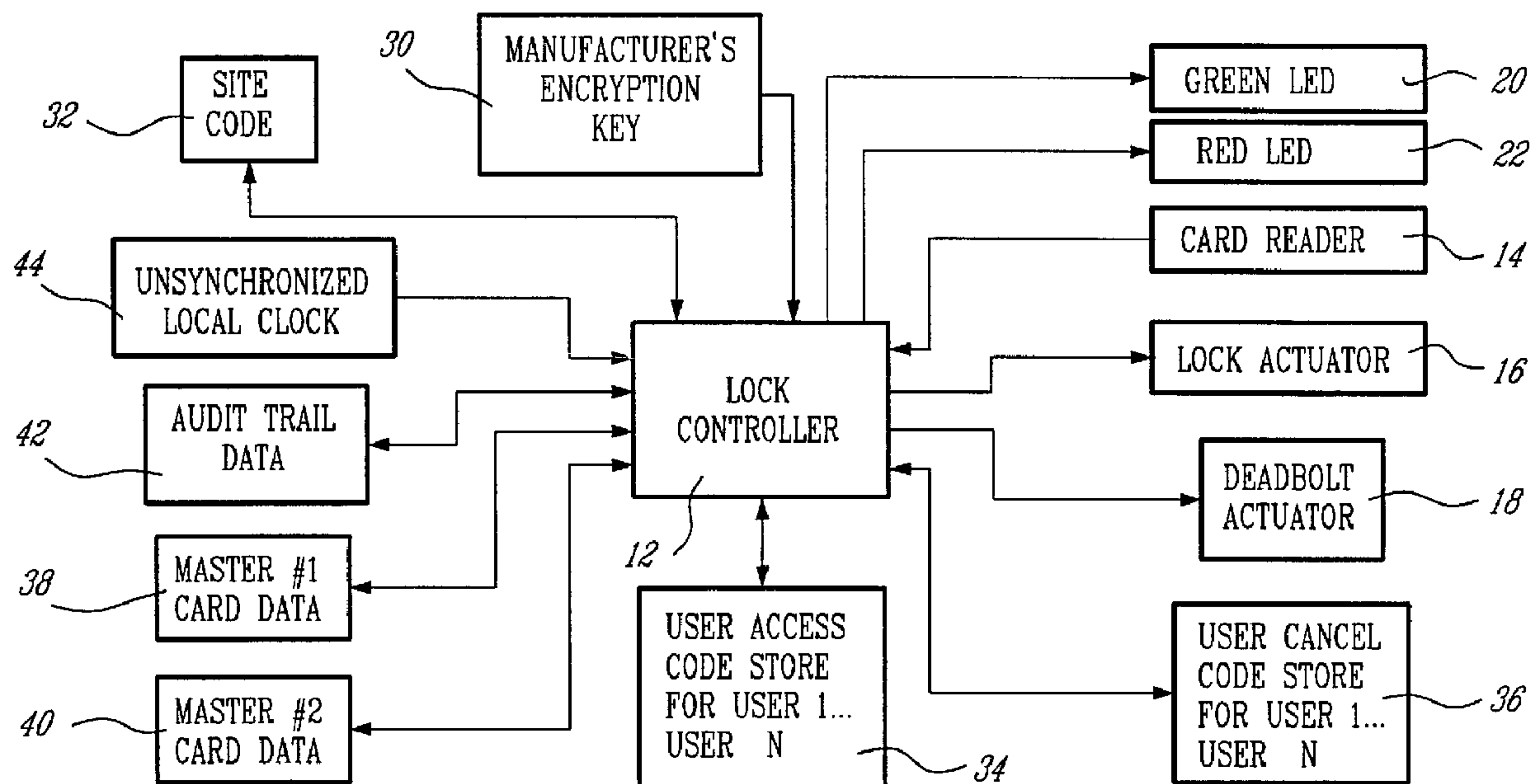




(86) Date de dépôt PCT/PCT Filing Date: 2000/12/01
(87) Date publication PCT/PCT Publication Date: 2001/06/14
(85) Entrée phase nationale/National Entry: 2002/06/05
(86) N° demande PCT/PCT Application No.: CA 2000/001416
(87) N° publication PCT/PCT Publication No.: 2001/042598
(30) Priorités/Priorities: 1999/12/07 (2,292,014) CA;
2000/06/30 (09/609,173) US

(51) Cl.Int.⁷/Int.Cl.⁷ E05B 49/00
(71) Demandeur/Applicant:
KABA ILCO INC., CA
(72) Inventeurs/Inventors:
MESSIER, YVES, CA;
DOYON, PIERRE, CA;
HUYHN, BAO CO PHAT, CA;
TOLEDANO, ANICK, CA;
LIVEANU, RODICA, CA;
BERNTSEN, STEVEN, CA
(74) Agent: OGILVY RENAULT

(54) Titre : SYSTEME DE COMMANDE PAR CLEF DE DONNEES POUR VERROU ELECTRONIQUE
(54) Title: KEY CONTROL SYSTEM FOR ELECTRONIC LOCKS



(57) **Abrégé/Abstract:**

An electronic door lock is programmable to accept new valid data key devices using a special data key device from with a set of special data key devices used for programming and control purposes. The lock has a learn mode controller responsive to a learn data key device to enter into a new valid access data key learn mode. A valid access code recorder is responsive to a first previously unknown code contained in a first new data key device while in the learn mode to record the first unknown code as a valid access code for operating said lock. A cancel code recorder is responsive to a second previously unknown code contained in a second new data key device while in the learn mode to record the second unknown code as a cancel code paired with the valid access code of the first new data key device. In use, the lock is activated to open in response to the valid access code of



(57) **Abrégé(suite)/Abstract(continued):**

the first new data key device, and is activated to cancel the recorded valid access code in response to the cancel code of said second data key device. The lock is able to operate with any data key device without requiring preprogramming specific to the lock. Programming and control is made easier by hierarchical distinctly labeled special data key devices used for specific corresponding programming and control purposes.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/42598 A1

(51) International Patent Classification⁷: **E05B 49/00**

(21) International Application Number: PCT/CA00/01416

(22) International Filing Date: 1 December 2000 (01.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,292,014 7 December 1999 (07.12.1999) CA
09/609,173 30 June 2000 (30.06.2000) US

(71) Applicant (for all designated States except US): **ILCO UNICAN INC.** [CA/CA]; 7301 Decarie, Montreal, Québec H4P 2G7 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MESSIER, Yves** [CA/CA]; 153 Anselme Lavigne, Dollard des Ormeaux, Québec H9A 1P4 (CA). **DOYON, Pierre** [CA/CA]; 3259 Chevremont, Ile Bizard, Québec H9C 2L8 (CA).

HUYHN BAO, Co, Phat [CA/CA]; 10180 Meilleur, Apt. #2, Montreal, Québec H3L 3H8 (CA). **TOLEDANO, Anick** [CA/CA]; 5999 Monkland, Apt. #2, Montreal, Québec H4A 1H9 (CA). **LIVEANU, Rodica** [CA/CA]; 39 Roxton Crescent, Montreal West, Québec H4X 1C7 (CA). **BERNTSEN, Steven** [CA/CA]; 2077 Belgrave Avenue, Montreal, Québec H2A 2L6 (CA).

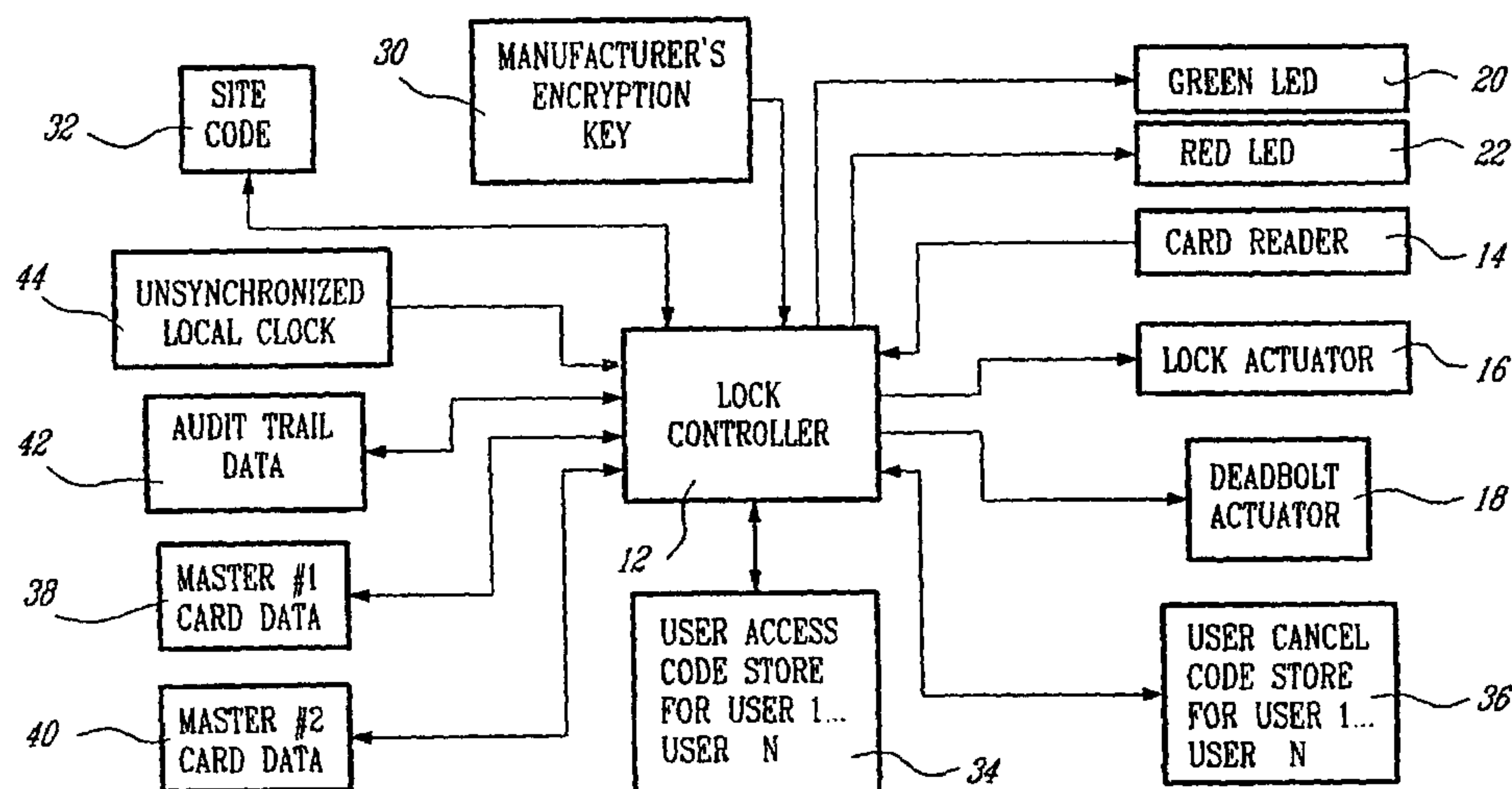
(74) Agents: **ANGLEHART, James et al.**; Swabey Ogilvy Renault, Suite 1600, 1981 McGill College Avenue, Montréal, Québec H3A 2Y3 (CA).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: KEY CONTROL SYSTEM FOR ELECTRONIC LOCKS



(57) Abstract: An electronic door lock is programmable to accept new valid data key devices using a special data key device from with a set of special data key devices used for programming and control purposes. The lock has a learn mode controller responsive to a learn data key device to enter into a new valid access data key learn mode. A valid access code recorder is responsive to a first previously unknown code contained in a first new data key device while in the learn mode to record the first unknown code as a valid access code for operating said lock. A cancel code recorder is responsive to a second previously unknown code contained in a second new data key device while in the learn mode to record the second unknown code as a cancel code paired with the valid access code of the first new data key device. In use, the lock is activated to open in response to the valid access code of the first new data key device, and is activated to cancel the recorded valid access code in response to the cancel code of said second data key device. The lock is able to operate with any data key device without requiring preprogramming specific to the lock. Programming and control is made easier by hierarchical distinctly labeled special data key devices used for specific corresponding programming and control purposes.

KEY CONTROL SYSTEM FOR ELECTRONIC LOCKS

Field of the Invention

The present invention relates to a key control system for electronic locks as well as to a method and apparatus for programming electronic door locks using a set of special programming keys. The invention also relates to a hierarchical key control method and system.

Background of the Invention

Electronic locks are commonly used for providing building security. In such systems, access to a building and secure areas within a building is achieved using a data key device, such as a magnetic stripe card, a proximity card, a Dallas™ key or tag, a smart card, an electronic physical key reader, or the like. Given the ease of use of such data key devices for opening doors, the use of such electronic door locks is convenient and presents little burden to authorized users. The door locks are known to include, among others, mortise door locks, latch release mechanisms mounted in the door frame for allowing a locked mortise door lock to be released from the door frame, magnetic door release locks, and in certain circumstances, more sophisticated turnstile access gates. Such electronic access locks are also used for controlling the use of elevators.

In the building access security industry, such electronic door locks fall into two general categories, i.e. either networked locks or stand-alone locks. In the networked configuration, there is a data network between each electronic door lock and a central control computer. In such a configuration, a code read from a data key device can be compared with authorized codes entered in a database at the central control computer to determine whether the door lock should allow access to the user. The central control computer can also control changes to access according to time of day, and in case of an emergency, such as a fire, the central control may allow all doors to be unlocked.

In the stand-alone type of electronic door lock, the electronic door lock is not connected to a central network and must be programmed by direct manipulation of the individual electronic door lock. This is conventionally done by using a data interface connection between the stand-alone electronic door lock and a portable computer for carrying out the programming functions. Where a door lock needs to be programmed with the codes from a large number of data key devices in a facility, the portable computer is typically connected to the electronic door lock in order to communicate to the electronic door lock the codes of all valid data key devices.

It is also known in the art to overcome the need to load codes for valid data key devices into an individual electronic door lock by using a set of codes in the data key devices which the stand-alone electronic door lock can recognize as being valid as a result of a characteristic inherent in the code information. A data key device from the set of acceptable user access data key devices can be barred access to the stand-alone electronic door lock by using a complementary cancel key having a code which the stand-alone electronic door lock automatically recognizes as being the complementary cancel code for the key device to be cancelled. In this known art, it is necessary to use a set of codes with the data key devices such that the stand-alone electronic door lock can recognize a valid access card and recognize a valid cancel card for a particular access card.

There is thus a need for an electronic door lock which does not require the burden of a portable computer and data interface for carrying out programming functions and which does not limit the lock to the use of a predetermined set of codes recorded in the data key devices. There is furthermore a need for such an electronic door lock in which the programming is simple, stepwise and flexible to the needs of small and medium facilities.

Summary of the Invention

It is accordingly a first object of the present invention to provide an electronic door lock in which a set of clearly identified special data key devices are used for programming and control purposes, in which a first

special data key device acts as a start-up key for initializing the lock with a code including a site code. A second key device in the set is then used as a learn or program data key device. The start-up data key device contains an encrypted code which the lock decrypts using a manufacturer's encryption key, and the remaining special data key devices in the set use codes which can be authenticated by the lock using the site code data. Remaining special data key devices may be used, for example, to carry out such functions as lockout, emergency open, temporary unlock or passage mode, card cancel mode and to initiate an audit trail download.

It is furthermore an object of the present invention to provide an electronic door lock programming system which uses a set of special data key devices which are identified by number, the start-up data key device being numbered #1, the learn data key device being numbered #2, and remaining ones of the set of special data key devices being sequentially numbered #3 and up. Any suitable form of distinct labeling such as color coding, lettering, pictograms, etc. may be used in accordance with the invention.

It is furthermore an object of the present invention to provide an electronic door lock in which a master level data key device can be programmed in addition to ordinary level user data key devices. Preferably, there are two master levels, #1 and #2. Master level #1 keys cannot be cancelled by a corresponding cancel key, however, all master level #1 keys can be cancelled using a master level cancel key from the set of special data key devices used for programming and control purposes. Master level #2 keys may have corresponding master level cancel cards. Preferably, a master level key is allowed access at all times, and is able to unlock a double-locked door, i.e. the master level key preferably is able to unlock a deadbolt. A master level key may also be allowed to place a door in passage mode, i.e. to unlock the door for an extended period of time.

It is a further object of the present invention to provide a method for initializing and programming a number of electronic door locks installed in a facility in which a start-up data key device is used to permanently set each stand-alone electronic door lock with a site code. Preferably, the use of the

start-up data key device is done with all locks in the facility prior to programming each stand-alone electronic door lock with each user access and user cancel key.

According to a first broad aspect of the invention, there is provided a
5 method of programming an electronic door lock, activated to open using a plurality of data key devices, and programmable to accept new valid data key devices using a special data key device. The method comprises providing a set of special data key devices used for programming and control purposes, reading a start-up data key device to decrypt data therein and record a site
10 code associated with the set of special data key devices, reading a learn data key device to decrypt data therein, comparing the decrypted data with the site code, causing the lock to enter a new valid access data key learn mode when the comparison is positive, reading a first previously unknown code contained in a first new data key device while in the learn mode to record the first
15 unknown code as a valid access code for operating the lock, and reading a second previously unknown code contained in a second new data key device while in the learn mode to record the second unknown code as a cancel code paired with the valid access code of the first new data key device. In use, the lock is activated to open in response to the valid access code of the first new
20 data key device, and is activated to cancel the recorded valid access code in response to the cancel code of the second data key device.

According to a further aspect of the invention, there is provided a method of programming a plurality of stand-alone electronic door locks installed at different locations within a facility, the locks being activated to
25 open using a plurality of data key devices, and programmable to accept new valid data key devices using a learn data key device. The method comprises presenting the learn data key device to one of the plurality of locks, the one lock reading a learn code from the learn data key and recognizing the learn code as a valid learn code for the plurality of locks. A previously unknown
30 access data key is presented to the one lock, the one lock reading a previously unknown access code from the learn data key and enrolling the access code as a valid access code for the one lock when the one lock

recognizes the learn code as a valid learn code for the plurality of locks. A previously unknown cancel data key is presented to the one lock, the one lock reading a previously unknown cancel code from the learn data key and enrolling the cancel code as a valid cancel code paired with the enrolled valid access code enrolled for the one lock. The preceding steps are repeated for other ones of the plurality of locks in the facility. According to this aspect of the invention, previously unknown keys can be "learned" by touring the locks in a facility and enrolling the unknown keys by using the learn key.

According to a further aspect of the invention, there is provided a method of programming and controlling a plurality of electronic door locks in a facility using data key devices, the method comprising: providing a set of distinctly labeled special programming data key devices for use with the locks, the set of key devices comprising at least two of the following key devices: a learn mode key device; a master level access cancel key device; a lock-out key device; a passage key device; an emergency key device; and an audit key device, the set of key devices sharing a data characteristic associated with a site code; and providing the locks with the site code. The method further comprises at least two of the following steps:

using the learn key device to enroll at least one of access and cancel key devices for use with the locks;

using the master level access cancel key device to cancel all access key devices of a predetermined master level enrolled in the locks;

using the lock-out key device to lock-out a selected one of the locks;

using the passage key device to unlock for an extended period of time a selected one of the locks;

using the emergency key device to unlock the locks in an emergency; and

using the audit key device to allow audit trail data to be transferred from the locks to a portable data storage device.

Preferably, the set of data key devices further comprises a start-up key device, the step of providing the locks with the site code comprising using the start-up key device when the locks are installed and/or assigned to the facility.

Preferably, the set of key devices comprises at least three of the key devices, and the method comprises at least three corresponding ones of the further steps.

5 The present invention is particularly advantageous when the electronic door lock is a non-networked or stand-alone lock. The invention can, however, be advantageously applied to networked locks, particularly in the case of large facilities where the central control computer is not easily accessible. In such cases, the local programming of a lock can be either immediately processed and stored locally with the central control computer
10 backing-up and verifying the programmed codes, or the local key reader can be used as a remote terminal of the central control computer for programming and learning new user or master access and cancel keys. Preferably, when the local key reader is used as a remote terminal, the lock system according to the invention allows the programmer to identify whether the key being
15 learned is for the local lock or a group of locks.

Brief Description of the Drawings

The invention will be better understood by way of the following detailed description of a preferred embodiment with reference to the
20 appended drawing in which:

Figure 1 is a schematic block diagram of the stand-alone electronic door lock according to the preferred embodiment.

Detailed Description of the Preferred Embodiment

25 As illustrated in Figure 1, the electronic door lock according to the preferred embodiment is a non-networked, stand-alone lock and can be adapted for the full range of mortise and cylindrical lock chassis in which an electromechanical lock actuator 16 causes the door lever to engage a drive for retracting the latch. A deadbolt actuator 18 likewise is capable of causing
30 the door lever to retract a deadbolt within the lock. Although not shown in Figure 1, the lock may be provided with a mechanical key override and may

be provided with a panic device for overriding the lock in an emergency situation.

In the preferred embodiment, the lock microcontroller 12 is connected to a magnetic stripe card reader 14 although other forms of data key devices and readers 14 are contemplated within the scope of the present invention, and it will thus be appreciated that reference herein to steps of swiping include steps such as contacting, inserting and otherwise having such key devices read by the reader. The reader device may be mounted on the door or to a building near the door. The lock controller 12 controls a green LED 20 and a red LED 22 for providing feedback to the user during operation and during programming. Audio feedback may alternatively be provided.

In the preferred embodiment, a set of key cards are provided when locks for a facility are purchased. The set includes user access and cancel cards for each user, as well as special data key devices including the start-up key card (number 1), the learn key card (number 2), a lockout key card (number 3), an emergency key card (number 4), a passage key card (number 5), a master level cancel key card (number 6), and an audit key card (number 7). The data on these key cards is encrypted with a random code and the code is unique for each starter pack. Additional user cards are available in packs, and each user pack is a set of user access key cards and user cancel key cards. The cancel key cards are preferably labeled with a cancel symbol or appropriate text to clearly identify those cards as cancel cards, although these cards have the same encoding format (ABA format) and the data on the user key cards need not be encrypted. In the starter pack of key cards, the cards are preferably numbered #1 through #7 with clearly visible indicia and color coding with the cards being labeled with the numbering recited.

In the preferred embodiment, there can be up to 200 master level #1 or #2 users. The number of such users is merely limited by memory and design choice, and any number of such users can be provided.

When the start-up key card is used, the card reader 14 reads the encrypted data on the start-up card and the lock controller 12 decrypts the data using the manufacturer's encryption key 30 and extracts a site code for

the lock and stores it in a memory location identified as 32. If the site code memory 32 already contained a site code, the lock controller 12 would ignore the start-up card. To move a lock from one facility to a new facility, the site code memory 32 needs to be reset. Once the lock controller has determined
5 the site code and stored the site code in memory 32, the lock is ready to operate with any of the cards #2 through #7 of the start-up key card set and, of course, only those cards from the set of key cards determined by the start-up key card will be functional with the lock.

In the presently preferred embodiment, the learn key card labeled as
10 #2 is swiped in the card reader 14 as the first step in programming the lock. The lock controller 12 decrypts the data on the learn card using the site code and confirms that the learn key card belongs to the same pack as the start-up card. At this point, the lock controller 12 enters the "learn" mode and waits for a subsequent card to be swiped. In the presently preferred embodiment, the
15 next magnetic stripe card passed through the card reader 14 will be read and the identification code on the key card will be memorized. If the next card swiped through the card reader 14 is a different card having a different code, then the controller 12 adds the first user card swiped to the list of user access codes 34 and then adds the code of the second key card swiped to the list of
20 user cancel codes 36. If the same card is swiped twice, the lock controller 12 recognizes that card as the master level #2 card whose code is stored in memory 40. If the same card is swiped a third time, then the lock controller 12 will recognize the card as the master #1 card and store its code in memory 38. Storage of card key codes in memory can be deferred until the learn card
25 key #2 is swiped again. In the preferred embodiment, master level #2 cards have individual corresponding cancel cards and the controller expects a different card to be swiped the third time to register the master level #2 card's cancel card.

Both master level key cards have the unique privilege of being able
30 to actuate the lock actuator 16 as well as the deadbolt actuator 18. Furthermore, in the presently preferred embodiment, the master level #1 data card is provided with an additional privilege, namely, it may place the lock in

an unlocked passage mode for a predetermined time period, preferably nine hours. In the preferred embodiment, the master level #1 card key is preferably used by a senior manager or small business owner who "opens up shop" and may wish to unlock some doors for an entire working day. The
5 passage mode is entered using the master level #1 card key by swiping the card twice in short succession.

It will be appreciated that all of the magnetic stripe cards used for access may be any standard magnetic stripe card such as a bank card or credit card. In the preferred embodiment, the master level #1 cards do not
10 have corresponding cancel cards, but rather, the master level cancel card is provided within the starter pack of key cards card for canceling all master level #1 users. It will be appreciated that the master level cancel card could also be used, for example by a double swipe, to cancel all master level #2 cards.

15 Each time a user swipes a card through the card reader 14, the lock controller 12 records the data read from the card, the time from the unsynchronized local clock 44 as well as the status, such as access denied, access granted, passage mode entered and user cancelled, which audit trail data is recorded in memory 42. The memory 42 preferably stores sufficient
20 data for a relatively long period of time which may vary from less than a week to several months. When the audit card is read by the card reader 14, the lock controller decrypts its code and determines whether the audit card read is from the same starter pack, i.e. whether its site code matches the site code in the memory 32. If this is the case, the lock controller 12 allows the audit trail
25 data in memory 42 to be uploaded via a bus (not shown) to a portable computer. When the controller 12 outputs the audit trail data, it reads the current unsynchronized local clock and outputs the current local time which the portable computer matches with its own real time clock, in order to provide an accurate time reference for the unsynchronized local clock 44. In this way,
30 the audit trail data 42 can be adjusted to represent real synchronized time. While in the preferred embodiment, the adjustment to real time is done in the portable computer, it could likewise be done in the lock controller 12 itself by

first reading the real time from the portable computer, and then adjusting the time data in the audit trail data 42. It will also be appreciated that the exchange of audit trail data could be carried out by wireless, wired or physical transfer of a data recorder, such as a flash memory card.

5 Although in the preferred embodiment a single learn card is used for learning both master level and user level cards, it would be possible to provide two separate learn cards, one for learning master level cards and another for learning user level cards. This may be advantageous in circumstances in which the arrival of a new employee requires using the learn
10 card at each stand-alone electronic door lock in a facility along with the new employee's user card and user cancel card. To avoid accidental or intentional misuse of the single learn card which would result in the creation of a master level card, the provision of a user learn level card can be used. Under such circumstances, the task of learning a new user level card can be delegated to
15 someone who is not a master level user without posing a security risk.

 Although in the preferred embodiment the cancel card can be any key card, cancel cards can also be key cards which the lock controller 12 can identify as specific cancel card keys. This can be achieved either by using a header code or the like which identifies the card to the lock as a cancel card.
20 Likewise, the card key code can be encrypted, and the information that the cancel card is a genuine cancel card can be determined either from the successful decryption of the code recorded on the card key and/or by the presence of a header code or the like. The lock controller 12 can then only accept card keys, identified as cancel cards, during enrolment or registration
25 as a cancel card. The controller can also refuse a card key, identified as a cancel card, during registration or enrolment as a user or master level access card. In this way, there can be no confusion between user access cards and user cancel cards.

 In the preferred embodiment, there is no distinction between user
30 keys and master keys in terms of the codes contained thereon. This allows any type of key to be used for either a user level or master level key. It will be appreciated, however, that a header code could be provided for master level

keys, and the controller could reject the registration of a master level key in absence of the header code being present in the key's code (whether encrypted or not). The master level keys could be distributed in separate packs and stored in a secure place prior to authorized initialization or
5 registration.

When a smart key is used (i.e. one having its own data processing abilities), it will be appreciated that it is possible for the key's code to be communicated only when the reader presents the correct key or identification data, or for the key's code not to be communicated at all, but rather for the
10 key's code to be verified by the reader as a result of the key's response to a query from the reader. This allows for greater security and reduces the chance that a key's code can be copied and used by an unauthorized intruder.

While the invention has been described above with reference to
15 embodiments in which the lock is a stand-alone lock, the invention can also be applied to networked locks. Lock controller 12 can be provided with a network communication interface, such as a LAN card. The local programming of the lock can be immediately processed and stored locally by controller 12, with a central control computer connected to controller 12 via
20 the network communications interface backing-up and verifying the programmed codes. Alternatively, the controller 12 can allow the local key reader 14 to be used as a remote terminal of the central control computer for programming and learning new user or master access and cancel keys by the central control computer. In such networked locks, the lock may store locally a
25 list of valid access codes to allow entry without need to communicate with the central computer. The central computer may be used for audit trail and list updating purposes only. Alternatively, the lock may not be able to authorize entry without permission from the central control computer, except in emergency situations. Preferably, when the local key reader is used as a
30 remote terminal, the lock system according to the invention allows the programmer to identify whether the key being learned is for the local lock or a

group of locks. This can obviate the need to enroll keys with each individual lock within a facility.

It will be appreciated that many variations to the preferred embodiment described above are possible within the spirit and scope of the
5 present invention.

CLAIMS:

1. An electronic door lock, activated to open using a plurality of data key devices, and programmable to accept new valid data key devices using a special data key device, the lock comprising:

a site code recorder responsive to a start-up data key device to decrypt data therein and record a site code associated with a set of special data key devices used for programming and control purposes;

a learn mode controller responsive to a learn data key device to decrypt data therein, compare said decrypted data to said site code, and enter into a new valid access data key learn mode when said comparison is positive;

a valid access code recorder responsive to a first previously unknown code contained in a first new data key device while in said learn mode to record said first unknown code as a valid access code for operating said lock; and

a cancel code recorder responsive to a second previously unknown code contained in a second new data key device while in said learn mode to record said second unknown code as a cancel code paired with said valid access code of said first new data key device;

wherein, in use, said lock is activated to open in response to said valid access code of said first new data key device, and is activated to cancel said recorded valid access code in response to said cancel code of said second data key device.

25

2. The electronic door lock as claimed in claim 1, wherein said lock operates with at least one master level and a user level, said valid access recorder being responsive while in said learn mode to a single reading of said first new data key device for recording said first unknown code as a valid user level access code for operating said lock, and said valid access recorder being responsive while in said learn mode to a repeated reading of said first

30

new data key device for recording said first unknown code as a valid master level access code for operating said lock.

3. The electronic door lock as claimed in claim 2, wherein said master level access code is not paired with a cancel code, said master level access code being cancelled by one of said set of special data key devices used for programming and control purposes.

4. The electronic door lock as claimed in claim 2, wherein said lock comprises a dead-bolt, and, in use, said lock is activated to open said dead-bolt only in response to said valid master level access code, whereby a master level key device can open said lock even when double-locked.

5. The electronic door lock as claimed in claim 2, wherein in use, said lock is activated to remain open for one of an undetermined period and an extended period of time in response to a repeated reading of said valid master level access code, whereby a master level key device can place said lock in passage mode.

6. The electronic door lock as claimed in claim 1, wherein said lock is a stand-alone lock.

7. The electronic door lock as claimed in claim 6, wherein one of said set of special data key devices used for programming and control purposes is provided for audit trail purposes, said lock comprising an audit trail memory, an audit trail data recorder recording audit trail data in said memory as said lock reads key devices and operates, and a data transfer controller for transferring audit trail data from said memory to a data communications interface, said data transfer controller allowing transfer of said audit trail data when said audit trail one of said set of key devices is read by said lock.

8. The electronic door lock as claimed in claim 7, further comprising an unsynchronized time clock, said audit trail memory containing a time value from said clock for at least some events recorded in said memory, said data transfer controller providing a current time reading from said clock when said
5 audit trail data is transferred to said data communications interface, whereby a recipient of said audit trail data having a synchronized real time clock can adjust said time values for said events to be synchronized.

9. A method of programming an electronic door lock, activated to open
10 using a plurality of data key devices, and programmable to accept new valid data key devices using a special data key device, the method comprising:

providing a set of special data key devices used for programming and control purposes;

15 reading a start-up data key device to decrypt data therein and record a site code associated with a said set of special data key devices;

reading a learn data key device to decrypt data therein;

comparing said decrypted data to said site code;

causing said lock to enter into a new valid access data key learn mode when said comparison is positive;

20 reading a first previously unknown code contained in a first new data key device while in said learn mode to record said first unknown code as a valid access code for operating said lock; and

25 reading a second previously unknown code contained in a second new data key device while in said learn mode to record said second unknown code as a cancel code paired with said valid access code of said first new data key device;

30 wherein, in use, said lock is activated to open in response to said valid access code of said first new data key device, and is activated to cancel said recorded valid access code in response to said cancel code of said second data key device.

10. The method as claimed in claim 9, wherein said lock operates with at least one master level and a user level, said step of reading and recording a valid access code comprising a single reading of said first new data key device and then recording while in said learn mode said first unknown code as
5 a valid user level access code for operating said lock, and a repeated reading of said first new data key device and recording while in said learn mode said first unknown code as a valid master level access code for operating said lock.

10 11. The method as claimed in claim 2, wherein said master level access code is not paired with a cancel code, said master level access code being cancelled by one of said set of special data key devices used for programming and control purposes.

15 12. The method as claimed in claim 2, wherein said lock is programmed to open a dead-bolt only in response to said valid master level access code, whereby a master level key device can open said lock even when double-locked.

20 13. The method as claimed in claim 2, wherein said lock is programmed to remain open for one of an undetermined period and an extended period of time in response to a repeated reading of said valid master level access code, whereby a master level key device can place said lock in passage mode.

25 14. The method as claimed in claim 9, wherein said lock is a stand-alone lock.

15. The method as claimed in claim 14, further comprising:
providing one of said set of special data key devices used for
30 programming and control purposes for audit trail purposes;
providing an audit trail memory and recording audit trail data in said memory as said lock reads key devices and operates; and

allowing transfer of said audit trail data to an external device only when said audit trail one of said set of key devices is read by said lock.

16. The electronic door lock as claimed in claim 15, further comprising:

5 providing an unsynchronized time clock;

recording a time value from said clock in association with at least some events in said memory;

10 providing a current time reading from said clock when said audit trail data is transferred to said external device, whereby a recipient of said audit trail data having a synchronized real time clock can adjust said time values for said events to be synchronized.

17. A method of programming a plurality of stand-alone electronic door locks installed at different locations within a facility, said locks being activated
15 to open using a plurality of data key devices, and programmable to accept new valid data key devices using a learn data key device, the method comprising:

20 presenting said learn data key device to one of said plurality of locks, said one lock reading a learn code from said learn data key and recognizing said learn code as a valid learn code for said plurality of locks;

25 presenting a previously unknown access data key to said one lock, said one lock reading a previously unknown access code from said learn data key and enrolling said access code as a valid access code for said one lock when said one lock recognizes said learn code as a valid learn code for said plurality of locks;

presenting a previously unknown cancel data key to said one lock, said one lock reading a previously unknown cancel code from said learn data key and enrolling said cancel code as a valid cancel code paired with said enrolled valid access code enrolled for said one lock; and

30 repeating said preceding steps for other ones of said plurality of locks in said facility.

18. A method of programming and controlling a plurality of electronic door locks in a facility using data key devices, the method comprising:

providing a set of distinctly labeled special programming data key devices for use with said locks, said set of key devices comprising at least two
5 of the following key devices: a learn mode key device; a master level access cancel key device; a lock-out key device; a passage key device; an emergency key device; and an audit key device, said set of key devices sharing a data characteristic associated with a site code; and

providing said locks with said site code;

10 the method further comprising at least two of the following steps:

using said learn key device to enroll at least one of access and cancel key devices for use with said locks;

using said master level access cancel key device to cancel all access key devices of a predetermined master level enrolled in said locks;

15 using said lock-out key device to lock-out a selected one of said locks;

using said passage key device to unlock for an extended period of time a selected one of said locks;

using said emergency key device to unlock said locks in an emergency; and

20 using said audit key device to allow audit trail data to be transferred from said locks to a portable data storage device.

19. The method according to claim 18, wherein said set of data key devices further comprises a start-up key device, said step of providing said
25 locks with said site code comprising using said start-up key device when said locks are installed and/or assigned to said facility.

20. The method according to claim 18, wherein said set of key devices comprises at least three of said key devices, and said method comprises at
30 least three corresponding ones of said further steps.

21. The method according to claim 19, wherein said set of key devices comprises at least three of said key devices, and said method comprises at least three corresponding ones of said further steps.

