



(72) MESSIER, YVES, CA

(72) DOYON, PIERRE, CA

(72) TOLEDANO, ANICK, CA

(72) LIVEANU, RODICA, CA

(72) BERNSTEN, STEVEN, CA

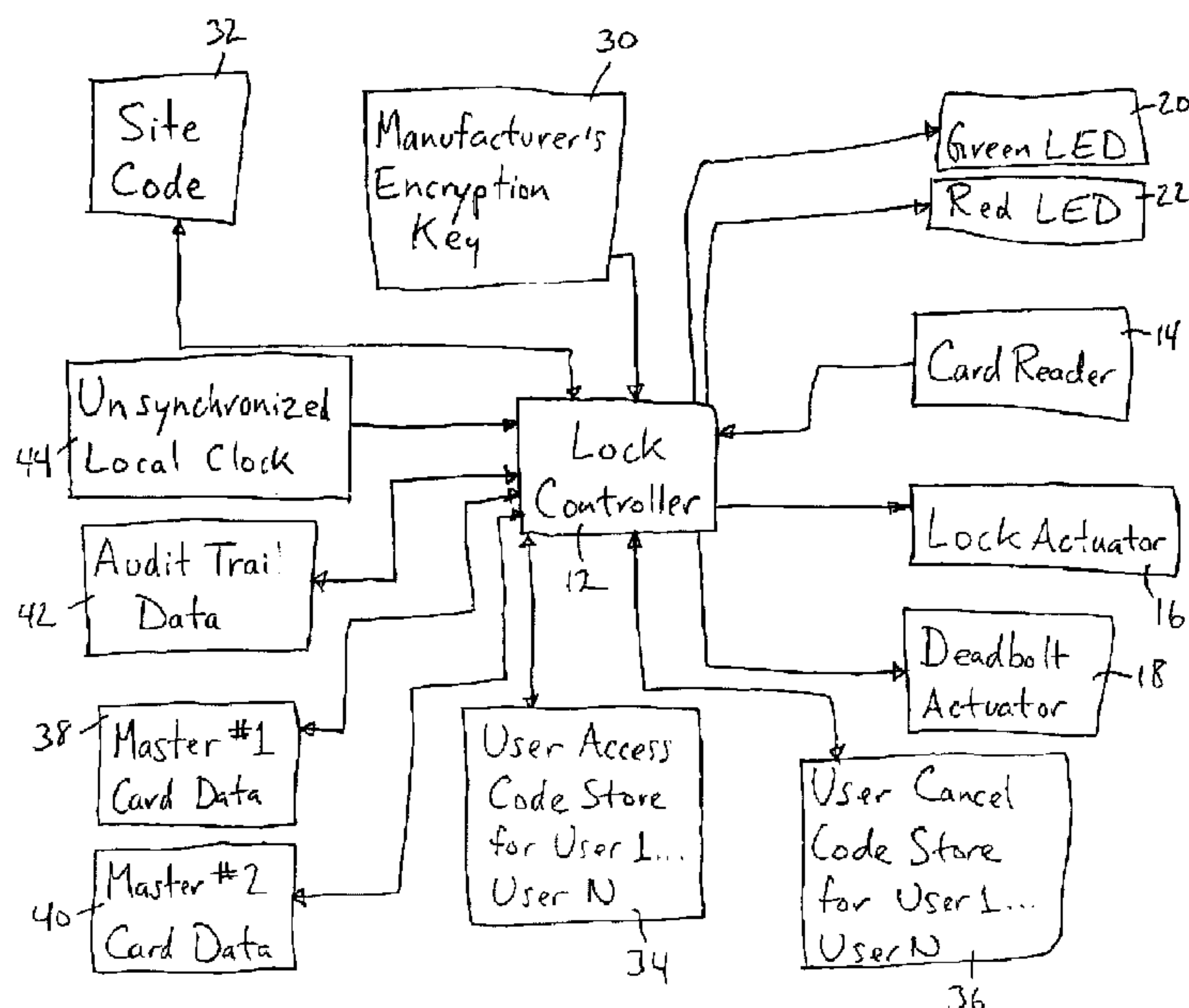
(72) BAO, CO PHAT HUYHN, CA

(71) ILCO UNICAN INC., CA

(51) Int.Cl.⁷ E05B 47/00, E05B 19/00

(54) **CLEF DE CONTROLE HIERARCHIQUE POUR
VERROUILLAGES ELECTRONIQUES**

(54) **HIERARCHICAL KEY CONTROL FOR ELECTRONIC LOCKS**



(57) 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.

- 11 -

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.

- 1 -

HIERARCHICAL KEY CONTROL FOR ELECTRONIC LOCKS**Field of the Invention**

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

Background of the Invention

10 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 smart card, a Dallas™ key or the like. Given the
15 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 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
20 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
25 between each electronic door lock and a central control computer. In such a configuration, a code read from a data key device is 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 also controls changes to access
30 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
35 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

8027-56CAPR
December 7, 1999

- 2 -

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.

5 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. In this case, a data key device from the set of
10 acceptable 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 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
15 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 a stand-alone 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
20 the use of a predetermined set of codes recorded in the data key devices. There is furthermore a need for such a stand-alone electronic door lock in which the programming is simple, stepwise and flexible to the needs of small and medium facilities.

25 **Summary of the Invention**

It is accordingly a first object of the present invention to provide a stand-alone 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
30 initializing the lock with a code including a site code. A second key device in the set is 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 to
35 carry out such functions as lockout, emergency open, temporary unlock or passage mode, card cancel mode and to initiate an audit trail download.

8027-56CAPR
December 7, 1999

- 3 -

5 It is furthermore an object of the present invention to provide a stand-alone 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.

10 It is furthermore an object of the present invention to provide a stand-alone electronic door lock in which a master level data key device can be programmed in addition to ordinary level user data key devices. Preferably, while individual user keys can be cancelled with a corresponding cancel key, master level keys cannot be cancelled by a corresponding cancel key, however, all master level keys can be cancelled using a master level cancel key from the set of special data key devices used for programming and control purposes. 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.

20 It is a further object of the present invention to provide a method for initializing and programming a number of stand-alone 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.

25 According to a first broad aspect of the invention, there is provided a method of programming a stand-alone electronic door lock, activated to open using a plurality of data key devices, and programmed 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 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 unknown code as a valid access code for operating the lock, and reading a second

8027-56CAPR
December 7, 1999

- 4 -

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 the second data key device.

Brief Description of the Drawings

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

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

15

Detailed Description of the Preferred Embodiment

As illustrated in Figure 1, the stand-alone electronic door lock according to the preferred embodiment 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 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.

25

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. 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.

30

In the preferred embodiment, the key cards come in two "packs", namely, a starter pack which is the set of 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

35

8027-56CAPR
December 7, 1999

- 5 -

5 encrypted with a random code and the code is unique for each starter pack. The 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 is not 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.

10 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.

15 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, which is done by disabling the battery power to the lock for a sufficient period of time to erase the memory. It will be appreciated that other means of erasing the site code memory are possible. Once the lock controller has determined 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.

25 In the presently preferred embodiment, the learn key card labeled as #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 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

8027-56CAPR
December 7, 1999

- 6 -

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 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 key #2 is swiped again.

Both master level key cards have the unique privilege of being able 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 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 cards do not have corresponding cancel cards, but rather, the master level cancel is provided within the starter pack of key cards card for canceling all master users. It will be appreciated that in an environment where a larger number of master level cards is required, it would be possible to provide for individual master level cancel cards rather than a single master level cancel card for removing all master users.

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 data for a relatively long period of time which may vary from 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

8027-56CAPR
December 7, 1999

- 7 -

lock controller 12 allows the audit trail 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, 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.

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 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 someone who is not a master level user without posing a security risk.

Although in the preferred embodiment the cancel card can be any user key card, cancel cards can also be key cards (or other data key devices) which the lock controller 12 can identify as 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. 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 as a cancel card. The controller can also refuse a card key, identified as a cancel card, during registration or enrolment as a user card. In this way, there can be no confusion between user access cards and user cancel cards. It will also be appreciated that the same type of coding could be

8027-88CAPR
December 7, 1999

- 8 -

used with master level cancel card keys, in the case that cancel card keys are used for master level users.

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

5

8027-58CAPR
December 7, 1999

- 9 -

What is claimed is:

1. A stand-alone electronic door lock, activated to open using a plurality of data key devices, and programmed to accept new valid data
5 key devices using a special data key device, the lock comprising:
means 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;
means responsive to a learn data key device to decrypt data
10 therein, compare said decrypted data to said site code, and enter a new valid access data key learn mode when said comparison is positive;
means 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
15 means 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
20 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.
2. A method of programming a stand-alone electronic door lock,
25 activated to open using a plurality of data key devices, and programmed 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;
30 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;

8027-56CAPR
December 7, 1999

- 10 -

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

5 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

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;

10 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.

8027-56CAPR
December 7, 1999

07/12/1999	17:37	514 288 8389	received
------------	-------	--------------	----------

