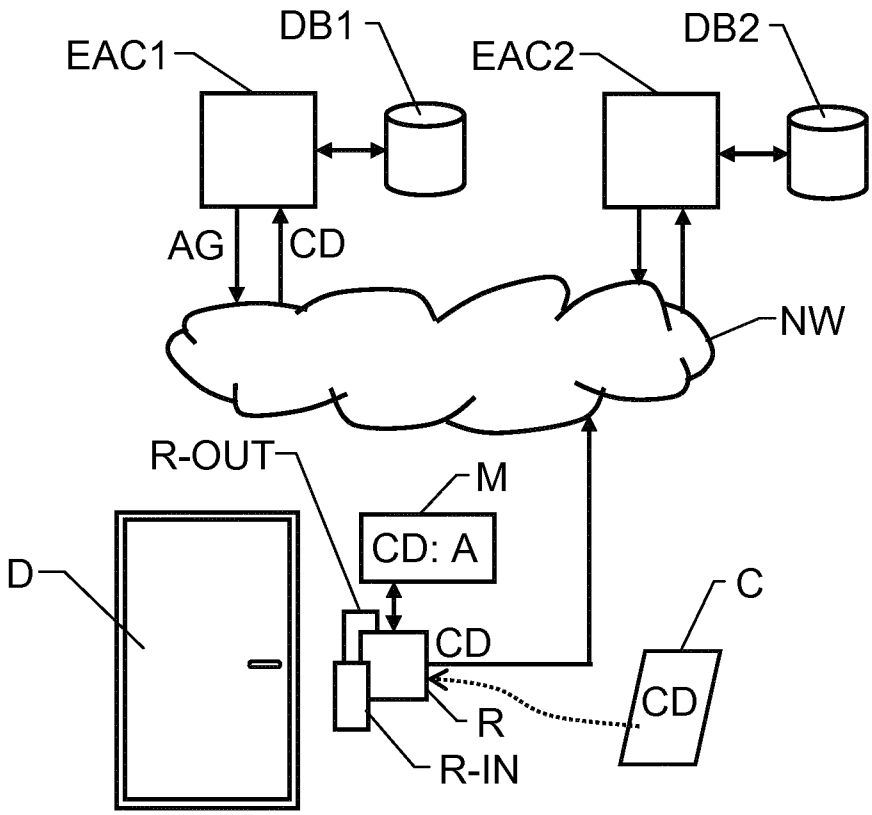

Fig. 4

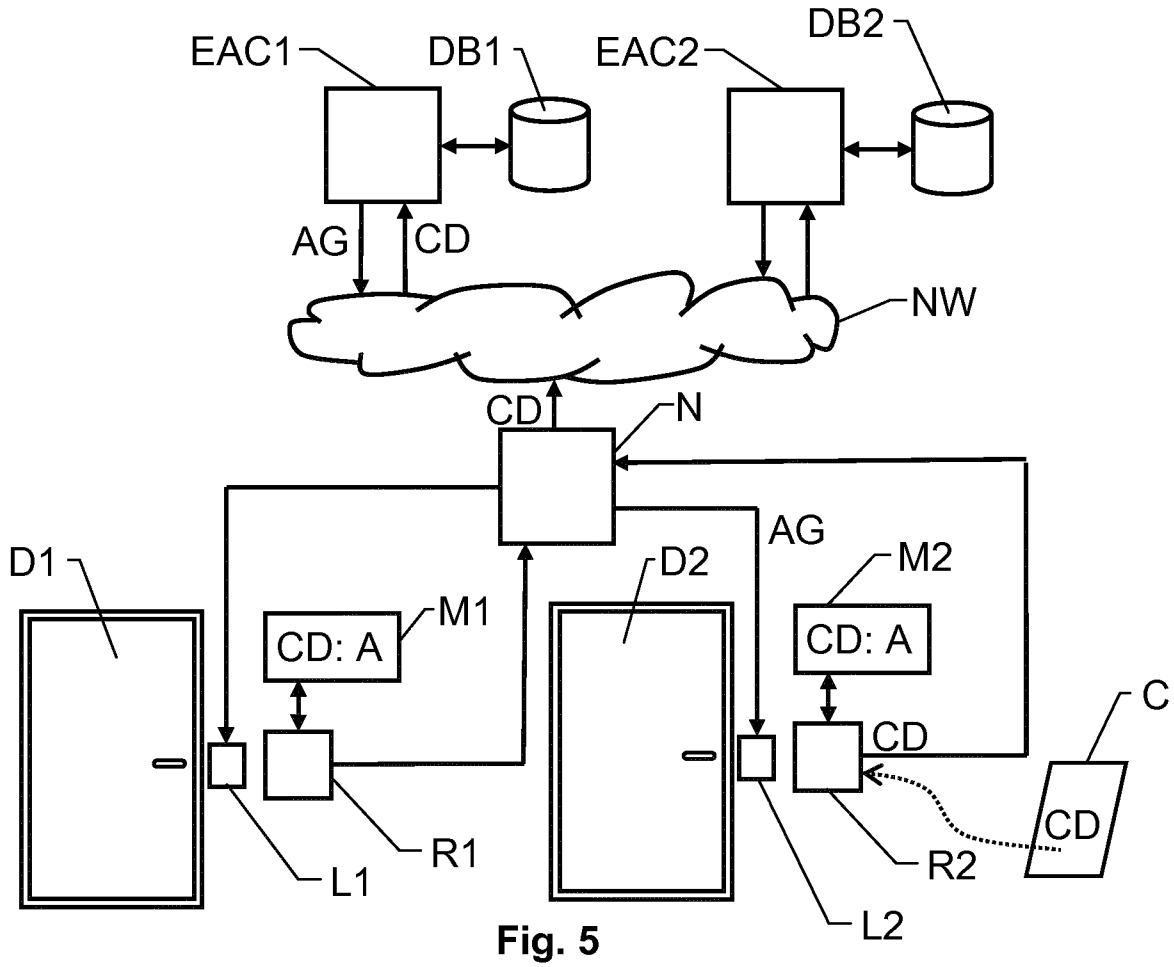
EAC1
DB1
EAC2
DB2
AG
CD
NW
CD
N
D1
AG
M2
D2
M1
CD: A
CD: A
C
CD
CD
R1
R2
L1
L2

Fig. 5

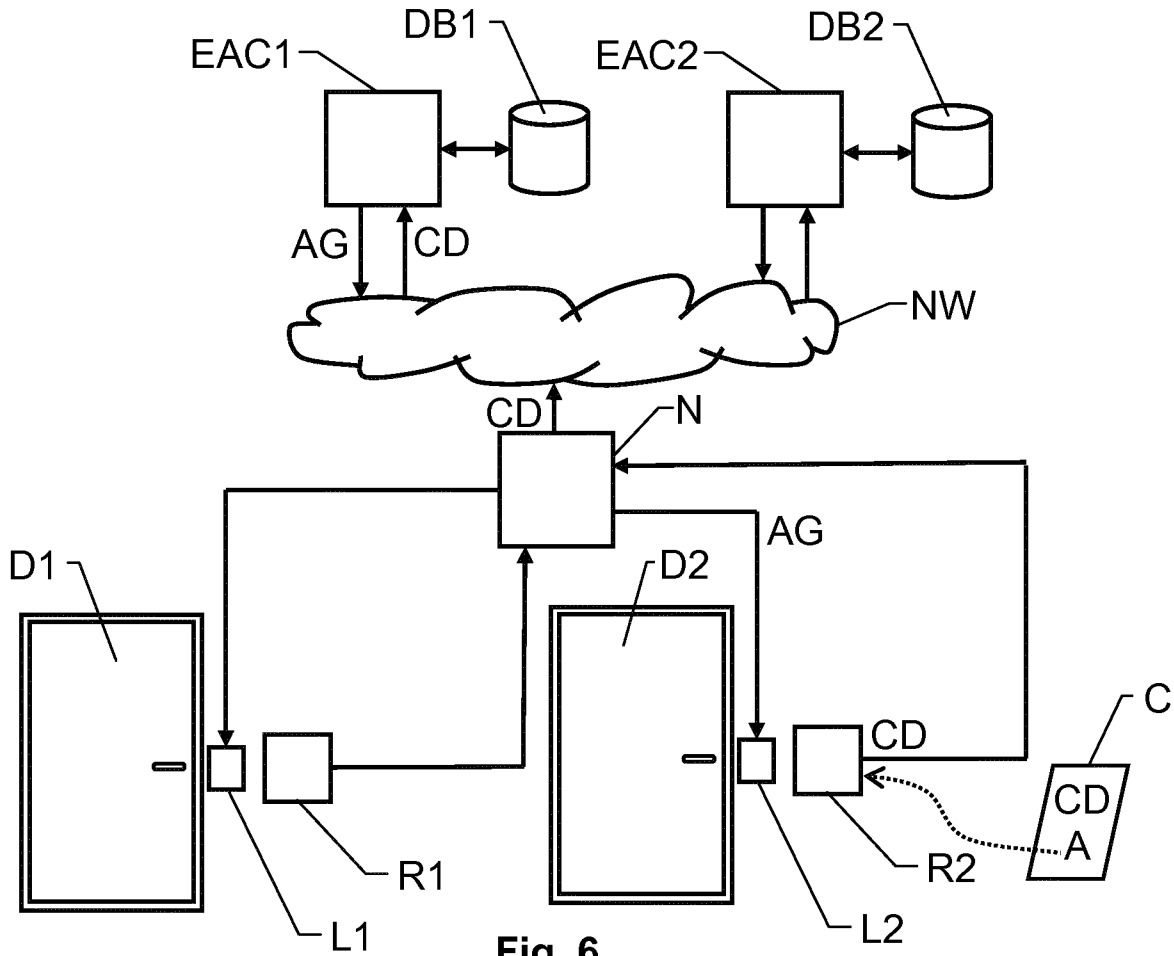
DB1
EAC1
EAC2
DB2
AG
CD
NW
CD
N
AG
D1
D2
C
CD
CD
A
R1
R2
L1
L2

Fig. 6

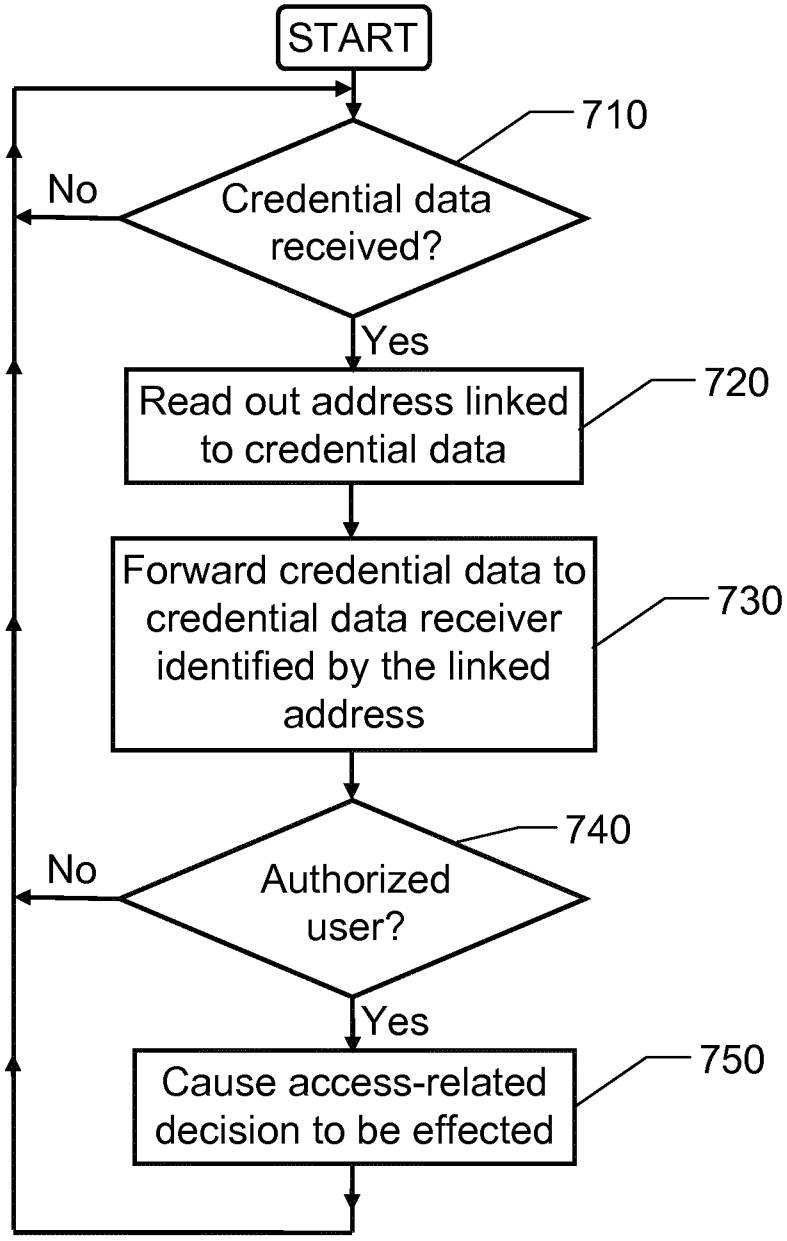
START
710
Credential data received?
No
Yes
720
Read out address linked to credential data
Forward credential data to credential data receiver identified by the linked address
730
740
Authorized user?
No
Yes
750
Cause access-related decision to be effected

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/072311

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/278901 A1 (BUENTER ADRIAN [CH]) 1 November 2012 (2012-11-01)	1-3,5, 7-9, 11-14
Y	paragraph [0007] - paragraph [0014] paragraph [0020] - paragraph [0026] figure 1 paragraph [0005]	4,6,10

Y	US 2013/093563 A1 (ADOLFSSON JOHAN [SE] ET AL) 18 April 2013 (2013-04-18)	4,6,10
A	paragraph [0033] - paragraph [0050] figures	1,2,8

A	US 2011/093928 A1 (NAKAGAWA HISASHI [JP] ET AL) 21 April 2011 (2011-04-21) paragraph [0072] - paragraph [0077] paragraph [0129] - paragraph [0149] figures 1,11-13	1,2,8, 13,14

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 January 2015	23/01/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Miltgen, Eric

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/072311

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 624 739 B1 (STOBBE ANATOLI [DE]) 23 September 2003 (2003-09-23) column 4, line 60 - column 6, line 6 figure 1 -----	1-14

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/072311

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012278901 A1	01-11-2012	EP 2691940 A1	05-02-2014
		US 2012278901 A1	01-11-2012
		WO 2012130640 A1	04-10-2012
US 2013093563 A1	18-04-2013	CN 103067350 A	24-04-2013
		EP 2584538 A1	24-04-2013
		JP 5603398 B2	08-10-2014
		JP 2013089242 A	13-05-2013
		KR 20130042447 A	26-04-2013
		US 2013093563 A1	18-04-2013
US 2011093928 A1	21-04-2011	CN 101084507 A	05-12-2007
		CN 101833796 A	15-09-2010
		CN 102831676 A	19-12-2012
		EP 1837792 A1	26-09-2007
		EP 2312487 A2	20-04-2011
		EP 2498199 A2	12-09-2012
		HK 1106840 A1	28-06-2013
		JP 4952249 B2	13-06-2012
		JP 5287963 B2	11-09-2013
		JP 5549758 B2	16-07-2014
		JP 2012018694 A	26-01-2012
		JP 2013191220 A	26-09-2013
		JP 2014132495 A	17-07-2014
		JP 2014157615 A	28-08-2014
		KR 20070092216 A	12-09-2007
		KR 20130041358 A	24-04-2013
		SG 170638 A1	30-05-2011
		US 2009058594 A1	05-03-2009
		US 2011093928 A1	21-04-2011
		WO 2006049181 A1	11-05-2006
US 6624739 B1	23-09-2003	DE 19844360 A1	13-04-2000
		EP 0990756 A2	05-04-2000
		US 6624739 B1	23-09-2003