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

(11) Publication number: **0 122 244**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **84850102.9**

(22) Date of filing: **30.03.84**

(51) Int. Cl.^{3}: **E 05 B 49/00**

(30) Priority: **08.04.83 SE 8301957**

(43) Date of publication of application: **17.10.84**
Bulletin 84/42

(84) Designated Contracting States: **AT BE CH DE FR GB IT LI NL SE**

(71) Applicant: **WSO CPU-SYSTEM AB, Björnnäsvägen 10,**
S-173 47 Stockholm (SE)

(72) Inventor: **Olenfalk, Bengt, Lilla Hundens Gränd 12,**
S-175 60 Järfälla (SE)
Inventor: **Witt, Göran, Riddargatan 45,**
S-114 57 Stockholm (SE)
Inventor: **Sarberg, Anders, Robertsviksvägen 14,**
S-182 35 Danderyd (SE)

(74) Representative: **Carminger, Lars et al, CARMINGER &**
UUSITALO PATENTBYRA AB Box 3554,
S-103 69 Stockholm (SE)

(54) A lock system.

(57) The invention relates to a lock system for rooms which are to be made exclusively accessible to different uses over different periods of time, for example hotel rooms. The keys of the system comprise magnetic cards which are provided with magnetically registered data, which for each card includes lock-identification data valid for a given lock or a given group of locks, a validity time expressed in real time and a randomly selected legitimacy code. Each lock includes an electrically actuable lock mechanism (4), a magnetic-card reader (3), a memory (6) for the storage of data, a real-time clock (7), a programming unit (10), a legitimacy comparator (8), and a time comparator (9). The memory (6) has stored therein the lock-identification data valid for the lock. When a magnetic card is introduced for the first time into the card reader (3) of a lock, the legitimacy comparator (8) compares the lock-identification data registered on the card with the lock-identification data stored in the memory (6), and the time comparator (9) compares the validity time registered on the card with the real time given by the real-time clock (7). If these comparisons show agreement, the lock opens and the programming unit (10) is instructed to store into the memory the validity time and the legitimacy code registered on the card. When a magnetic card is later introduced to the card reader (3) the time comparator compares the real time given by the real-time clock (7) with the validity time in the card data stored in the memory and the legitimacy comparator (8) compares the data registered on the card with the data stored in the memory (6) of the lock, and the lock is opened when agreement is found between the data compared. If the comparison made by the time comparator (9) show disagreement, the time comparator compares the validity time registered on the card with the real time given by the real-time clock (7) and the legitimacy comparator (8) compares the lock-identification data registered on the card with the lock-identification data stored in the memory and, if these comparisons show agreement, the lock is opened and the programming unit (10) is used to replace the card data already stored in the memory (6) with the data registered on the card.

ACTORUM AG

A lock system

The present invention relates to a lock system, and in particular to a lock system intended for locking rooms to which a limited number of persons are permitted access over spaced periods of time. Such rooms may include hotel rooms, safes and drink cabinets placed in hotel rooms for use by guests, and also a diversity of storage facilities placed at the disposal of selected persons for a limited period of time, such as dress-changing rooms, banks and post offices.

Conventional locks and keys are not totally satisfactory security devices for such rooms, since the keys can be readily copied or stolen. Moreover, the holder of a key is often prone to either misplace it, or to forget to return it when his allotted period has expired. In order to safeguard against unauthorized entry into a room of which the key is missing, it is necessary, each time, to replace the lock. Such measures are too costly and time consuming to be practical in reality. Neither are mechanical nor electrical combination locks fully satisfactory for the aforesaid purposes, since such locks require the combination to be changed when the room served by the lock changes hands, this task being time consuming and requiring the employment of personnel. The person to whom the room has been allocated or let is also liable to forget the correct combination.

Consequently, in respect of rooms of the aforesaid kind there is an express need for a lock system which is practical in use, while affording the security desired.

In this regard there have been proposed in recent times lock systems which, instead of conventional keys, incorporate the use of magnetic cards, on which a digital code can be magnetically registered, and locks which include an electrically operable locking mechanism, a magnetic-card reading means, a memory in which a digital code can be stored, and means for making a comparison between the digital code read by the card reader from the magnetic card, serving as the "key", and the code stored in the memory, whereupon the locking mechanism is unlocked, provided that there is agreement between the two codes compared. Since in lock mechanisms of this kind it is a relatively simple matter to change the code registered on the card, and also a relatively simple matter to change the content of the lock memory, such a lock system affords,in principle, an essential advantage sought for in lock systems for use in the aforesaid respect, namely that it is relatively easy to render a key unusable for opening the lock and to replace the key with one which is functional in this respect.

Previously suggested and known lock systems of this kind are encumbered with many disadvantages, however, both with respect to their practical use and to their reliability against unauthorized opening of the lock. This is particularly true of such known lock systems as those used in connection with locales, such as hotels and the like in particularly, in which it must be possible for each lock, e.g. a hotel-room door lock, to be opened by more than one authorized person, for example, a hotel guest, cleaning personnel and like personnel, and hotel security personnel, and in which it is impossible to say definitely, with full assuredness beforehand, for how long a certain "key" shall be valid, i.e. at which point in time the key shall be made obsolete for the lock in question, this point in time normally varying in respect of the different people authorized to use the key.

Consequently, the object of the present invention is to provide an improved lock system of the aforementioned kind which includes at least one lock containing a lock mechanism provided with electrically actuable means for operating the lock mechanism between a locked and unlocked state, a magnetic-card reader for receiving a card on which data has been registered magnetically; a memory for storing data; and means for making a comparison between data stored in the memory and data read by said magnetic-card reader from a card inserted into the lock system, and for actuating the operating means of said lock mechanism in response to said comparison; and at least one magnetic card which serves as a key for unlocking said lock and which has data magnetically recorded thereon, said improved lock system having an improved utility and affording greater security than previously known lock systems of a similar kind.

This object is achieved with the lock system according to the present invention, which is characterized by the features set forth in the following claims.

The most significant features of the lock system according to the present invention reside in:

that the data registered on the magnetic card contains information concerning the time within which the card is valid (validity time) expressed in real time;

that the lock incorporates a real-time clock;

that the memory is designed to receive data relating to the card validity time; and

that the lock includes comparison means for making a comparison between firstly the validity time registered on the card,which validity time can be read-off by the magnetic-card reader when the card is introduced thereto, secondly the present time given by the real-time clock of the lock, and thirdly the card validity time stored in the lock memory.

A lock system designed in accordance with the invention affords several important advantages. For example, with the lock system according to the invention it is possible to establish accurately the validity time of the card in real time; this does not simply imply an initial date and a final date with respect to said validity time, but also those days and those times of day on which the card can be used within the interim period. Thus, it is possible to issue a card which can be used effectively only on certain weekdays and/or during certain times of the day, while being able, at the same time, to establish a total card validity time, i.e. a first and a last day of validity. It is also possible to issue a card long beforehand, i.e. long before the first day of the validity period. Thus, when the card has expired it is invalid and unusable once and for all. Further, in a system which includes a large number of locks, such as in a hotel for example, no connection whatsoever is required between the various locks themselves or between the locks and a central unit. Moreover, in a multi-lock system which incorporates the present invention, it is a relatively simple matter to replace a lock or to provide additional locks. It is also possible to issue several cards all apertaining to one and the same lock, and to issue a card which will open a number of specifically designated locks in the system, thereby providing access to a number of rooms.

The lock system according to the invention affords many other advantages, as will become apparent when reading the following description, which is made with reference to a preferred embodiment of a lock system according to the invention, illustrated in the accompanying drawing, in which

Figure 1 illustrates schematically a magnetic card serving as a "key"; and

Figure 2 is a block schematic view of a lock incorporated in said lock system.

Since the various members and components incorporated in the lock are such which are either generally commercially available or which can be readily constructed by one skilled in the art with the aid of the functional data given in the following description with regard to said components and members, the lock in Figure 2 has simply been illustrated in its block schematic form.

In the following, the lock system according to the invention is described, by way of example, with respect to its use in a hotel, although it will be understood that a lock system according to the invention can also be used to the same advantage for many other types of institution, and that the magnetic cards serving as keys can be of another kind with respect to the different usages for which they are legitimized.

Figure 1 illustrates schematically and by way of example a conventional magnetic card 1, which can be used as a "key" in a lock system according to the invention and which is provided with, for example, a strip 2 of magnetisable material on which data, preferably in digital form, can be magnetically registered. The magnetic registration, or the writing of data into the card is effected by means of a separate, conventional programming or write-in apparatus (not shown in detail) which is suitably placed in the reception facilities of the hotel.

The card programming or write-in appratus includes a real-time clock and a microprocessor, e.g. AIM 65 from Rockwell, which is programmed to determine the date registered on an inserted card 1.

In a lock-system according to the invention intended for hotel use, the aforementioned programming or write-in apparatus can be arranged to issue or to program different types of card. For example, there may be found three main types of card, namely:

- guest cards, which are intended for issue to hotel guests, and to afford each guest access to only one given room during all times of the day for a specific, selectable period of time, validity time;

- service cards, which are intended for cleaning personnel and other personnel, and which afford access to a given floor, during a certain time of day, for example between 8.00 and 17.00, and/or on certain days of the week, for example all weekdays, and for a given validity time, i.e. from a first validity day to a final validity day;

- master cards, intended for the hotel security staff or management, which afford access to all rooms in the hotel or in a certain part of the hotel at all times of the day for a given validity time, i.e. from a first validity day to a final validity day.

In the described embodiment of the invention the data registered magnetically on the card, preferably in digital form, by means of the programming or write-in apparatus, may comprise the following information:

- type of card, i.e. whether a guest card, a service card or a master card;

- system identification, i.e. a code which is unique to the lock system in question, e.g. the hotel, and which may comprise a plurality of check digits or check totals in the digital data registered on the card;
- lock identification, i.e. information disclosing which lock or locks, i.e. hotel room(s), the card is legitimized to open;
- validity time, including information concerning both the total validity time, i.e. the first and the final day of validity, and the days of the week and times of day to which the functionability of the card is restricted;
- individual legitimacy code, which may comprise a multi-digit number selected at random, said number containing so many digits as to render the risk of several cards containing the same individual legitimacy code highly improbable. In a lock system intended for hotels for example, not all cards need be provided with such randomly selected individual code. For example, only the guest cards and master cards need be provided with such a code, while in service cards the code may be omitted.

The programming or write-in apparatus is designed so that when issuing or programming a card, the operator is able to determine the type of card concerned, the system identification, the lock identification, and the validity time, but not the legitimacy code randomly selected by the apparatus itself. Naturally, the apparatus is designed so that it can only be operated by selected, authorized personnel, which may have varying grades of authorization, such that, for example, the system identification can only be determined and changed by a few people, which may also apply to the issue of a master card, for example.

The lock illustrated in the block schematic of Fig. 2 includes a conventional magnetic card reader 3, for example a reader of the Magdat-type MSC-170-IR, or the Ericsson-type KDT 30201, into which a magnetic card 1 according to Figure 1 can be inserted, and which reads the data magnetically registered on the card. The lock also includes a conventional locking mechanism 4 which can be operated electrically between a locked and an unlocked state. Also incorporated in the lock is a memory 6, for example a direct access store of the type designated Fujitse MB8414E, and a real-time clock 7, for example of the kind designated MM 58174 from National Semiconductor. In addition hereto, the lock includes a legitimacy comparator 8, a time comparator 9 and a programming unit 10, the functional purpose of which will be made apparent hereinafter. The lock may also incorporate a position sensor 5, for example in the form of a microswitch, which detects the position of a lock bolt in the lock mechanism 4.

The memory 6, which is suitably of the direct access type, is suitably arranged to store digital data. This data can be changed with the aid of the programming unit 10. The aforementioned system identification and the lock identification pertaining to said lock are always stored in the memory. The aforesaid items of data are entered into the memory 6 before the lock is installed by, temporarily connecting the lock to the aforementioned programming or write-in apparatus from which the system identification and lock identfication is obtained, and entering said data into the memory 6 through the programming unit 10.

The legitimacy comparator 8 is arranged to receive from the card reader 3, the data or information registered on the magnetic card fed to the card reader 3, and to compare this data with data stored in the memory 6.

The time comparator 9 is designed to be able to make a mutual comparison between the real time given by the real-time clock of said lock, the time-information read from an inserted card by the card reader 3, and time-information stored in the memory 6.

The functional mode of the lock will be described hereinafter, first wich reference to a guest card of the kind aforedescribed, i.e. a card bearing registered data concerning the type of card, system identification, validity time, and a randomly selected legitimacy code.

When a guest card of this kind is first inserted into the card reader 3, so that data registered on the card is transferred to the legitimacy comparator 8, the reader first determines that the card inserted is a guest card. A microprocessor (not shown in detail) incorporated in the lock and being, for example, of the aforementioned kind designated AlM65 from Rockwell instructs the time comparator 9 to compare the validity time read from the card with the real time given by the real-time clock 7, and further instructs the legitimacy comparator 8 to compare the system identification and the lock identification in the data read from the card with the system-identification data and the lock-identification data previously stored in the lock memory 6. If these comparisons show that the real time given by the clock 7 lies within the validity time registered on the card, and that the system and lock identification data stored in the memory 6 agree with the system and lock identification data registered on the card, the programming unit 10 is ordered to store all the data registered on the card in a site in memory 6 intended herefor, and actuates the lock mechanism, to open the lock. If, on the other hand, one of the comparisons shows a negative result, the lock remains locked and no further action takes place. Thus, the lock cannot be opened with a guest card unless the card is intended for the location and the lock in question, and unless it is presented to the lock within the validity time registered on the card.

When the same guest card is again introduced to the card reader 3, the time comparator 9 is instructed to compare the time given by the real-time clock 7 with the validity time stored as described above in the site in the memory 6 reserved for guest-card date. If the result of this comparison is positive, i.e. the validity time stored in the memory has not yet expired, the legitimacy comparator 8 is instructed to compare the whole of the data read from the card with the data stored in the aforesaid manner in the memory 6, in the site reserved for the guest-card data. If the comparison shows agreement between the two sets of data, the legitimacy comparator 8 actuates the lock mechanism 4, to open the lock. It will be evident from this that is is not possible to open the lock with the aid of any other guest card, even though said card should have a still current validity time and contain both the relevant system identification data and the lock identification data relevant to the lock in question. This other guest card will namely have a different randomly selected legitimacy code to that stored in the memory 6 of said lock in the site for guest-card data.

If the validity time stored in the memory 6 in the site for guest-card data has expired, when a guest-card is inserted into the card reader 3, this will be discovered at the comparison made by the time comparator 9, as described above, between said validity time and the time given by the real-time clock 7. When this comparison gives a negative result, the programming unit 10 is instructed to erase the validity time stored in the memory 6, wherefore the subsequent comparison made by the legitimacy comparator 8, as described above, between the data registered on the guest card and the guest-card data stored in the memory 6 will also give a negative result, whereby the lock is not opened. Consequently, the card can not be used to open the lock, when the validity time registered on the card has expired.

If the validity time for the previously valid quest card has expired, and a newly issued guest card is inserted into the card reader 3, the comparisons described in the foregoing paragraph will of course also in this case give negative results. The time comparator 9 is then instructed to compare the time given by the real-time clock 7 with the validity time registered on the new guest card, and the legitimacy comparator 8 is instructed to check the system identification data and lock identification data registered on the new guest card in the aforedescribed manner. If all of these checks give positive results, the programming unit 10 is instructed to store the data registered in the new guest card in the site reserved for guest-card data in the memory 6, and to open the lock mechanism 4. Thus, the person possessing the new guest card is able to open the lock, provided that the validity time of the previously valid card has expired, and at the same time the data on the new guest card is stored in the memory 6 so that the new guest card can be used for future opening of the lock.

As will be understood, in the case of a hotel a guest may decide to vacate his/her room earlier than was initially intended, i.e. before the validity time of the card issued to the guest has expired. Similar circumstances may occur with other types of institutions or established organizations. In such cases, in order to enable a new guest to enter the room, it is necessary to issue a card which will be accepted by the lock, despite the fact that the memory 6 of the lock has stored therein data relating to a guest card whose validity time has not yet expired. This is readily achieved in the lock system according to the invention by simply issuing the new guest in such cases with a guest card containing data which includes a separate so-called override-code, which is detected by the legitimacy comparator 8 of the lock, whereupon the lock is opened and the data contained in the new guest card replaces the data pertaining to the earlier card in the lock memory 6, always provided, of course, that the aforedescribed checks relating to the system and the lock identification data and to the validity time of the new guest card give positive results. Those guest cards provided with an override code are given consecutive numbering by the programming or write-in apparatus, so that only the card last issued with an override function is valid for use.

The lock-functions in respect of a master card of the aforedescribed kind in the same manner as that described above with reference to a guest card, with the exception that the lock identification data registered in the master card is constructed so that the master card will be accepted by a plurality of locks, for example by all the locks in a hotel or by all the locks within a given part thereof. When wishing to issue a new master card which is to replace an exisiting master card whose validity time has not expired, the procedure adopted differs from that taken with the aforescribed guest card, insomuch as the new master card is not given a special override code. Instead, it is ensured, in accordance with a preferred embodiment of the invention, that when programming the new master card, it obtains a validity time which extends beyond the validity time of the earlier master card. Thus, the lock is so designed that the legitimacy comparator 8 accepts such a new master card, provided with a longer validity time than the validity time previously registered in the memory 6 of said master card, and in conjunction therewith substitutes the master card data previously stored in said memory with the data found registered on the new master card.

The data registered on a service card contains no randomly selected legitimacy code, but only data referring to system identification, lock identification, i.e. identifications of those locks or rooms to which the service card has access, and a validity time. Thus, in the case of a service card the lock functions in the above-described manner, with the exception that none of the data registered in the service card is stored in the memory 6 of the lock. Thus, in respect of a service card, the legitimacy comparator 8 solely checks the system-identification data and the lock-identification data on the card with the system and lock identification data stored in the memory 6, while the time-comparator 9 checks the card validity-time with the real time given by the real-time clock 7.

For security reasons it may be necessary to be able to change the system identification common to all locks in a system, for example a hotel. As previously mentioned, the system-identification data has originally been stored in the lock memory 6, by temporarily connecting the lock, prior to its installation, to the programming or write-in apparatus. In order to obviate the necessity of carrying out a similar procedure when changing the system-identification for the system, a lock system according to a preferred embodiment of the invention is designed to enable the system identification to be changed, by issuing a new master card which contains both the old and the new system identitication, and also a special operation code. When this new master card is inserted into a lock, the lock detects said operation code and the programming unit 10 in the lock is ordered to replace the old system-identification data stored in the lock memory 6 with the new system-identification data registered on the new master card.

In a preferred embodiment of the invention the position sensor 5 of the lock illustrated in Figure 2 may be arranged to sense a special position for a lock bolt in the lock mechanism 4, to which the lock bolt may be moved manually by the hotel guest from inside the door. Upon manual actuation of the lock bolt in this way, the position sensor 5 acts upon the legitimacy comparator 8 in a manner such that said comparator no longer accepts, for example, a service card, but only master cards and guest cards. This function can be employed when a guest does wish to be disturbed. If the hotel room is furnished with a safe, in which a guest's valuables can be kept, the safe lock can be designed so that the position sensor 5 is constantly activated, whereupon the safe can only be opened with a guest card and a master card. In this respect, the position sensor 5 may also be arranged to act upon the legitimacy comparator 8 in a manner such that the comparator will not accept a guest card provided with an override code of the aforementioned kind.

So that the locks will not be effected by a power failure, the locks of a lock system according to the invention are suitably supplied with power from individual batteries. When a lock is taken out of operation or removed from the system, e.g. for repair, change of batteries, or to change a whole lock, the repaired or new lock can be readily made operable , by connecting it temporarily to the programming or write-in apparatus,such as to insert the requisite system and lock identification data into the memory of said lock. At the same time, the clock 7 of the lock is synchronised with the real-time clock in the programming apparatus.

As will be understood it is possible to incorporate many further functions in a lock system according to the invention, and that such a system can be designed in various ways for different purposes of use.

Although not expressly mentioned in the aforegoing, it will be understood that the magnetic card 1 can be reprogrammed and used a repeated number of times, simply by presenting the card to the aforedescribed programming and write-in apparatus each time the card is to be renewed. In this respect, the programming and write-in apparatus is advantageously designed to record therein the number of times an individual card has been renewed and fresh data registered therein. In this way, it is possible to estimate when a card has been used so many times that there is danger of it being worn to such an extent as to render the card unserviceable and unreliable.

CLAIMS

1. A lock system including at least one lock and at least one key for unlocking the lock, in which

the key comprises a card (1) provided with magnetically registered data (2), and

the lock includes a locking mechanism (4) having electrically actuable means for unlocking the same, a magnetic-card reader (3) arranged to receive a card (1) of the aforementioned kind and to read the data registered thereon, a memory (6) for storing data, and a comparison means (8, 9) for comparing the data stored in said memory (6) with data read from said card by means of said magnetic-card reader (3) and for acting upon the locking mechanism (4) in response to said comparison,

characterized in that

the data (2) registered on the card (1) includes a lock identification allotted to the lock, a validity time expressed in real time, and a randomly selected legitimacy code allotted individually to the card;

the lock includes a real-time clock (7) and a programming unit (10) for entering data into said memory (6) and for changing the data content of said memory;

the comparison means of the lock includes a legitimacy comparator (8) and a time comparator (9);

the memory (6) of said lock includes said lock-identification data and is capable of storing card data of the aforementioned kind;

and in that upon insertion of a card of the aforementioned kind in the card reader (3),

a) the time comparator (9) is arranged to compare the real time given by the real-time clock (7) with the validity time in the card data stored in the memory (6) and the legitimacy comparator (8) is arranged to compare the data registered on said card with the card data stored in the memory (6), the locking mechanism (4) being caused to take its

unlocked state if all said comparisons are in agreement,
b) whereas, if the comparison made by the time comparator (9) between the real time given by the real-time clock (7) and the validity time in the card data store in the memory (6) indicates disagreement, or no card data is stored in the memory (6), the time comparator (9) is arranged to compare the validity time registered on said card with the real time given by the real-time clock (7), and the legitimacy comparator (8) is arranged to compare the lock-identification data registered on said card with the lock-identification data stored in the memory (6), and if these comparisons are in agreement, the lock mechanism (4) is caused to take its unlocked state and the programming unit (10) is caused to remove any card date already stored in the memory and to store the data registered on said card in the memory (6),

2. A lock system according to claim 1, characterized in that the data registered on the card may also include a separate override code, which the legitimacy comparator (8) in the lock is arranged to detect, when the card is introduced to the magnetic-card reader (3), in which case, if the aforementioned comparison made by the time comparator (9) between the real time given by the real-time clock (7) and the validity time stored in the memory (6) results in agreement, whereas the aforesaid comparison made by the legitimacy comparator (8) between the data registered on the card and the card data stored in the memory(6)indicates disagreement, the time comparator (9) is arranged to compare the validity time registered on said card with the real time given by the real-time clock (7), and the legitimacy comparator (8) is arranged to compare the lock-identification data registered on said card with the lock-identification data stored in the memory and, if these comparisons are in agreement, the lock mechanism (4) is caused to take its unlocked state and the programming unit (10) is caused to replace the card data previously stored in the memory (6) with the card data registered on said card.

3. A lock system according to claim 1 or claim 2 and including a plurality of locks, characterized in that mutually different locks have mutually different lock-

identification codes stored in their memories and also a system-identification code common for the whole of the system; in that all the magnetic cards intended for unlocking respective locks in the system also contain said system identification in the data registered on the card, the legitimacy comparators (8) in respective locks being arranged to compare the system-identification code registered on an inserted card with the system-identification code stored in the memory (6) of said lock in the same manner as the comparison between the lock identification code registered on an inserted card with the lock-identification code stored in the memory of said lock.

4. A lock system according to Claim 3, characterized in that it includes at least one further magnetic card, the stored data of which, in addition to said system identification, the validity time expressed in real time and a randomly selected legitimacy code, also contains a lock identification which is so formed as to coincide with lock identification data stored in the memories in a pre-determined number of the locks incorporated in the system, so that said card can be used for unlocking said pre-determined number of locks.

5. A lock system according to Claim 3, characterized in that it includes at least one further magnetic card, whose registered data includes said system identification, a lock identification valid for a given lock or a number of given locks in the system, and a validity time expressed in real time, but no randomly selected legitimacy code, but merely a code which identifies this type of additional card, wherewith the legitimacy comparator (8) incorporated in a lock is arranged, when said additional card is introduced to the card reader (3) of said lock, to detect said code identifying said card type, wherewith the legitimacy comparator is arranged to compare the system and lock identification data registered on the card with the system and lock identification data registered in the memory (6) of the lock, and the time comparator (9) of said lock is arranged to compare the validity time registered on the card with the real time given by the

real-time clock (7) and, when all the comparisons are in agreement with another, to cause the lock mechanism (4) to take an unlocking state.

Fig. 1

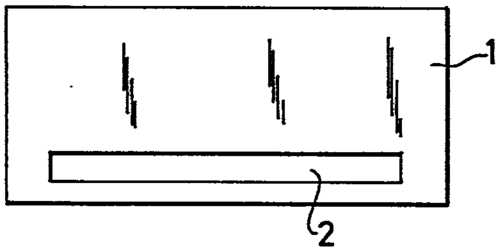
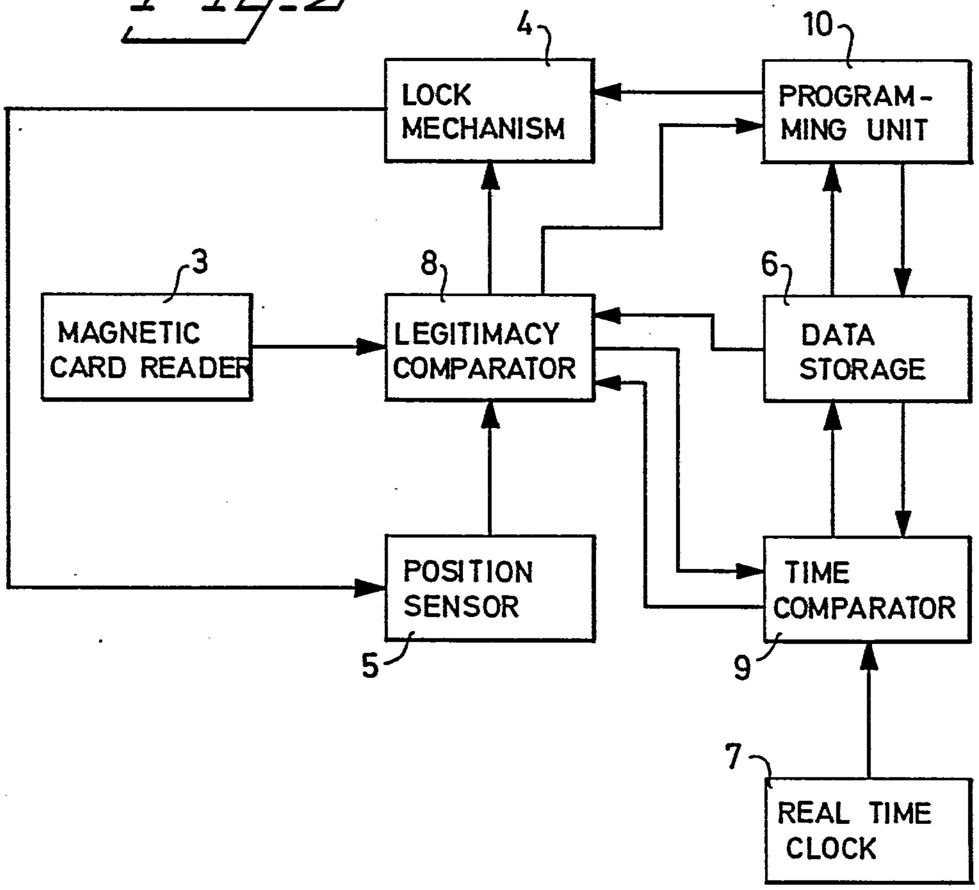

1
2

Fig. 2


4
LOCK MECHANISM
10
PROGRAM-MING UNIT
3
MAGNETIC CARD READER
8
LEGITIMACY COMPARATOR
6
DATA STORAGE
POSITION SENSOR
5
TIME COMPARATOR
9
7
REAL TIME CLOCK