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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2007 (08.11.2007)

PCT

(10) International Publication Number
WO 2007/126375 A1

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

(21) International Application Number:
PCT/SE2007/050266

(22) International Filing Date: 24 April 2007 (24.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0600959-1 28 April 2006 (28.04.2006) SE

(71) Applicant *(for all designated States except US)*: **SICS, SWEDISH INSTITUTE OF COMPUTER SCIENCE AB** [SE/SE]; Box 1263, S-164 29 Kista (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SADIGHI, Babak** [SE/SE]; Vallarevägen 51, S-183 51 Täby (SE). **CAO, Ling** [CN/SE]; Emmylundsvägen 1/0111, S-172 72 Solna (SE). **SEITZ, Ludwig** [DE/SE]; S:t Paulsgatan 7B, S-118 46 Stockholm (SE).

(74) Agents: **ASKERBERG, Fredrik** et al.; Groth & Co KB, Box 6107, S-102 32 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

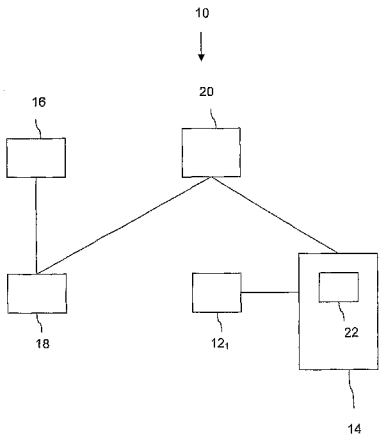
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** ACCESS CONTROL SYSTEM AND METHOD FOR OPERATING SAID SYSTEM



(57) **Abstract:** The present invention relates to a system (10) operable to control access to different physical spaces, each provided with an electrica! locking device (12_1,..., 12_n), with the aid of a programmable, mobile unit (14). The system (10) comprises an authority means (16) operable to issue access rights connected to the programmable, mobile unit (14) in the form of an authorizing data (AD), which authorizing data (AD) is sent to an authorization means (18) connected to the authority means (16), and operable to generate an alpha-numerical key for the mobile unit (14), and to send the alpha-numerical key and a unique identifier of the mobile unit (14) to an operator (20), which is connected to the authorization means (18). The operator (20) is operable to send the alpha-numerical key to the mobile unit (14) identified by the unique identifier. An electrical locking device (12_i), wherein $1 \leq i \leq n$, and the mobile unit (14) uses an authentication protocol with the alpha-numerical key to authenticate the mobËe unit (14), wherein the mobile unit, if it has been authenticated, sends the authorizing data (AD) to the electrical locking device (12_i), and if the authorizing data (AD) comprises an identifier of the electrical locking device (12_i), the mobile unit (14) is able to open the electrical locking device (12_i,) with the aid of a communication means (22) comprised in the mobile unit (14) for communication in the near field.

WO 2007/126375 A1

ACCESS CONTROL SYSTEM AND METHOD FOR OPERATING SAID SYSTEM

Field of the invention

The present invention relates, in a fist aspect to a system operable to control access to different physical spaces.

According to a second aspect, the present invention relates to a method for controlling access to different physical spaces.

According to a third aspect, the present invention relates to at least one computer software product for controlling access to different physical spaces.

Background of the invention

At present, traditional metal keys and/or passes are often used to open locks in connection with doors, whereby passes often are combined with the use of a code. When electrical locks are being used more frequently, different solutions for wireless unlocking or locking of electrical locks have been presented.

The document WO-A2-2005/066908 discloses an access control system and a method for operating said system. The system comprises an access control system (2 – 4, 8) (see figure), which controls a plurality of access points (1), e.g. doors (1) by means of respective individual physical closing mechanisms (8). At least one reader (2) and a controller (3), which is connected to the latter in order to control the closing mechanism (8), are provided at each access point (1). The system also comprises at least one access control server (4), which carries out the centralised management of access data and is connected to the respective controllers (3). The system also comprises at least one mobile telephone server (5), which is connected to the access control server (4). The mobile telephone server (5) can also be an integral component of the access control server (4). At least one access point (1) is equipped with a short-range transmitter (9), which transmits identification information that is specific to the access point in such a way that it is only received by a mobile telephone (7) located in the direct vicinity of the access point (1) and is used at least indirectly by the telephone to control the access verification process. The document discloses the use of Bluetooth or WLAN transmitters (9). As is apparent from the figure, each access point (1) has to be connected to the access control server (4) which is a drawback in relation to your idea. Another difference in relation to our solution is that the user actually has

to call the access control server (4). Moreover, authentication is performed with the aid of the calling number and a PIN code, which is not the case in your solution.

The document WO-A1-01/63425 discloses a system and method for, by means of a mobile terminal, wireless hotel search and selection, reservation/ booking, check-in, room access control, check-out and payment services for hotel customers. After successful reservation, the wireless door lock system of the reserved room receives information about the valid key token, or a secret key, from the hotel reservation/IT system. By means of the short range wireless device in the mobile wireless terminal, the key token is transmitted to nearby wireless devices associated with electrically operable door locks. On receiving the appropriate key token from the wireless device in the mobile terminal, the door lock wireless device of the reserved room can notify the associated hotel reservation/IT system of the arrival of the user for check-in, and unlocks the door. The communication protocol between the mobile terminal and the wireless door lock system is performed over a Bluetooth, Infrared or other suitable bearer. To achieve optimal security, this information could be protected in the user's terminal by means of a PIN code, fingerprint or other local authentication methods.

The document 20051201ddm France Telecom, "Focus on contact less technology", DDM du mois, France Telecom, describes briefly the use of NFC (Near Field Communication) technology integrated in a mobile telephone to open gates and barriers for instance in parking lots.

The document EP-A1-1,600,885 relates to a SIM reader/writer provided with a detachable SIM having contact and non-contact interfaces. The SIM reader/writer can be used for non-contact gate management in transportation facilities. In Figure 28 there is disclosed a perspective view of assistance in explaining a mode of using a non-contact communication device to operate a ticket gate. A non-contact communication device 201 having the function of an IC card is brought into contact with a receiving unit 208 installed in a ticket gate 207 of transportation facilities in the direction of the arrow Y. Then the receiving unit 208 of the ticket gate 207 receives an electromagnetic wave emitted by the non-contact communication device 201, and then a door 209 is opened or kept closed. The non-contact communication device 201 can be similarly used for operating the doors of a building of a corporation and the entrance of facilities.

The document US-A1-2004/0127256 relates to a mobile device that is equipped with a contact-less smart card reader/writer for conducting financial transactions with a contact-less smart card. The mobile device can be used for shopping with authentication via a telecommunication network.

The document US-A1-2005/0210283 relates to a key system 10 (see fig. 1) for locking and unlocking a door 12 of a room, house, office or other such structure. Installed in the door 12 is a lock device 14 that locks and unlocks the door 12 in cooperation with a paired key device 16. In the key system 10, the lock device 14 and key device 16 exchange key information by short-range wireless communication, the lock device 14 authenticates the key information received from the key device 16, and the door 12 is unlocked if the authentication succeeds. The key device 16 has a page button 18 for initiating transmission of the key information, and functions uniquely for transmitting the key information when the page button 18 is pressed, The short-range wireless communication technology used in this embodiment is the Bluetooth technology®.

The document US-A1-2002/0130763 describes a security system to enable authenticated access of an individual to a protected area, including a remote control unit (22) (see fig. 1) with a transponder (28), carried by the individual, which transmits an identification code group on reception of an interrogation signal. A control unit located within the protected area transmits an interrogation signal when activated by the individual, and verifies the identification code group received from the transponder. Access to the protected area will only be permitted on positive verification of the right to access. The transponder (28), contained within the remote control unit (22) is a passive transponder which obtains a supply voltage from the interrogation signal transmitted by the control unit (16) and then feeds this to a supply voltage rail. The remote control unit (22) contains a battery (34) that can be connected to the supply voltage rail (46) by means of a controllable battery coupling switch (42) via a high-resistance path when the remote control unit (22) is in its quiescent state or via a low-resistance path when the remote control unit (22) is in its active state. A pulse detector (58) obtains its supply voltage in the quiescent state of the remote control unit (22) via the high-resistance path of the battery coupling switch (42). On reception of the interrogation signal by the transponder (28), the pulse detector (58) outputs a recognition signal. A remote-field detector (64) receives the recognition signal and

outputs a remote-field signal as soon as the value of the recognition signal comes within a predetermined range.

None of the above mentioned documents presents a solution supporting the following essential features:

- At least as secure as magnetic card and smart card solutions
- Support for fine-grained access rights
- Decentralised administration of access rights
- Remote distribution and revocation of access rights (no need for face to face distribution and revocation of keys, and no need for reprogramming of locks)
- Managing access to remotely located locks with very limited power supply and no or temporary communication abilities.

Summary of the invention

The above mentioned problems are solved by a system operable to control access to different physical spaces according to Claim 1. Each physical space is provided with an electrical locking device. The system is operable with the aid of a programmable, mobile unit. The system comprises an authority means operable to issue access rights connected to said programmable, mobile unit in the form of an authorizing data (AD), which authorizing data (AD) is sent to an authorization means connected to the authority means. The authorization means is operable to generate an alphanumerical key for the programmable, mobile unit, and to send the alphanumerical key and a unique identifier of the mobile unit to an operator which is connected to the authorization means. The operator is operable to send the alphanumerical key to the mobile unit identified by the unique identifier. An electrical locking device and the mobile unit use an authentication protocol with the alphanumerical key to authenticate the mobile unit. If the mobile unit has been authenticated, it sends the authorizing data (AD) to the electrical locking device. If the authorizing data (AD) comprises an identifier of the electronic locking device, the mobile unit is able to open the electrical locking device with the aid of a communication means comprised in the mobile unit for communication in the near field.

A main advantage with this system according to the present invention, is that it supports the following essential features:

- At least as secure as magnetic card and smart card solutions
- Support for fine-grained access rights
- Decentralised administration of access rights
- Remote distribution and revocation of access rights (no need for face to face distribution and revocation of keys, and no need for reprogramming of locks)
- Managing access to remotely located locks with very limited power supply and no or temporary communication abilities.

A further advantage in this context is achieved if said unique identifier of said mobile unit is a number, and in that said authorizing data (AD) comprises an identification (ID_1; ...; ID_n) of each locking device which said mobile unit (14) should be able to open.

Furthermore, it is an advantage in this context if said alphanumerical key is a symmetric, secret key (kp), and in that a physical space Is provided with an electrical master locking device, wherein said authorization means also is operable to send said secret key (kp) and said number identifying said mobile unit to said master locking device.

A further advantage in this context is achieved if said master locking device and said mobile unit use said authentication protocol with said secret key (kp) to authenticate said mobile unit.

Furthermore, it is an advantage in this context if said master locking device is operable, after said mobile unit has been authenticated, to send an authorization request to said authorization means whereafter said authorization means also is operable to send said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit with a symmetric key (kl) (E_{kl} (kp)) to said master locking device.

A further advantage in this context is achieved if said master locking device also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit with said symmetric key (kl) (E_{kl} (kp)) to said mobile unit with the aid of

a communication means comprised in said master locking device for communication in the near field.

Furthermore, it is an advantage in this context if said mobile unit is operable to send said encrypted secret key of said mobile unit with said symmetric key (kl) (E_{kl} (kp)) to said electrical locking device, which in turn also is operable to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

A further advantage in this context is achieved if mobile unit also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device, whereby said electrical locking device is operable to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

According to another embodiment, it is an advantage if said alphanumerical key is a symmetric, secret key (kp), wherein said authorization means also is operable to generate said secret key (kp), said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit with a symmetric key (kl) (E_{kl} (kp)), and to send said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), said encrypted secret key of said mobile unit with said symmetric key (E_{kl} (kp)), and said number to said operator.

A further advantage in this context is achieved if said operator also is operable to send, besides said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit with said symmetric key (E_{kl} (kp)) to said mobile unit.

Furthermore, it is an advantage in this context if said mobile unit also is operable to establish a communication channel in the near field with said electrical locking device, and to send said encrypted secret key of said mobile unit with said symmetric key (E_{kl} (kp)) to said electrical locking device, which in turn also is operable to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

A further advantage in this context is achieved if said mobile unit also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device, whereby said

electrical locking device is operable to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

According to another embodiment, it is an advantage if said alphanumerical key is an asymmetric key pair (privP, publP), wherein said authorization means also is operable to generate said asymmetric key pair (privP, publP), a certificate (certP), and an authorizing data (AD) electronically signed by said authorization means private key (privA), ($Sign_{privA}$ (AD)) for said mobile unit, and to send said authorizing data (AD), said private key (privP) of said mobile unit, said certificate (certP), said public key (pubA) of said authorization means, said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)), and said number to said operator.

A further advantage in this context is achieved if said operator also is operable to send said authorizing data (AD), said private key (privP) of said mobile unit, said certificate (certP), said public key (pubA) of said authorization means, and said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)) to said mobile unit.

Furthermore, it is an advantage in this context if said mobile unit also is operable to establish a communication channel in the near filed with said electrical locking device, and to send said certificate (certP) to said electrical locking device, and to receive a certificate of said locking device containing its public key (privL) (certL) from said electrical locking device.

A further advantage in this context is achieved if said mobile unit and said electrical locking device are operable to authenticate each other using their certificates (certP, certL) and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

Furthermore, it is an advantage in this context if mobile unit also is operable, if said mobile unit and said electrical locking device have been authenticated, to send said authorizing data (AD) and said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)) to said electrical locking device, which verifies said signature.

The above mentioned problems are furthermore solved by a method for controlling access to different physical spaces according to Claim 18. Each physical space is provided with an electrical locking device. The method is carried

out by means of a programmable, mobile unit and a system. The method comprises the steps of:

- an authority means comprised in said system issues access rights connected to said mobile unit in the form of an authorizing data (AD);
- to send said authorizing data (AD) to an authorization means comprised in said system and connected to said authority means;
- said authorization means generates an alphanumerical key for said mobile unit;
- to send said alphanumerical key and a unique identifier of said mobile unit to an operator which is connected to said authorization means;
- said operator sends said alphanumerical key to said mobile unit identified by said unique identifier;
- wherein an electrical locking device, wherein $1 \leq i \leq n$, and said mobile unit use an authentication protocol with said alphanumerical key to authenticate said mobile unit;
- if said mobile unit has been authenticated, it sends said authorizing data (AD) to said electrical locking device;
- to verify the validity of the authorization data (AD); and
- if said authorizing data (AD) comprises an identifier of said electrical locking device, said mobile unit is able to open said electrical locking device with the aid of a communication means comprised in said mobile unit for communication in the near field.

A main advantage with this method according to the present invention, is that it support the following essential features:

- At least as secure as magnetic card and smart card solutions
- Support for fine-grained access rights
- Decentralised administration of access rights
- Remote distribution and revocation of access rights (no need for face to face distribution and revocation of keys, and no need for reprogramming of locks)
- Managing access to remotely located locks with very limited power supply and no or temporary communication abilities.

A further advantage in this context is achieved if said unique identifier of said mobile unit is a number, and in that said authorizing data (AD) comprises an identification (ID_1; ...; ID_n) of each locking device which said mobile unit should be able to open.

Furthermore, it is an advantage in this context if alphanumerical key is a symmetric, secret key (kp), and in that a physical space is provided with an electrical master locking device, wherein said method also comprises the step:

- said authorization means sends said secret key (kp) and said number identifying said mobile unit to said master locking device.

A further advantage in this context is achieved if method also comprises the step:

- to authenticate said mobile unit with the aid of said master locking device and said mobile unit using said authentication protocol with said secret key (kp).

Furthermore, it is an advantage in this context if said method also comprises the steps:

- if said mobile unit has been authenticated, with the aid of said master locking device, to send an authorization request to said authorization means; and
- with the aid of said authorization means, to send said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted secret key of said mobile unit with a symmetric key (kl) (E_{kl} (kp)) to said master locking device.

A further advantage in this context is achieved if said method also comprises the step:

- with the aid of said master locking device, to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit with said symmetric key (kl) (E_{kl} (kp)) to said mobile unit with the aid of a communication means comprised in said master locking device for communication in the near field.

Furthermore, it is an advantage in this context if said method also comprises the steps:

- with the aid of said mobile unit, to send said encrypted secret key of said mobile unit with said symmetric key (kl) (E_{kl} (kp)) to said electrical locking device; and
- with the aid of said electrical locking device, to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

A further advantage in this context is achieved if said method also comprises the steps:

- with the aid of said mobile unit, to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device; and
- with the aid of said electrical locking device, to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

According to another embodiment, it is an advantage if said alphanumerical key is a symmetric, secret key (kp), and in that said method also comprises the steps:

- with the aid of said authorization means, to generate said secret key (kp), said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit with a symmetric key (kl) (E_{kl} (kp)); and
- to send said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), said encrypted secret key of said mobile unit with said symmetric key (E_{kl} (kp)), and said number of the mobile unit to said operator.

A further advantage in this context is achieved if said method also comprises the step:

- with the aid of said operator, to send, besides said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit with said symmetric key (E_{kl} (kp)) to said mobile unit.

Furthermore, it is an advantage in this context if said method also comprises the steps:

- with the aid of said mobile unit, to establish a communication channel in the near field with said electrical locking device;

- to send said encrypted key of said mobile unit with said symmetric key (E_{kl} (kp)) to said electrical locking device; and
- with the aid of said electrical locking device, to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

A further advantage in this context is achieved if said method also comprises the steps:

- with the aid of said mobile unit, to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device; and
- with the aid of said electrical locking device, to verify the validity of said authorizing data (AD) with aid message authentication code (MAC) and said symmetric key (kl).

According to another embodiment, it is an advantage if said alphanumerical key is an asymmetric key pair (privP, publP), and in that said method also comprises the steps:

- with the aid of said authorization means, to generate said asymmetric key pair (privP, publP), a certificate (certP), and an authorizing data (AD) electronically signed by said authorization means private key (privA), ($Sign_{privA}$ (AD)) for said mobile unit; and
- -to send said authorizing data (AD), said private key (privP) of said mobile unit, said certificate (certP), said public key (pubA) of said authorization means, said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)), and said number of the mobile unit to said operator.

A further advantage in this context is achieved if said method also comprises the step:

- with the aid of said operator, to send said authorizing data (AD), said private key (privP) of said mobile unit, said certificate (certP), said public key (pubA) of said authorization means and said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)) to said mobile unit.

Furthermore, it is an advantage in this context if said method also comprises the steps:

- with the aid of said mobile unit, to establish a communication channel in the near field with said electrical locking device;
- to send said certificate (certP) to said electrical locking device; and
- to receive a certificate of said locking device containing its public key (privL) (certL) from said electrical locking device.

A further advantage in this context is achieved if said method also comprises the step:

- with the aid of said mobile unit and said electrical locking device, to authenticate each other using their certificates (certP, certL) and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

Furthermore, it is an advantage in this context if said method also comprises the step:

- if said mobile unit and said electrical locking device have been authenticated, with the aid of said mobile unit, to send said authorizing data (AD), and said authorization data electronically signed by said authorization means private key ($Sign_{privA}$ (AD)) to said electrical locking device.

The above mentioned problems are furthermore solved by at least one computer program product according to Claim 35.

A main advantage with the at least one computer program product according to the present invention, is that it/they support the following essential features:

- At least as secure as magnetic card and smart card solutions
- Support for fine-grained access rights
- Decentralised administration of access rights
- Remote distribution and revocation of access rights (no need for face to face distribution and revocation of keys, and no need for reprogramming of locks)
- Managing access to remotely located locks with very limited power supply and no or temporary communication abilities.

Embodiments of the invention will now be described, reference being made to the accompanying drawings, where:

Brief description of the drawings

Fig. 1 shows a block diagram of a first embodiment of a system operable to control access to different physical spaces according to the present invention;

Fig. 2 shows a block diagram of a second embodiment of a system operable to control access to different physical spaces according to the present invention;

Fig. 3 shows a flow chart of a first embodiment of a method for controlling access to different physical spaces according to the present invention;

Fig. 4 shows a flow chart of a second embodiment of a method for controlling access to different physical spaces according to the present invention;

Fig. 5 schematically shows a third embodiment of a system and a method for controlling access to different physical spaces according to the present invention;

Fig. 6 schematically shows a fourth embodiment of a system and method for controlling access to different physical spaces according to the present invention;

Fig. 7 schematically shows a fifth embodiment of a system and method for controlling access to different physical spaces according to the present invention; and

Fig. 8 schematically shows a number of computer program products according to the present invention.

Detailed description of preferred embodiments

In fig. 1 there is disclosed a block diagram of a first embodiment of a system 10 operable to control access to different physical spaces according to the present invention. Each physical space is provided with an electrical locking device 12_1, ..., 12_n, where n is an integer. For the sake of simplicity, in fig. 1 there is only disclosed one electrical locking device 12_1. In fig. 1 there is also disclosed a programmable, mobile unit 14 which plays an important role in this invention. The system 10 comprises an authority means 16 operable to issue access rights connected to the programmable, mobile unit 14 in the form of an authorizing data

(AD). The authorizing data (AD) is sent from the authority means 16 to an authorization means 18 connected to the authority means 16. The authorization means 18 is operable to generate an alphanumerical key for the programmable, mobile unit 14 and to send the alphanumerical key and a unique identifier for the mobile unit 14 to an operator 20. As is apparent in fig. 1, the operator 20 is connected to the authorization means 18. The operator 20 is operable to send the alphanumerical key to the mobile unit 14 identified by the unique identifier. The electrical locking device 12_1 and the mobile unit 14 use an authentication protocol with the alphanumerical key to authenticate the mobile unit 14. If the mobile unit 14 has been authenticated, it sends the authorizing data (AD) to the electrical locking device 12_1. If the authorizing data (AD) comprises an identifier of the electrical locking device 12_1, the mobile unit 14 is able to unlock/lock the electrical locking device 14 with the aid of a communication means 22 comprised in the mobile unit 14 for communication in the near field. The communication means 22 can be based on NFC technology (Near Field Communication) which is a wireless technology, which makes it possible to establish communication between two objects, for instance between a mobile device and a base that has been equipped with an ad hoc antenna. NFC's specificity is that the communication is established over a distance of a few centimetres, or even with the two objects touching. This is the main difference with other wireless technologies such as Bluetooth® and WiFi that allow communication over a much larger distance.

According to a preferred embodiment of the system 10 according to the present invention, the unique identifier of the mobile unit 14 is a number, and the authorizing data (AD) comprises an identification ID_1; ...; IC_n of each locking device 12_1; ...; 12_n which the mobile unit 14 should be able to open.

In fig. 2 there is disclosed a block diagram of a second embodiment of a system 10 operable to control access to different physical spaces according to the present invention. The same functional elements in fig. 1 and 2 have been designated with the same reference signs and will not be described in detail again. In comparison to fig. 1, fig. 2 also discloses an electrical, master locking device 24 connected both to the authorization means 18 and the mobile unit 14. In this case, the alphanumerical key is a symmetric, secret key (kp), and a physical space is provided with the master locking device 24. The authorization means 18 is also

operable to send the secret key (kp), and the number identifying the mobile unit 14 to the master locking device 24.

In a preferred embodiment of the system 10 according to the present invention, the master locking device 24 and the mobile unit 14 use the authentication protocol with the secret key (kp) to authenticate the mobile unit 14.

In another embodiment of the system 10 according to the present invention, the master locking device 24 is operable, after the mobile unit 14 has been authenticated, to send an authorization request to the authorization means 18. Thereafter, the authorization means 18 also is operable to send the authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted secret key of the mobile unit 14 with a symmetric key (kl) (E_{kl} (kp)) to the master locking device 24.

According to a further embodiment of the system, 10, the master locking device 24 also is operable to send the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)), and the encrypted secret key of the mobile unit 14 with the symmetric key (kl) (E_{kl} (kp)) to the mobile unit 14 with the aid of a communication means 26 comprised in the master locking device 24 for communication in the near field. (See fig. 2.)

According to yet another embodiment of the system 10, the mobile unit 14 also is operable to send the encrypted secret key of the mobile unit 14 with the symmetric key (kl) (E_{kl} (kp)) to the electrical locking device 12_1. The locking device 12_1 is also operable to retrieve the secret key (kp) by decrypting E_{kl} (kp) with the symmetric key (kl).

According to another embodiment of the system 10, the mobile unit 14 also is operable to send the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)) to the electrical locking device 12_1. Thereafter, the electrical locking device 12_1 is operable to verify the validity of the authorizing data (AD) with the message authentication code (MAC) and the symmetric key (kl).

According to another preferred embodiment of the system 10 according to the present invention, the alphanumerical key is a symmetric, secret key (kp) and the authorization means 18 is operable to generate the secret key (kp), the authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted secret key of the mobile unit 14 with a symmetric key (kl)

E_{kl} (kp)). The authentization means 18 sends the secret key (kp), the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)), the encrypted secret key of the mobile unit 14 with the symmetric key (E_{kl} (kp)), and the number of the mobile unit 14 to the operator 20.

According to another embodiment of the system 10, the operator 20 is also operable to send, besides the secret key (kp), the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)), and the encrypted secret key of the mobile unit 14 with the symmetric key (E_{kl} (kp)) to the mobile unit 14.

According to yet another embodiment of the system 10, the mobile unit 14 is also operable to establish a communication channel in the near field with the electrical locking device 12_1, and to send the encrypted secret key of the mobile unit 14 with the symmetric key (E_{kl} (kp)) to the electrical locking device 12_1. The locking device 12_1 is also operable to retrieve the secret key (kp) by decrypting E_{kl} (kp) with the symmetric key (kl).

According to another embodiment of the system 10, the mobile unit 14 is also operable to send the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)) to the electrical locking device 12_1, which in turn is operable to verify the validity of the authorizing data (AD) with the message authentication code (MAC) and the symmetric key (kl).

According to another embodiment of the system 10 according to the present invention, the alphanumerical key is an asymmetric key pair (privP, pubIP). The authorization means 18 is also operable to generate the asymmetric key pair (privP, pubP), a certificate (certP), and an authorizing data (AD) elctronically signed by the authorization means 18 private key (privA), ($Sign_{privA}$ (AD)) for the mobile unit 14. The authorization means 18 is also operable to send the authorizing data (AD), the private key (privP) of the mobile unit 14, the certificate (certP), the public key (pubA) of the authorization means 18, the authorization data electronically signed by the authorization means 18 private key ($Sign_{privA}$ (AD)), and the number of the mobile unit 14 to the operator 20.

According to yet another embodiment of the system 10, the operator 20 is also operable to send the authorizing data (AD), the private key (privP) of the mobile unit 14, the certificate (certP), the public key (pubA) of the authorization

means 18, and the authorization data electronically signed by the authorization means 18 private key ($Sgin_{privA}$ (AD)) to the mobile unit 14.

According to another embodiment of the system 10, the mobile unit 14 is also operable to establish a communication channel in the near field with the electrical locking device 12_1, and to send the certificate (certP) to the electrical locking device 12_1. The mobile unit 14 is also operable to receive a certificate of the locking device 12_1 containing its public key (publ. L) (CertL) from the electrical locking device 12_1.

According to yet another embodiment of the system 10, the mobile unit 14 and the electrical locking device 12_1 are operable to authenticate each other using their certificates (certP, certL), and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

According to another embodiment of the system 10, the mobile unit 14 also is operable, if the mobile unit 14 and the electrical locking device 12_1 have been authenticated, to send the authorizing data (AD) and the authorization data electronically signed by the authorization means 18 private key ($Sign_{privA}$ (AD)) to the electrical locking device 12_1.

In fig. 3 there is disclosed a flow chart of a first embodiment of a method for controlling access to different physical spaces according to the present invention. Each physical space is provided with an electrical locking device 12_1; ...; 12_n. The method is performed with the aid of a programmable, mobile unit 14 and a system 10. (See e.g. fig. 1.) The method begins at block 30. The method continues, at block 32, with the step: an authority means 16 comprised in the system 10 issues access rights connected to the mobile unit 14 in the form of an authorizing data (AD). Thereafter, at block 34, the method continues with the step: to send the authorizing data (AD) to an authorization means 18 comprised in the system 10 and connected to the authority means 16. The method continues at block 36, with the step: the authorization means 18 generates an alphanumerical key for the mobile unit 14. Thereafter, at block 38, the method continues with the step: to send the alphanumerical key and a unique identifier of the mobile unit 14 to an operator 20 which is connected to the authorization means 18, The method continues, at block 40, with the step: the operator 20 sends the alphanumerical key to the mobile unit 14 identified by the unique identifier. Thereafter, at block 42, the method continues with the step: an electrical locking device 12_1 and the mobile

unit 14 use an authentication protocol with the alphanumerical key to authenticate the mobile unit 14. The method continues, at block 44, with the step: if the mobile unit 14 has been authenticated, it sends the authorizing data (AD) to the electrical locking device 12_1. Thereafter, at block 45, the method continues with the step: to verify the validity of the authorization data (AD). Thereafter, at block 46, the method continues with the step: if the authorizing data (AD) comprises an identifier of the electrical locking device 12_1 the mobile unit 14 is able to open the electrical locking device 12_1, with the aid of a communication means 22 comprised in the mobile unit 14 for communication in the near field. The method is completed at block 48.

According to another embodiment of the method according to the present invention, the unique identifier of the mobile unit 14 is a number, and the authorizing data (AD) comprises an identification (ID_1; ...; ID_n) of each locking device 12_1; ...; 12_n which the mobile unit 14 should be able to open.

In fig. 4 there is disclosed a flow chart of a second embodiment of a method for controlling access to different physical spaces according to the present invention. In this embodiment, the alphanumerical key is a symmetric, secret key (kp), and a physical space is provided with an electrical master locking device 24. (See fig. 2.) This method also comprises, besides the steps of fig. 3, the following steps: The method also begins at block 50. The method continues, at block 52, with the step: to send the secret key (kp) and the number identifying the mobile unit 14 to the master locking device 24. Thereafter, at block 54, the method continues with the step: to authenticate the mobile unit 14 with the aid of the master locking device 24 using the authentication protocol with the secret key (kp). The method continues, at block 56, with the step: if the mobile unit 14 has been authenticated, the master locking device 24 sends an authorization request to the authorization means 18. Thereafter, at block 58, the method continues with the step: with the aid of the authorization means 18, to send the authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted secret key of the mobile unit 14 with a symmetric key (kl) (E_{kl}(kp)) to the master locking device 24. The method continues, at block 60, with the step: with the aid of the master locking device 24, to send the authorizing data (AD) concatenated with the message authentication code (MAC_{kl} (AD)), and the encrypted secret key of the mobile unit 14 with the symmetric key (kl) (E_{kl} (kp)) to the mobile unit 14 with

the aid of a communication means 26 comprised in the master locking device 24 for communication in the near field. The method is completed at step 62.

According to another embodiment of the method, it also comprises the steps:

- with the aid of said mobile unit 14, to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device 12_1; and
- with the aid of said electrical locking device 12_1, to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

According to yet another embodiment of the method, it also comprises the steps:

- with the aid of said authorization means 18, to generate said secret key (kp), said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit (14) with a symmetric key (kl) (E_{kl} (kp)); and
- to send said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), said encrypted secret key of said mobile unit 14 with said symmetric key (E_{kl} (kp)), and said number to said operator 20.

According to another embodiment of the method, it also comprises the step:

- with the aid of said operator 20, to send, besides said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit 14 with said symmetric key (E_{kl} (kp)) to said mobile unit 14.

According to a further embodiment of the method it also comprises the steps:

- with the aid of said mobile unit 14, to establish a communication channel in the near field with said electrical locking device 12_1;
- to send said encrypted key of said mobile unit 14 with said symmetric key (E_{kl} (kp)) to said electrical locking device 12_1; and
- -with the aid of said electrical locking device 12_1, to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

According to yet another embodiment of the method, it also comprises the steps:

- with the aid of said mobile unit 14, to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device 12_1; and
- with the aid of said electrical locking device 12_1, to verify the validity of said authorizing data (AD) with aid message authentication code (MAC) and said symmetric key (kl).

According to another embodiment of the method, the alphanumerical key is an asymmetric key pair (privP, publP). The method also comprises the steps:

- with the aid of said authorization means 18, to generate said asymmetric key pair (privP, publP), a certificate (certP), and an aces control list (AD) electronically signed by said authorization means 18 private key (privA), ($Sign_{privA}$ (AD)) for said mobile unit 14; and
- -to send said authorizing data (AD), said private key (privP) of said mobile unit 14, said certificate (certP), said public key (pubA) of said authorization means 18, said authorization data electronically signed by said authorization means 18 private key ($Sign_{privA}$ (AD)), and said number to said operator 20.

According to yet another embodiment of the method, it also comprises the step:

- with the aid of said operator 20, to send said authorizing data (AD), said private key (privP) of said mobile unit 14, said certificate (certP), said public key (pubA) of said authorization means 18 and said authorization data electronically signed by said authorization means 18 private key ($Sign_{privA}$ (AD)) to said mobile unit.

According to another embodiment of the method, it also comprises the steps:

- with the aid of said mobile unit 14, to establish a communication channel in the near field with said electrical locking device 12_1;
- to send said certificate (certP) to said electrical locking device 12_1; and
- to receive a certificate of said locking device 12_1 containing its public key (privL) (certL) from said electrical locking device 12_1.

According to yet another embodiment of the method, it also comprises the step:

- with the aid of said mobile unit 14 and said electrical locking device 12_1, to authenticate each other using their certificates (certP, certL) and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

According to another embodiment of the method, it also comprises the step:

- if said mobile unit 14 and said electrical locking device 12_1 have been authenticated, with the aid of said mobile unit 14, to send said authorizing data (AD), and said authorization data electronically signed by said authorization means 18 private key ($Sign_{privA}$ (AD)) to said electrical locking device 12_1.

In fig. 5 there is schematically disclosed a third embodiment of a system and method for controlling access to different physical spaces according to the present invention. The message flow shown in fig. 5 is described below:

1) The authority 16 sends both the mobile phone number and the AD to the authorization server 18 via a secure connection.
2) The authorization server 18 generates a secret key "kp" for the mobile phone 14. Then, the server 18 sends the kp as well as the mobile phone number to both the master lock 24 and the OTA (Over The Air) operator 20 via a secure connection
3) The OTA operator 20 sends the secret key (kp) to the SIM card of the mobile phone 14 by using some OTA technique.
4) The master lock 24 and the mobile phone 14 use the Challenge Handshake Authentication protocol with kp to authenticate the phone 14.
5) After the mobile phone 14 has been authenticated, the master lock 24 sends an authorization request to the authorization server 18.
6) The authorization server 18 sends back an AD concatenated with a message authentication code "MAC" and an encrypted secret key of the phone "E_{kl}(kp)" to the master lock 24.
7) The master lock 24 forwards the E_{kl}(kp) and the AD concatenated with *MAC* to the mobile phone 14 using NFC.

8) When the mobile phone 14 comes to a simple lock 12_1, it sends the $E_{kl}(kp)$ to the simple lock 12_1. The simple lock 12_1 retrieves kp by decrypting $E_{kl}(kp)$ with kl.
9) Then, the mobile phone 14 and the simple lock 12_1 use the Challenge Handshake Authentication protocol with kp to authenticate the phone 14.
10) If the mobile phone 14 has been authenticated, it sends an *AD* concatenated with MAC to the simple lock 12_1. The simple lock 12_1 verifies the validity of the AD with the MAC and kl.

Finally, if the number of the simple lock 12_1 is in the *AD*, and all the authorization conditions are fulfilled, the lock is opened.

In fig. 6 there is schematically disclosed a fourth embodiment of a system and a method for controlling access to different physical spaces according to the present invention. The message flow shown in fig. 6 is described below:

1) The authority 16 sends both the mobile phone number and the AD to the authorization server 18 via a secure connection.
2) The authorization server 18 generates a secret key "kp" , an AD concatenated with a message authentication code "MAC" and an encrypted secret key "$E_{kl}(kp)$" for the mobile phone 14. Then, the server 18 sends the kp , $E_{kl}(kp)$, AD, MAC as well as the mobile phone number to the OTA operator 20 via a secure connection.
3) The OTA operator 20 sends the kp , $E_{kl}(kp)$, AD and MAC to the SIM card of the mobile phone 14 by using some OTA technique.
4) The mobile phone 14 establishes a NFC communication channel with the lock12_1 and sends the $E_{kl}(kp)$ to the lock 12_1. The lock 12_1 retrieves kp by decrypting $E_{kl}(kp)$ with kl.
5) Then, the mobile phone 14 and the simple lock 12_1 use the Challenge Handshake Authentication protocol with kp to authenticate the phone 14.
6) If the mobile phone 14 has been authenticated, it sends AD concatenated with MAC to the lock12_1. The simple lock 12_1 verifies the validity of the AD with the MAC and kl.

Finally, if the number of the simple lock 12_1 is in the *AD*, and all the authorization conditions are fulfilled, the lock is opened.

In fig. 7 there is schematically disclosed a fifth embodiment of a system and method for controlling access to different physical spaces according to the present invention. The message flow shown in fig. 7 is described below:

1) The authority 16 sends both the mobile phone number and the AD to the authorization server 18 via a secure connection.
2) The authorization server 18 generates an asymmetric key pair (privP and pubP), a certificate (certP) and an AD signature signed by the authorization server's private key ($Sign_{privA}(AD)$) for the mobile phone 14. Then, the server 18 sends the AD, privP, certP, $Sign_{privA}(AD)$, mobile phone number as well as the authorization server's public key (pubA) to the OTA operator 20 via a secure connection.
3) The OTA operator 20 sends the AD, privP, certP, $Sign_{privA}(AD)$, and pubA to the SIM card of the mobile phone 14 by using OTA technique.
4) The mobile phone 14 establishes a NFC communication channel with the lock 12_1 and exchanges the certificate with the lock 12_1.
5) Then, the mobile phone 14 and the simple lock 12_1 use the two-way Authentication protocol to authenticate each other using their certificates and their private keys.
6) If both sides have been authenticated, the mobile phone 14 sends the AD and $Sign_{privA}(AD)$ to the lock 12_1.

Finally, if the number of the simple lock is in the AD, and all the authorization conditions are fulfilled, the lock is opened.

Symbol	Meaning
AD	Authorization Data Contains the ids of the locks the user should be able to open
privP	Private key of the mobile phone
pubP	Public key of the mobile phone
$E_k(m)$	Encryption of message m with symmetric key k
$MAC_k(m)$	Message authentication code of m with symmetric key k. protects message integrity of m.
Kp	Symmetric key of the phone
Kl	Symmetric key shared between the locks
pubL	Public key of locks
$Sign_k(m)$	Signature of m with private key k. Protects message integrity of m.

privA	Private key of the authorization server
pubA	Public key of the authorization server
privL	Private key of locks
certP	Certification of the phone containing its public key. Signed with privA
certL	Certification of locks containing its public key. Signed with privA

In Fig. 8, some computer program products $102_1,\ldots,102_n$ according to the present invention are schematically shown. In Fig. 8, n different digital computers $100_1,\ldots,100_n$ are shown, where n is an integer. In Fig. 8, n different computer program products $102_1,\ldots,102_n$ are shown, here shown in the form of CD discs. The different computer program products $102_1,\ldots,102_n$ are directly loadable in the internal memory of the n different digital computers $100_1,\ldots,100_n$. Each computer program product $102_1,\ldots,102_n$ comprises software code portions for executing a part of or all the steps according to Fig. 3 or 4 when the product/products $102_1,\ldots,102_n$ are run on said computer $100_1,\ldots,100_n$. The computer program products $102_1,\ldots,102_n$ may, for instance, be in the form of diskettes, RAM discs, magnetic tapes, magneto-optical discs or some other suitable products.

The invention is not limited to the described embodiments. It will be evident for those skilled in the art that many different modifications are feasible within the scope of the following claims.

CLAIMS

1. A system (10) operable to control access to different physical spaces, each provided with an electrical locking device (12_1, ..., 12_n), with the aid of a programmable, mobile unit (14), **characterized** in that said system (10) comprises an authority means (16) operable to issue access rights connected to said programmable, mobile unit (14) in the form of an authorizing data (AD), which authorizing data (AD) is sent to an authorization means (18) connected to said authority means (16) and operable to generate an alphanumerical key for said programmable, mobile unit (14) and to send said alphanumerical key and a unique identifier of said mobile unit (14) to an operator (20), which is connected to said authorization means (18), wherein said operator (20) is operable to send said alphanumerical key to said mobile unit (14) identified by said unique identifier, wherein an electrical locking device (12_i), wherein $1 \leq i \leq n$, and said mobile unit (14) uses an authentication protocol with said alphanumerical key to authenticate said mobile unit (14), wherein said mobile unit (14), if it has been authenticated, sends said authorizing data (AD) to said electrical locking device (12_i), and if said authorizing data (AD) comprises an identifier of said electrical locking device (12_i) said mobile unit (14) is able to open said electrical locking device (12_i) with the aid of a communication means (22) comprised in said mobile unit (14) for communication in the near field.

2. A system (10) operable to control access to different physical spaces according to Claim 1, **characterized** in that said unique identifier of said mobile unit (14) is a number, and in that said authorizing data (AD) comprises an identification (ID_1; ...; ID_n) of each locking device (12_1, ..., 12_n) which said mobile unit (14) should be able to open.

3. A system (10) operable to control access to different physical spaces according to Claim 2, **characterized** in that said alphanumerical key is a symmetric, secret key (kp), and in that a physical space Is provided with an electrical master locking device (24), wherein said authorization means (18) also is operable to send said secret key (kp) and said number identifying said mobile unit (14) to said master locking device (24).

4. A system (10) operable to control access to different physical spaces according to Claim 3, **characterized** in that said master locking device (24) and said mobile unit (14) use said authentication protocol with said secret key (kp) to authenticate said mobile unit (14).

5. A system (10) operable to control access to different physical spaces according to Claim 4, **characterized** in that said master locking device (24) is operable, after said mobile unit (14) has been authenticated, to send an authorization request to said authorization means (18) whereafter said authorization means (18) also is operable to send said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit (14) with a symmetric key (kl) (E_{kl} (kp)) to said master locking device (24).

6. A system (10) operable to control access to different physical spaces according to Claim 5, **characterized** in that said master locking device (24) also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit (14) with said symmetric key (kl) (E_{kl} (kp)) to said mobile unit (14) with the aid of a communication means (26) comprised in said master locking device (24) for communication in the near field.

7. A system (10) operable to control access to different physical spaces according to any one of Claims 1 – 6, **characterized** in that said mobile unit (14) is operable to send said encrypted secret key of said mobile unit (14) with said symmetric key (kl) (E_{kl} (kp)) to said electrical locking device (12_i), which in turn also is operable to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

8. A system (10) operable to control access to different physical spaces according to Claim 7, **characterized** in that said mobile unit (14) also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device (12_i), whereby said electrical

locking device (12_i) is operable to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

9. A system (10) operable to control access to different physical spaces according to Claim 2, **characterized** in that said alphanumerical key is a symmetric, secret key (kp), wherein said authorization means (18) also is operable to generate said secret key (kp), said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit (14) with a symmetric key (kl) (E_{kl} (kp)), and to send said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), said encrypted secret key of said mobile unit (14) with said symmetric key (E_{kl} (kp)), and said number to said operator (20).

10. A system (10) operable to control access to different physical spaces according to Claim 9, **characterized** in that said operator (20) also is operable to send, besides said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit (14) with said symmetric key (E_{kl} (kp)) to said mobile unit (14).

11. A system (10) operable to control access to different physical spaces according to Claim 10, **characterized** in that said mobile unit (14) also is operable to establish a communication channel in the near field with said electrical locking device (12_i), and to send said encrypted secret key of said mobile unit (14) with said symmetric key (E_{kl} (kp)) to said electrical locking device (12_i), which in turn also is operable to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

12. A system (10) operable to control access to different physical spaces according to Claim 11, **characterized** in that said mobile unit (14) also is operable to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device (12_i), whereby said electrical locking device (12_i) is operable to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

13. A system (10) operable to control access to different physical spaces according to Claim 2, **characterized** in that said alphanumerical key is an asymmetric key pair (privP, publP), wherein said authorization means (18) also is operable to generate said asymmetric key pair (privP, publP), a certificate (certP), and an authorizing data (AD) electronically signed by said authorization means (18) private key (privA), ($Sign_{privA}$ (AD)) for said mobile unit (14), and to send said authorizing data (AD), said private key (privP) of said mobile unit (14), said certificate (certP), said public key (pubA) of said authorization means (18), said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)), and said number to said operator (20).

14. A system (10) operable to control access to different physical spaces according to Claim 13, **characterized** in that said operator (20) also is operable to send said authorizing data (AD), said private key (privP) of said mobile unit (14), said certificate (certP), said public key (pubA) of said authorization means (18), and said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)) to said mobile unit (14).

15. A system (10) operable to control access to different physical spaces according to Claim 14, **characterized** in that said mobile unit (14) also is operable to establish a communication channel in the near filed with said electrical locking device (12_i), and to send said certificate (certP) to said electrical locking device (12_i), and to receive a certificate of said locking device (12_i) containing its public key (privL) (certL) from said electrical locking device (12_i).

16. A system (10) operable to control access to different physical spaces according to Claim 15, **characterized** in that said mobile unit (14) and said electrical locking device (12_i) are operable to authenticate each other using their certificates (certP, certL) and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

17. A system (10) operable to control access to different physical spaces according to Claim 16, **characterized** in that said mobile unit (14) also is operable, if said mobile unit (14) and said electrical locking device (12_i) have been

authenticated, to send said authorizing data (AD) and said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)) to said electrical locking device (12_i), which verifies said signature.

18 A method for controlling access to different physical spaces, each provided with an electrical locking device (12_1; ...; 12_n), with the aid of a programmable, mobile unit (14) and with the aid of a system (10), wherein said method comprises the steps:

- an authority means (16) comprised in said system (10) issues access rights connected to said mobile unit (14) in the form of an authorizing data (AD);
- to send said authorizing data (AD) to an authorization means (18) comprised in said system (10) and connected to said authority means (16);
- said authorization means (18) generates an alphanumerical key for said mobile unit (14);
- to send said alphanumerical key and a unique identifier of said mobile unit (14) to an operator (20) which is connected to said authorization means (18);
- said operator (20) sends said alphanumerical key to said mobile unit (14) identified by said unique identifier;
- wherein an electrical locking device (12_i), wherein $1 \leq i \leq n$, and said mobile unit (14) use an authentication protocol with said alphanumerical key to authenticate said mobile unit (14);
- if said mobile unit (14) has been authenticated, it sends said authorizing data (AD) to said electrical locking device (12_i);
- to verify the validity of the authorization data (AD); and
- if said authorizing data (AD) comprises an identifier of said electrical locking device (12_i), said mobile unit (14) is able to open said electrical locking device (12_i) with the aid of a communication means (22) comprised in said mobile unit (14) for communication in the near field.

19. A method for controlling access to different physical spaces according to Claim 18, **characterized** in that said unique identifier of said mobile unit (14) is a number, and in that said authorizing data (AD) comprises an identification (ID_1; ...;

ID_n) of each locking device (12_1; ... 12_n) which said mobile unit (14) should be able to open.

20. A method for controlling access to different physical spaces according to Claim 19, **characterized** in that said alphanumerical key is a symmetric, secret key (kp), and in that a physical space is provided with an electrical master locking device (24), wherein said method also comprises the step:

- said authorization means (18) sends said secret key (kp) and said number identifying said mobile unit (14) to said master locking device (24).

21. A method for controlling access to different physical spaces according to Claim 20, **characterized** in that said method also comprises the step:

- to authenticate said mobile unit (14) with the aid of said master locking device (24) and said mobile unit (14) using said authentication protocol with said secret key (kp).

22. A method for controlling access to different spaces according to Claim 21, **characterized** in that said method also comprises the steps:

- if said mobile unit (14) has been authenticated, with the aid of said master locking device (24), to send an authorization request to said authorization means (18); and
- with the aid of said authorization means (18), to send said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted secret key of said mobile unit (14) with a symmetric key (kl) (E_{kl} (kp)) to said master locking device (24).

23. A method for controlling access to different spaces according to Claim 22, **characterized** in that said method also comprises the step:

- with the aid of said master locking device (24), to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), and said encrypted secret key of said mobile unit (14) with said symmetric key (kl) (E_{kl} (kp)) to said mobile unit (14) with the aid of a communication means (26) comprised in said master locking device (24) for communication in the near field.

24. A method for controlling access to different physical spaces according to any one of Claim 18 – 23, **characterized** in that said method also comprises the steps:

- with the aid of said mobile unit (14), to send said encrypted secret key of said mobile unit (14) with said symmetric key (kl) (E_{kl} (kp)) to said electrical locking device (12_i); and
- with the aid of said electrical locking device (12_i), to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

25. A method for controlling access to different physical spaces according to Claim 24, **characterized** in that said method also comprises the steps:

- with the aid of said mobile unit (14), to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device (12_i); and
- with the aid of said electrical locking device (12_i), to verify the validity of said authorizing data (AD) with said message authentication code (MAC) and said symmetric key (kl).

26. A method for controlling access to different physical spaces according to Claim 19, **characterized** in that said alphanumerical key is a symmetric, secret key (kp), and in that said method also comprises the steps:

- with the aid of said authorization means (18), to generate said secret key (kp), said authorizing data (AD) concatenated with a message authentication code (MAC_{kl} (AD)), and an encrypted, secret key of said mobile unit (14) with a symmetric key (kl) (E_{kl} (kp)); and
- to send said secret key (kp), said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)), said encrypted secret key of said mobile unit (14) with said symmetric key (E_{kl} (kp)), and said number of the mobile unit (14) to said operator (20).

27. A method for controlling access to different physical spaces according to Claim 26, **characterized** in that said method also comprises the step:

- with the aid of said operator (20), to send, besides said secret key (kp), said authorizing data (AD) concatenated with said message authentication code

(MAC_{kl} (AD)), and said encrypted secret key of said mobile unit (14) with said symmetric key (E_{kl} (kp)) to said mobile unit (14).

28. A method for controlling access to different physical spaces according to Claim 27, **characterized** in that said method also comprises the steps:

- with the aid of said mobile unit (14), to establish a communication channel in the near field with said electrical locking device (12_i);
- to send said encrypted key of said mobile unit (14) with said symmetric key (E_{kl} (kp)) to said electrical locking device (12_i); and
- with the aid of said electrical locking device (12_i), to retrieve said secret key (kp) by decrypting E_{kl} (kp) with said symmetric key (kl).

29. A method for controlling access to different physical spaces according to Claim 28 **characterized** in that said method also comprises the steps:

- with the aid of said mobile unit (14), to send said authorizing data (AD) concatenated with said message authentication code (MAC_{kl} (AD)) to said electrical locking device (12_i); and
- with the aid of said electrical locking device (12_i), to verify the validity of said authorizing data (AD) with aid message authentication code (MAC) and said symmetric key (kl).

30. A method for controlling access to different physical spaces according to Claim 19, **characterized** in that said alphanumerical key is an asymmetric key pair (privP, publP), and in that said method also comprises the steps:

- with the aid of said authorization means (18), to generate said asymmetric key pair (privP, publP), a certificate (certP), and an authorizing data (AD) electronically signed by said authorization means (18) private key (privA), ($Sign_{privA}$ (AD)) for said mobile unit (14); and
- -to send said authorizing data (AD), said private key (privP) of said mobile unit (14), said certificate (certP), said public key (pubA) of said authorization means (18), said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)), and said number of the mobile unit (14) to said operator (20).

31. A method for controlling access to different physical spaces according to Claim 30, **characterized** in that said method also comprises the step:

- with the aid of said operator (20), to send said authorizing data (AD), said private key (privP) of said mobile unit (14), said certificate (certP), said public key (pubA) of said authorization means (18) and said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)) to said mobile unit.

32. A method for controlling access to different physical spaces according to Claim 31, **characterized** in that said method also comprises the steps:

- with the aid of said mobile unit (14), to establish a communication channel in the near field with said electrical locking device (12_i);
- to send said certificate (certP) to said electrical locking device (12_i); and
- to receive a certificate of said locking device (12_i) containing its public key (privL) (certL) from said electrical locking device (12_i).

33. A method for controlling access to different physical spaces according to Claim 32, **characterized** in that said method also comprises the step:

- with the aid of said mobile unit (14) and said electrical locking device (12_i), to authenticate each other using their certificates (certP, certL) and their private keys (privP, privL) with the aid of a two-way Authentication protocol.

34. A method for controlling access to different physical spaces according to Claim 33, **characterized** in that said method also comprises the step:

- if said mobile unit (14) and said electrical locking device (12_i) have been authenticated, with the aid of said mobile unit (14), to send said authorizing data (AD), and said authorization data electronically signed by said authorization means (18) private key ($Sign_{privA}$ (AD)) to said electrical locking device (12_i).

35. At least one computer program product (102_1, ..., 102_n) directly loadable into the internal memory of at least one digital computer (100_1, ..., 100_n), comprising software code portions for performing the steps of Claim 18 when said at least one product (102_1, ..., 102_n) is/are run on said at least one computer

$(100_1, \ldots, 100_n)$.

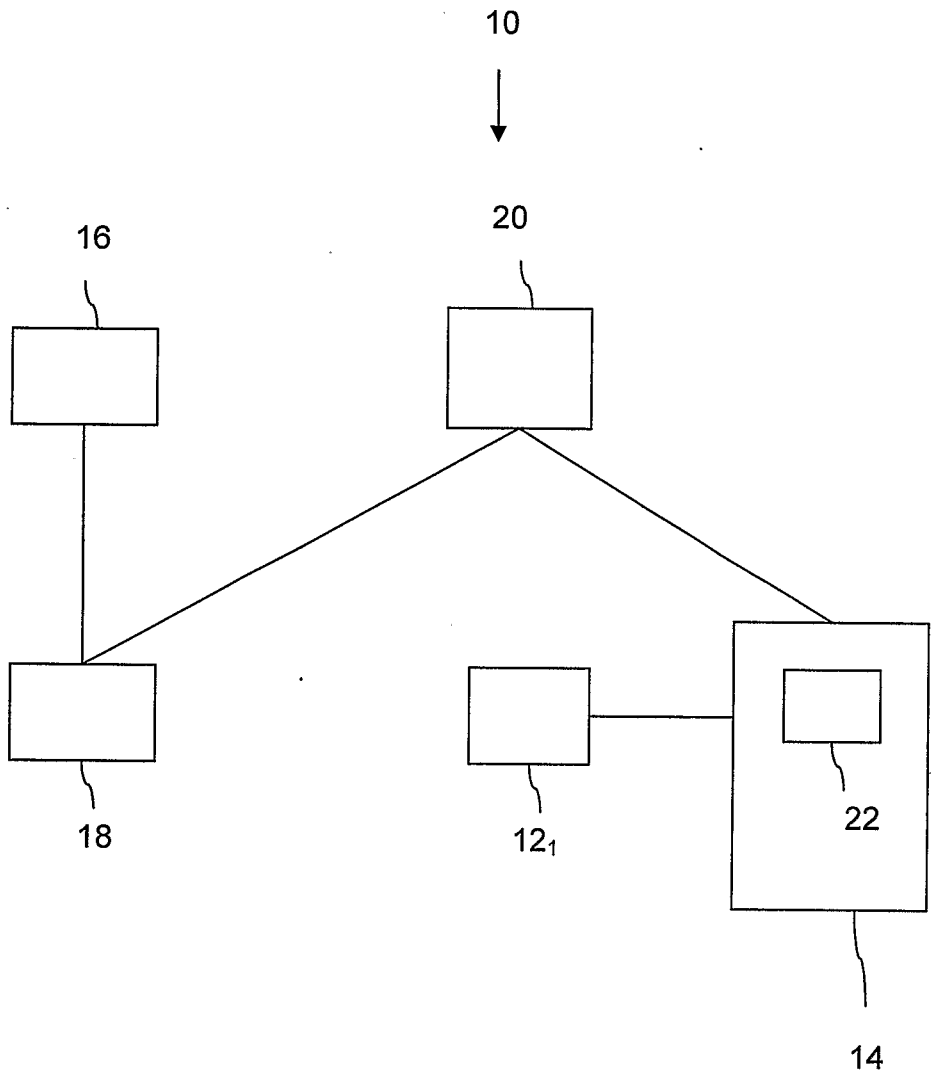


Fig. 1

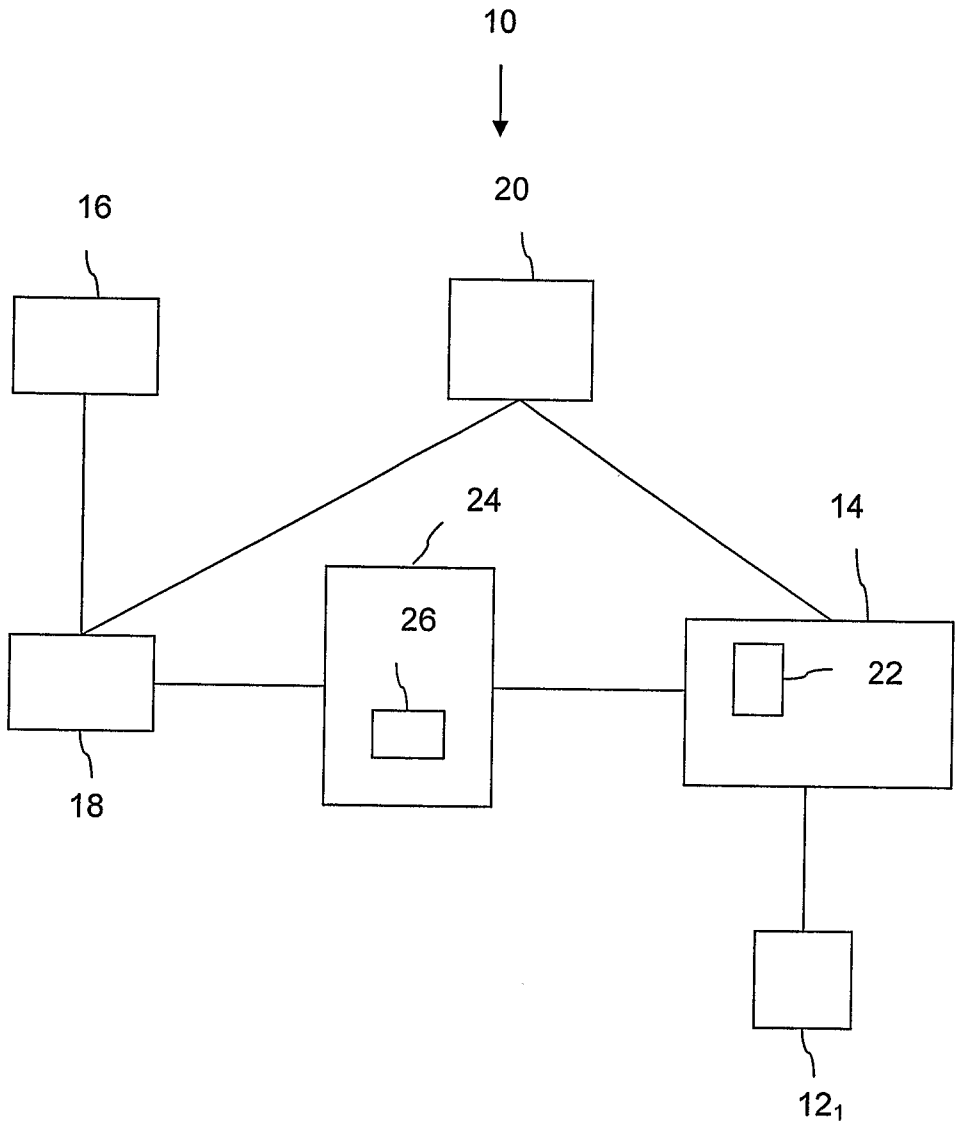


Fig. 2

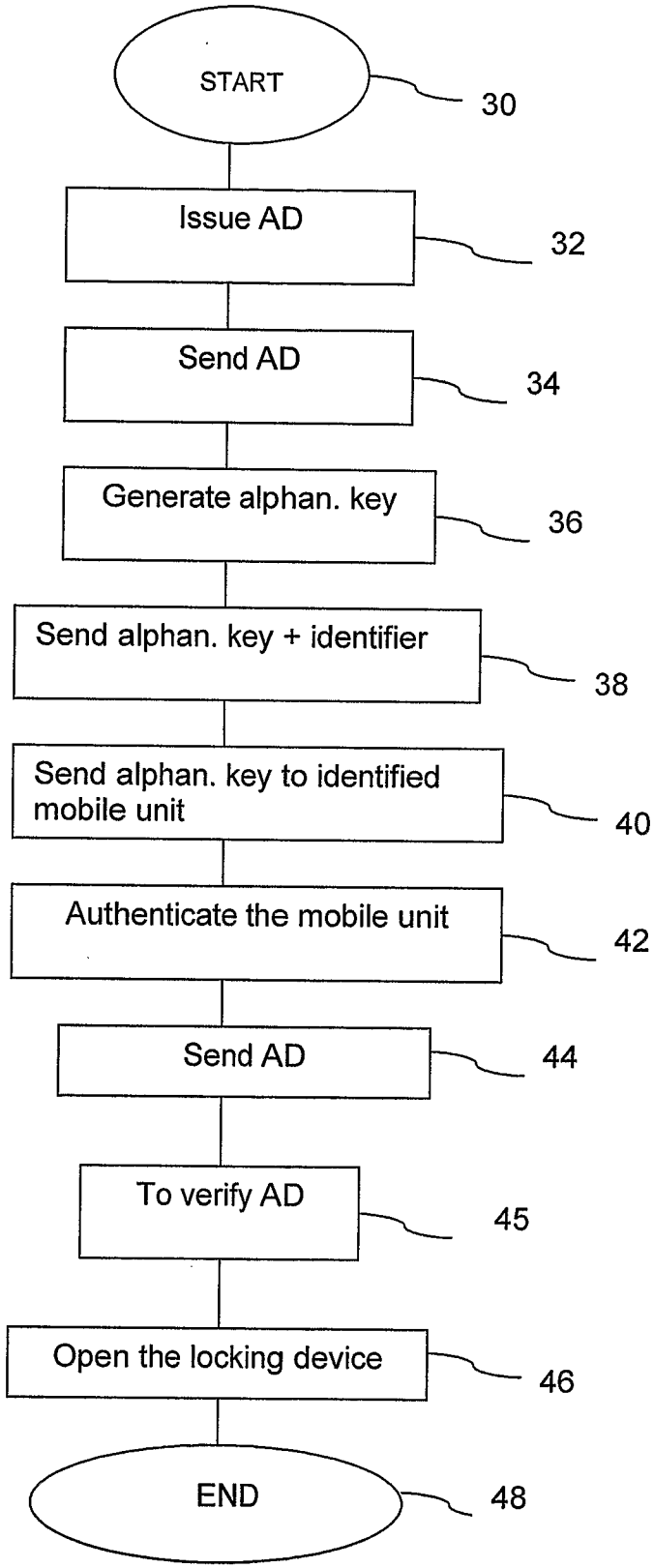

START
30
Issue AD
32
Send AD
34
Generate alphan. key
36
Send alphan. key + identifier
38
Send alphan. key to identified mobile unit
40
Authenticate the mobile unit
42
Send AD
44
To verify AD
45
Open the locking device
46
END
48

Fig. 3

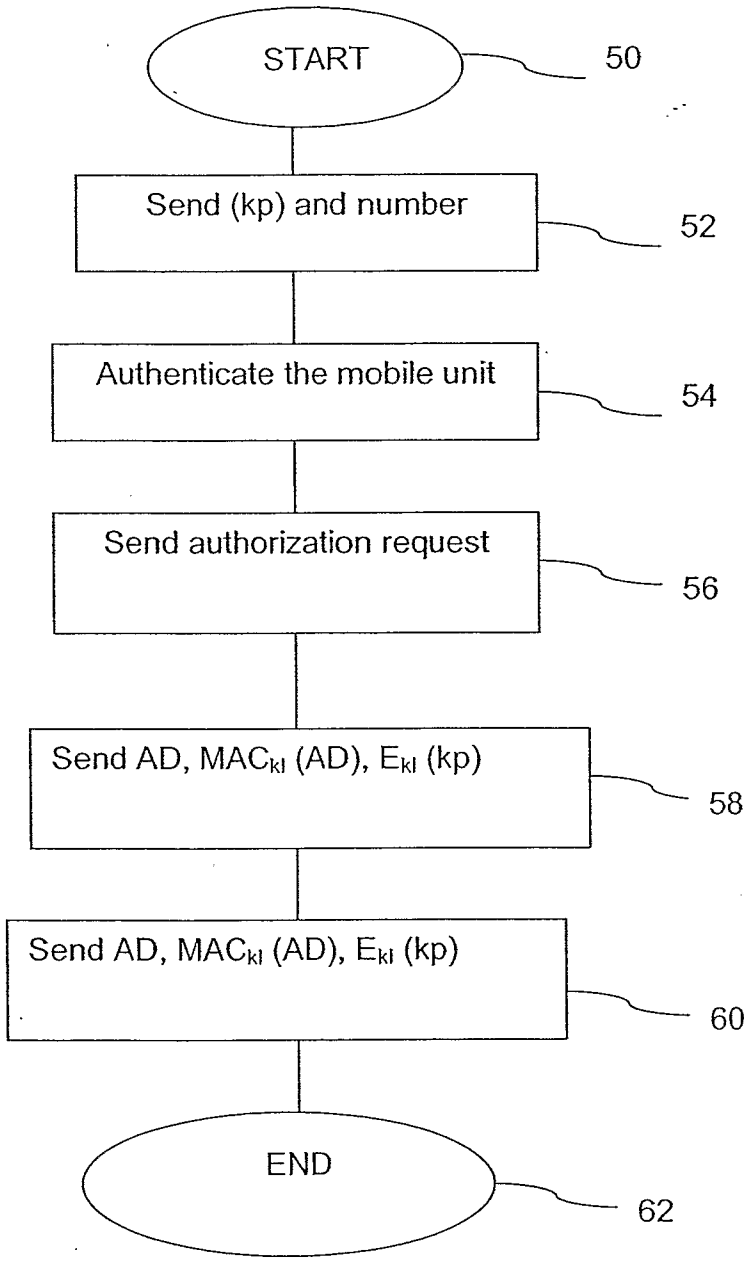

START
50
Send (kp) and number
52
Authenticate the mobile unit
54
Send authorization request
56
Send AD, MACkl (AD), Ekl (kp)
58
Send AD, MACkl (AD), Ekl (kp)
60
END
62

Fig. 4

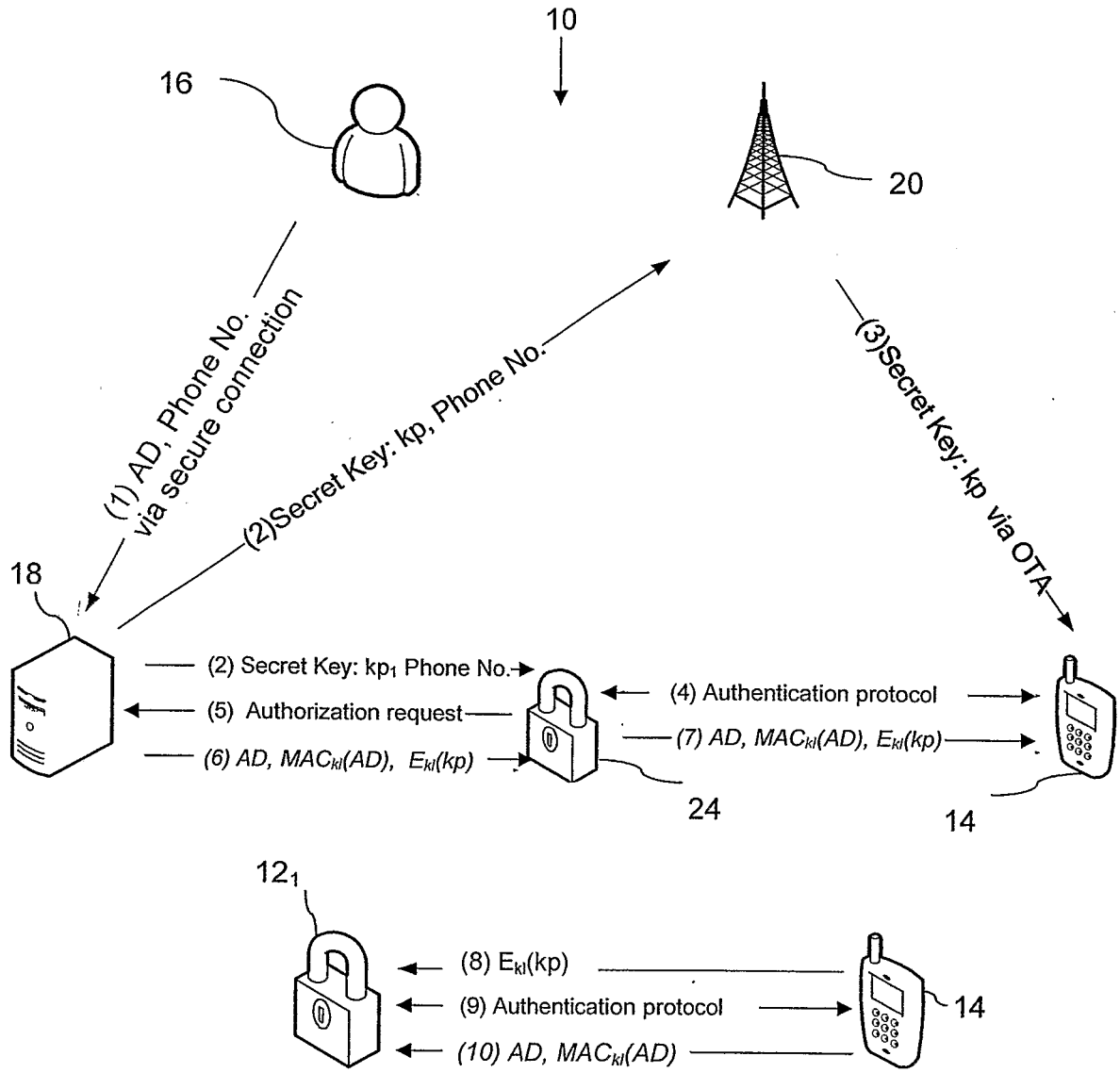

10
16
20
(1) AD, Phone No. via secure connection
(2)Secret Key: kp, Phone No.
(3)Secret Key: kp via OTA
18
(2) Secret Key: kp1 Phone No.
(5) Authorization request
(6) AD, MACkl(AD), Ekl(kp)
(4) Authentication protocol
(7) AD, MACkl(AD), Ekl(kp)
24
14
12 1
(8) Ekl(kp)
(9) Authentication protocol
(10) AD, MACkl(AD)
14

Fig. 5

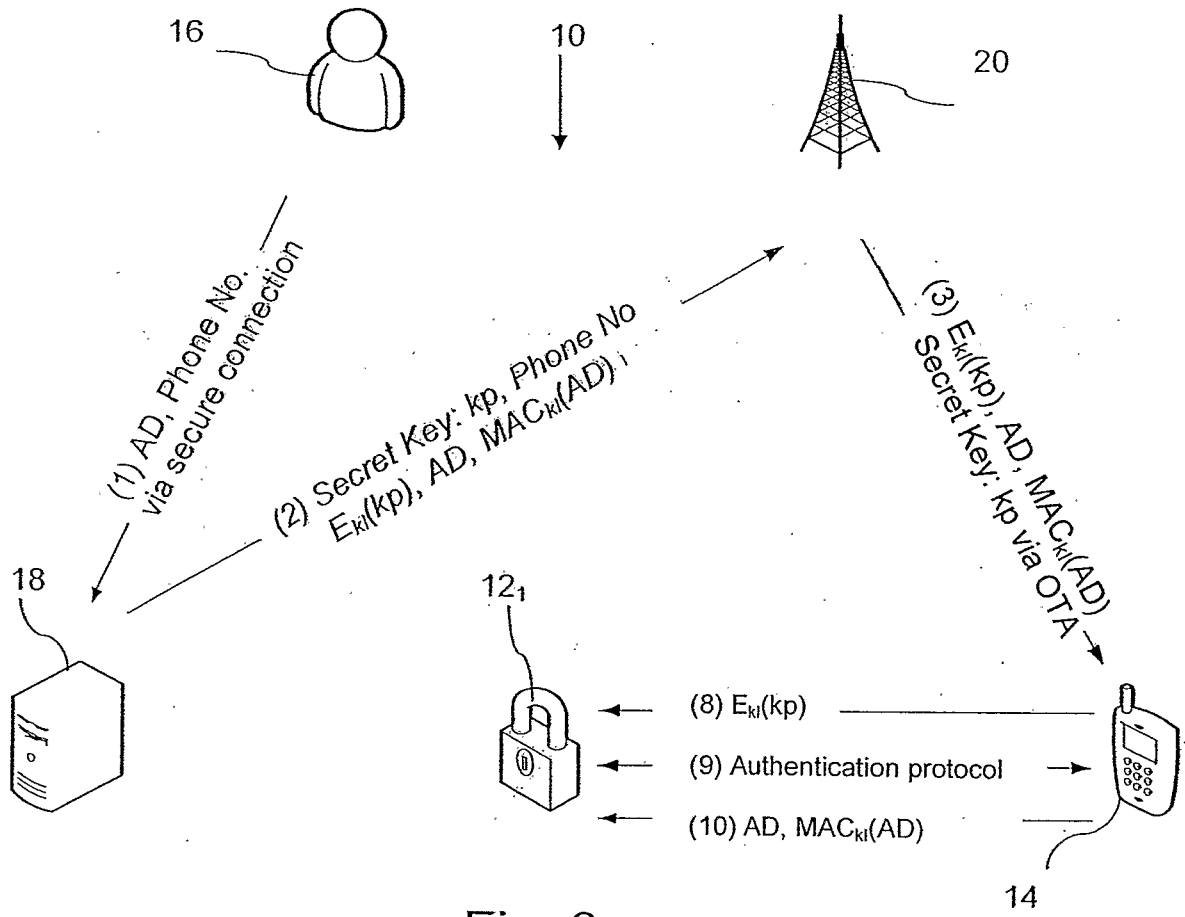

16
10
20
(1) AD, Phone No. via secure connection
(2) Secret Key: kp, Phone No $E_{kl}(kp)$, AD, $MAC_{kl}(AD)$
(3) $E_{kl}(kp)$, AD, $MAC_{kl}(AD)$ Secret Key: kp via OTA
18
12_1
(8) $E_{kl}(kp)$
(9) Authentication protocol
(10) AD, $MAC_{kl}(AD)$
14

Fig. 6

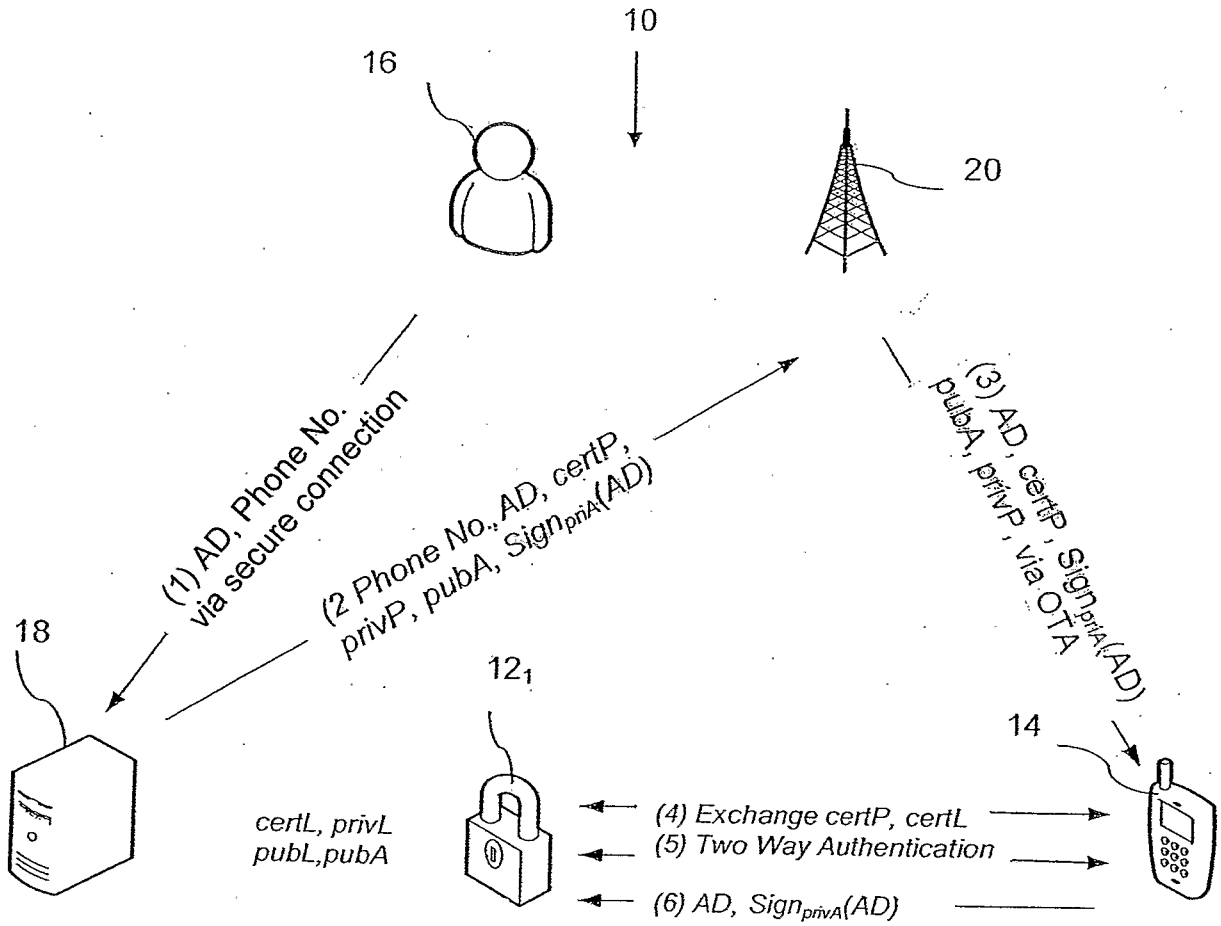

10
16
20
(1) AD, Phone No. via secure connection
(2 Phone No., AD, certP, privP, pubA, Sign$_{privA}$(AD)
(3) AD, certP, Sign$_{privA}$(AD) pubA, privP, via OTA
18
12$_1$
14
certL, privL publL,pubA
(4) Exchange certP, certL
(5) Two Way Authentication
(6) AD, Sign$_{privA}$(AD)

Fig. 7

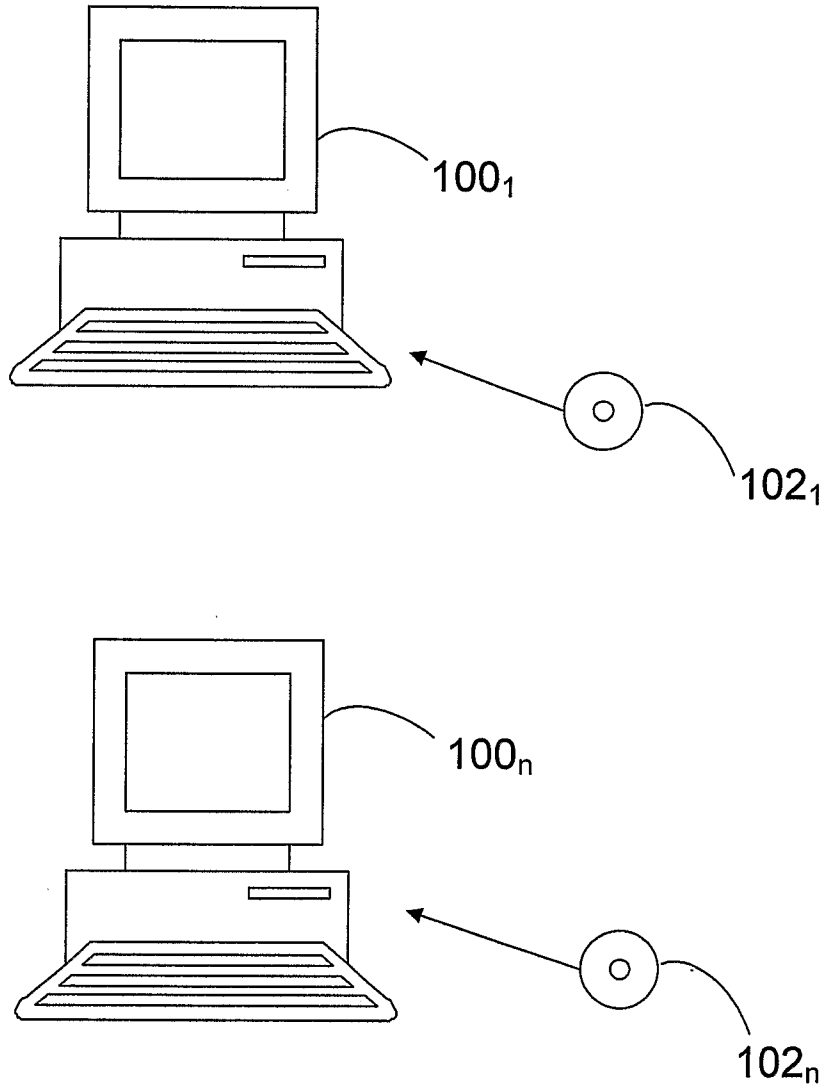


Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2007/050266

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
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)

IPC: G07C

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2364202 A (NOKIA MOBILE PHONES LTD.), 16 January 2002 (16.01.2002), page 5, line 21 - page 9, line 20, figures 3-5	1-35
A	US 20020178385 A1 (P.W.DENT ET AL), 28 November 2002 (28.11.2002), [0004], [0012]-[0015],fig 1	1-35
A	Beaufour A. "Personal Servers as Digital Keys" in: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications, March 14-17 2004, pp 319-328	1-35

☐ Further documents are listed in the continuation of Box C. ☒ 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
8 August 2007	10 -08- 2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Göran Magnusson /itw Telephone No. +46 8 782 25 00

International patent classification (IPC)
G07C 9/00 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **XYFKDUEIVC**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

GB	2364202	A	16/01/2002	GB	0015716 D	00/00/0000
				US	20020031228 A	14/03/2002
US	20020178385	A1	28/11/2002	AU	2002308549 A	03/12/2002
				EP	1423826 A	02/06/2004
				US	7114178 B	26/09/2006
				WO	02095689 A	28/11/2002