(54) Title: THE MANAGEMENT OF KEY USAGE

(57) Abstract: The invention provides a key storage device (16) which includes a secure container (20) for securely storing a plurality of keys (12). The device (16) includes a dispensing arrangement for dispensing a particular one of the keys (12) upon request, to permit removal of that key from the container (20). The invention also provides a system (10) for managing use of a plurality of keys (12), the system comprising the key storage device (16) and a control means (18) in communication with the secure storage device (20) to control the dispensing of keys (12) from the storage device (20) upon request. The invention extends to a method of managing the use of a plurality of keys (12).
Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

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

This invention relates to the management of key usage. In particular, the invention relates to a secure storage device for the secure storage of a plurality of keys. The invention also relates to a key storage device. The invention extends to a system for management of the use of a plurality of keys. The invention also relates to a method of managing the use of a plurality of keys. The invention extends yet further to a computer program, to a data storage device, and to a data carrier.

The invention provides a key storage device which includes:

- a secure container having an interior for securely storing a plurality of keys; and
- a dispensing arrangement for dispensing a particular one of the keys upon request, to permit removal of the particular key from the secure container.

By dispensing is meant that access is provided to the requested key for removal thereof, while the rest of the keys remain securely stored and inaccessible. It will thus be appreciated that the dispensing arrangement will be arranged to dispense the requested key such that access to the remainder of the keys in the secure container is prevented while a requested key is being dispensed.

The storage device may thus function in a manner similar to conventional vending machines, in that a person standing at the device will be able to remove from the container only a key which has been requested particularly and which has been dispensed by the storage device. By key is meant any device which is required for the operation of another machine or device, or which is required for gaining access to a restricted area. The invention is thus applicable to the management of the use of mechanical keys, key-cards, electronic keys, and the like.

The secure container may be a safe-type unit having a lockable theft-
resistant door. It will be appreciated that secure storage of the keys means that the keys are inaccessibly stored in the storage device.

The device may include a tag reading means for reading tags respectively attached to the keys upon dispensing and/or replacement of any key, each tag being attached to a respective key. The tag reading means may be arranged for reading electronic tags on which are stored respective unique tag codes, each tag, for instance, being an i-Button or the like.

The tag reading means may include a tag reading device positioned at a dispensing bay where keys are dispensed from the secure container. The device may have a plurality of dispensing bays and the tag reading means may comprise a plurality of tag reading devices associated respectively with the dispensing bays.

The secure container may include a dispensing bay for dispensing requested keys, the dispensing arrangement including a conveyor for conveying a particular key which is to be dispensed to the dispensing bay. The dispensing bay may have an openably closable access opening for permitting access to a key held in the dispensing bay, the access opening being closed off by a barrier which is displaceable between an open position in which access to the dispensing bay, and hence to a key in the dispensing bay, is permitted, and a closed position in which access to the dispensing bay is securely barred by the barrier.

The access opening may be a cut-out in a wall of the container adjacent the dispensing bay, and the barrier is a plate which is mounted face-to-face with the wall of the container, the plate being slidably displaceable in a direction parallel to a plane in which the plate lies, the plate having an access aperture which can be brought into register with the access opening in the wall of the container to permit access to the interior of the dispensing bay.

The container may have a plurality of dispensing bays, said wall of the container having a corresponding number of cut-outs therein and the barrier plate having a corresponding number of access apertures. The access apertures in the barrier plate and the cut-outs in said wall of the container may be arranged such that the
dispensing bays can be opened separately by appropriate sliding displacement of the barrier plate.

Thus, in use, to dispense a particular key, the conveyor is moved such that the key is moved into the dispensing bay, whereafter the barrier plate is displaced into a position in which the access opening to the dispensing bay is unobstructed, so that the key can be removed manually from the conveyor.

The conveyor may be an endless belt or chain drive to which key-holders are connected at regular intervals, each key-holder being arranged for removably holding at least one of the keys. Each key-holder may be a bar which extends transversely to the belt or chain, so that two separate keys can be secured to opposite ends of each bar.

The device may include a control means for authorising dispensing of particular keys from the secure container in response to requests for dispensing of the keys. The control means will typically be an electronic processor in communication with the dispensing arrangement, the electronic processor, for instance, being provided by computer equipment which is in electronic communication with the dispensing arrangement. In one embodiment of the invention, the control means is provided by a computer system connected to the secure container, the computer system being provided with computer software for authorising and monitoring the dispensing of particular keys from the secure container.

The storage device may thus include a connection interface mounted on the secure container for connection to computer equipment, the connection interface being for placing electronic control equipment of the dispensing arrangement in the container in communication with off-board computer equipment.

The device may include a biometric identification device for reading a biometric parameter of a person to whom a key is to be dispensed, the biometric identification device being in communication with the control means. The control means may be arranged to dispense a key upon request only if the measured biometric parameter of a person requesting dispensing of a particular key is matched with a pre-stored biometric parameter associated with a person who is authorised to use that
particular key.

The device may include a printer mounted on the container for producing a printed document upon issuing and/or returning of a key.

The storage device may include a visual display mounted on the container, for instance being an LCD display or the like.

The invention extends to a system for managing use of a plurality of keys, which system includes:

- a key storage device as defined above; and
- a control means in communication with the secure storage device to control the dispensing of keys from the storage device upon request.

The control means may include an electronic processor which is in communication with the dispensing arrangement forming part of the secure storage device, the electronic processor being configure for controlling operation of the dispensing arrangement. The control means may be provided by a computer positioned adjacent the secure storage device, the computer providing a user interface for requesting the dispensing of keys from the device. The secure storage device may be connected to a network of computers, so that a user can request the dispensing of a particular key at any one of a plurality of computers on the network.

The control means may be provided by computer equipment and include computer software associated with the computer or computers.

The system may include an information database on which is stored identification data associated with persons who are authorised to remove respective keys from the secure storage device. The information database may include data indicative of a personal identification code and/or a biometric parameter associated with the respective authorised persons.

The system may include a verification arrangement for verifying whether or not dispensing of a particular key to a person requesting dispensing of that key is
authorised. The verification arrangement may be configured for checking whether or not an entered identification code corresponds to an identification code on the information database.

The verification arrangement may be configured for reading a biometric parameter of a person requesting dispensing of a particular key, and for verifying whether or not the measured biometric parameter corresponds to a biometric parameter associated in the information database with a person authorised to remove the requested key.

The control means may provide a request arrangement is configured for requiring the entry of an identification code on an input means connected to the secure storage device, as well as for prompting the entry of an indication of which key is required.

The system may include computer equipment in communication with the storage device and arranged to receive and store information from a tag reading means incorporated in the storage device for reading electronic tags connected to the respective keys, the computer equipment being configured for generating and storing a record of the time at date at which respective keys were removed from the storage device, the record including the identification code which was entered for dispensing of each key.

The system may thus include a monitoring arrangement for monitoring use of the keys, the monitor arrangement being arranged for recording when and by whom each key is removed from and/or returned to the secure storage device.

The system may be configured for managing the use of keys which are for operating respective vehicles, the system including an interface for connection to an access control system of a compound on which the vehicles are resident, the system being arranged for permitting the exit of a particular one of the vehicles from the compound only if the respective key of the particular vehicle has been dispensed from the secure storage device to an authorised person. The access control system of the compound may thus form part of the key management system.
The invention extends to a method of managing the use of a plurality of keys, which method includes securely storing the keys in a secure storage device and automatically dispensing a particular key to an authorised person upon request.

By automatic dispensing of a key is meant that dispensing of the key is automated, being performed by a dispensing means in response to a request by an authorised person, without human intervention in processing the request or in dispensing the key.

The method may include the step of verifying whether or not dispensing of a particular key to a person requesting dispensing of that key is authorised. Such verification may include requiring the input of an identification code, the key which has been requested being dispensed only if the entered code corresponds with a pre-established identification code associated with the requested key. The identification code may be entered on an input means which is in electronic communication with the secure storage device, the input means being positioned adjacent the secure storage device, or forming part of a computer network which to which the secure storage device is connected.

The identification code may be a personal identification code for identifying a particular person who is authorised to access at least some of the keys, the method including the step of checking the entered personal identification code against a database of authorised identification codes, and permitting dispensing of a particular key only if the entered personal identification code is associated in the database with the particular key. It will be appreciated that each person will be authorised to access one or more of the keys, each personal identification code being associated in the information database with those keys which the respective person is authorised to use.

The method may include measuring a biometric parameter of a person who is positioned at the secure storage device, and dispensing the key to that person only if the measured biometric parameter corresponds to a pre-authorised biometric parameter. Measuring a biometric parameter of the person may comprise reading a fingerprint of the person and dispensing the requested key only if the fingerprint reading corresponds to a stored fingerprint associated with the identified person on the
database, the requested key is dispensed.

In one embodiment of the invention, a person who wishes to use one of the securely stored keys will be required to enter a personal identification code on an input means connected to the secure storage device, and to indicate which key is required. The entered identification code is then automatically checked against the information database, and it is verified whether or not that person is authorised to use the requested key. At the secure storage device, a fingerprint reading is taken and if the fingerprint reading corresponds to a stored fingerprint associated with the identified person on the database, the requested key is dispensed.

The method may include keeping a record of particulars of the dispensing of keys from the secure storage device and the return of keys to the secure storage device.

Each key may be uniquely associated with an electronic tag which is connected to the key, the tag being read by the secure storage device upon dispensing from and return of the respective keys to the secure storage device, to monitor movement of the keys. In such case, the access control system of the compound may require reading of each tag at an exit from the compound, the vehicle being permitted to exit the compound only if the associated key, as indicated by the tag, has been dispensed from the secure storage device.

The method may include identifying each person to whom one of the keys is dispensed, and noting and recording the date and time at which each key is dispensed.

The keys may be for operating respective vehicles, the method including permitting the exit of any one of the vehicles from a compound on which the vehicles are resident only if the respective key of the particular vehicle has been dispensed from the secure storage device to an authorised person.

The access control system of the compound may require require reading of each tag at an exit from the compound, the vehicle being permitted to exit the compound only if the associated key, as indicated by the tag, has been dispensed from the secure storage
device.

The invention extends yet further to a computer program, and to a set of computer readable instructions, for enabling a computer system to perform a method of managing the use of a plurality of keys, as defined above, when the computer program is executed on the computer system.

The invention also extends to computer equipment which has stored thereon a computer program as defined above.

The invention also relates to a data storage device, and to a data carrier, which has stored thereon a computer program as defined above.

The invention will now be further described, by way of example, with reference to the accompanying diagrammatic drawings, in which:

Figure 1 is a schematic sectional side view of a system for managing the use of a plurality of keys, in accordance with the invention;

Figure 2 is, on an enlarged scale, a view corresponding to Figure 1 of a secure storage device forming part of the system of Figure 1, in use, taken at line II-II in Figure 4;

Figure 3 is a view corresponding to Figure 2, showing the manual removal of a key from the secure storage device, taken at line III-III in Figure 5;

Figure 4 is a front elevation of the storage device of Figure 2, showing both dispensing bays of the storage device in a closed condition;

Figure 5 is a view corresponding to Figure 4, one of the dispensing bays being in an open condition for dispensing a key from the storage device; and

Figure 6 is a schematic view of a further embodiment of a system for managing the use of a plurality of keys, in accordance with the invention.

In Figure 1 of the drawings, reference numeral 10 generally indicates a system for managing the use of a plurality of keys, in accordance with the invention. In this example, the system 10 is used for controlling and monitoring the use of a plurality of keys 12 of motor vehicles (not shown) on a used car compound (schematically indicated by reference numeral 14 in Figure 6). For ease of illustration, the keys 12 are
omitted in Figures 4 and 5.

It should be appreciated that the invention is particularly useful in the safe storage of keys for motor vehicles, but that the invention is not limited to this application and can indeed be used for the storage of any keys. The system 10 can thus, for instance, be used with similar effectiveness for the storage of building keys in a real estate environment, keys for any fixed or movable assets, keys for earthmoving equipment, keys for mechanised transport such as motorbikes or jetskis, and keys for providing access to pharmaceutical drugs.

The system 10 includes a secure storage device 16 for storing the keys 12 in a secure and theft-resistant manner. The storage device 16 has a dispensing arrangement for dispensing any one of the keys 12 upon request. The system 10 further includes a control means provided by a personal computer 18 which is in electronic communication with the storage device 16 for controlling dispensing of keys 12 from the storage device 16 and for keeping record of use of the keys 12.

In this example, the storage device 16 includes a box-shaped container in the form of a safe 20 which has a hollow interior in which the keys 12 are stored. The safe 20 has walls of 3mm powder-coated plate steel, the interior being accessible only through a securely lockable maintenance door (not indicated) which is unlocked only for maintenance purposes, and through a pair of access openings in the form of cut-outs 22 in a front wall 24 of the safe 20.

Each access opening 22 is operable between a closed condition (Figures 2 and 4) in which the access opening 22 is barred by a barrier plate 26 which is positioned flush against the inside of the front wall 24, face-to-face with the front wall 24; and an open condition in which a complementary access aperture 28 in the barrier plate 26 is in register with the access opening 22 in the front wall (Figures 1, 3 and 5), permitting manual access to a key 12 in a corresponding dispensing bay 30 inside the safe 20.

Each dispensing bay 30 is defined inside the safe 20 by a cup-shaped shield 32 which is stationary relative to the front wall 24. In use, the shield serves to prevent
access to keys 12 other than the key 12 which is positioned inside the dispensing bay 30, when the access opening 22 is open.

The barrier plate 26 is connected to a displacement mechanism for slidably displacing the plate 26 up or down, to bring one of the pair of access apertures 28 in the plate 26 in register with a desired access opening 22 in the front wall, to open one of the dispensing bays 30. As can best be seen in Figures 4 and 5, the access apertures 28 in the plate 26 are vertically aligned with the respective access openings 22 in the front wall 24, but the access apertures 28 are horizontally staggered, so that the dispensing bays 30 can be opened separately by vertical displacement of the barrier plate 26.

The displacement mechanism is in the form of a telescopic shaft 34 which is variable in length by relative screwing displacement of a pair of telescopic members forming the shaft 34. To this end, the device 10 includes an electric motor 36 for driving the telescopic shaft 34 to effect displacement of the barrier plate 26. The motor 36 is connected to a control unit 38 which includes an electronic PC-board for controlling the motor 36, thus controlling opening and closing of the dispensing bays 30 by controlling the position of the barrier plate 26.

It will be appreciated that the mechanism for opening the dispensing bays 30 as described with reference to this example is one of many possible configurations. Thus, in other examples of the invention, each dispensing bay can be a corner unit with a revolving door, the door being pivotally displaceable about an upright pivot axis through 180° in either direction. In another embodiment, the dispensing bays can be opened and closed by a horizontally extending barrel with openings therein, so that pivotal displacement of the barrel about a horizontal pivot axis will result in opening and closing of the bays.

The device 10 further includes a conveyor to which the keys 12 are connected, the conveyor being movable to position a particular key in one of the dispensing bays 30. In this example, the conveyor is the form of an endless chain 40 which passes over a driven pulley 42 and a return pulley 44. The pulleys 42, 44 are mounted in the interior of the safe 20 for rotation about horizontal axes which are vertically spaced apart. In other embodiments, the chain 40 can extend horizontally.
A series of key holders in the form of transverse bars 46 are secured to the chain 40 at regular intervals. Each bar 46 extends horizontally, transverse to the chain 40. Each bar 46 has recesses at opposite ends thereof for supporting a key 42 on the bar 46 via a key ring. Each bar 46 thus supports two separate keys 42. As can best be seen in Figures 4 and 5, keys 12 on one end of the bars 46 are in vertical register with one of the dispensing bays 30, while keys 12 on the other end of the bars 46 are in vertical register with the other dispensing bay 30. The shields 32 which define the respective dispensing bays 30 each has slots therein to permit passage of the chain 40, bars 46, and keys 12 through the dispensing bays 30.

The conveyor includes a micro-switch 53 for measuring the position of the chain 40, or an opto-coupler transmitter and receiver pair that senses the chain’s position, the micro-switch being in communication with the control unit 38, to permit accurate positioning of the chain 40 such that one of the key bars 46 is exactly in register with the dispensing openings 22.

It should be appreciated that, in other examples of the invention, the safe can have more than two dispensing bays 30. In particular, the device can, for instance, have two of the chains 40, thus having four dispensing bays 30, and so forth. Instead, or in addition, each key bar 46 can be used to support not only two sets of keys 12, but can, for instance support four sets of keys 12, or more. To this end, each key bar 46 can have connected to it a plurality of key holders, such as key hooks, for holding respective keys or sets of keys. Instead, each key or set of keys can be held on the chain 40 in a bucket- or tray type holder connected to the chain 40.

The secure storage device 16 further includes a tag reading means in the form of a pair of tag readers 48 mounted in the safe 20, the tag readers 48 respectively being positioned to read electronic tags 50 connected to keys 12 in the dispensing bays 30. To this end, each shield 32 has a window for permitting reading of the tags 50 by the respective readers 48.

It will be appreciated that, in use, the ring of each key 12 will carry, in addition to the key 12, an electronic tag 50, in this case an i-button, for identifying each key 12. Each tag 50 carries a unique code associated with the respective key 12.
In this example, the tag readers 48 are mounted inside the safe 20, so that there has to be one tag reader 48 for each dispensing bay 30. However, in other embodiments of the invention, a single tag reader can be mounted outside the safe 20, so that only one tag reader is required, irrespective of the number of dispensing bays.

The secure storage device 16 yet further includes a biometric reading device in the form of an electronic fingerprint reader 52 mounted on the front wall 24 of the safe 20. Although not shown in the drawings, the fingerprint reader 52 is in electronic communication with the control unit 38, so that a reading taken by the fingerprint reader 52 can be sent to the control unit 38 and therefore to the PC 18.

A small printer 54 is also provided at the front wall 24, to print receipts or passes which evidence dispensing of a particular key 12. The printer 54 is of course also in communication with the control unit 38 and with the PC 18. The storage device 16 further includes an LCD display 60 mounted in the front wall 24, so that commands or information can be displayed on the display 60 for communication with a user requesting dispensing of a key 12.

The PC 18 is provided with a computer program (not shown) for controlling the storage device 16, and particularly for verifying whether or not any person requesting the dispensing of a key 12 is authorised to use that particular key 12.

The PC 18 maintains an information database, which for ease of description is described as two databases 56 and 58. The first is an authorisation database 56 on which is stored information regarding each of the plurality of keys 12 and the identities of persons who are permitted to use the respective keys 12 or to remove the keys 12 from the safe 20. In respect of each key 12, there will thus be stored data indicative of: the vehicle which is operated by that key 12; the code of the tag 50 associated with that key; and a list of persons who are permitted to use or remove that key 12.

The authorisation database 56 also includes personal details of each person who is authorised to remove some of the keys 12. In particular, the database 56 includes, in respect of each person, data indicative of: the personal details of that person, such as his name, employee number, etc; a personal identification code
associated with that person; and fingerprint details of that person.

The other database is a logging database 58 for recording or logging the particulars of use of the keys 12. The database 58 will thus record, in respect of each key removal, by who the key 12 was removed, as well as the date and time of removal of the key.

In conventional fashion, the PC 18 includes an input means in the form of a keyboard 62, and a display means in the form of a computer screen 64.

In use, the keys 12 for operating a plurality of used cars 12 are securely stored in the storage device 16. When thus stored, the keys 12 can only be removed from the safe 20 by breaking open of the safe 20 or by authorised dispensing of a particular key 12. This restricts unauthorised usage of the keys 12, and thus of the vehicles which are operated by the keys 12.

If a person requires use of a particular key 12, a request for that key is entered on the keyboard 62 of the PC 18. The person is then prompted to enter a personal identification code, so that the user can be identified. The PC 18, by operation of the software provided on it, verifies, with reference to the authorisation database 56, whether or not the entered personal identification code corresponds to any of the codes stored on the database 56. If the identification code is correct, the PC 18 checks whether or not the person associated with the entered identification code is authorised to remove the particular key 12 which has been requested.

In this example, the issuing of a key is requested by entering data on the keyboard of the 62 of the PC 18. However, in other examples of the invention, the method may include reading a code, for example a bar code, on a vehicle whose keys 12 are required, so that the system 10 automatically identifies the vehicle which is to be used and automatically dispenses the associated key 12, if the person making the request is authorised to use the key 12.

If the person is authorised, the person is instructed to press a particular one of his fingers against the fingerprint reader 52, as shown in Figure 2, and a fingerprint
reading is taken. If the fingerprint reading corresponds to the pre-stored fingerprint reading on the database 56, removal of the requested key is authorised and the key 12 is dispensed by the storage device 16.

It will be appreciated that although both the entry of an identification code and a fingerprint reading is required for the dispensing of a key in this example, only one of these checks, or other requirements, can be used in other embodiments of the invention. Thus, for example, only a fingerprint identification can be required, only an identification code can be required, or the submission of an electronic key, such as a smart card, can be required. Other forms of biometric measurements which can be used include iris recognition, hand palm recognition, or facial recognition.

To dispense the requested key 12, the chain 40 is displaced by the driven pulley 42 until the requested key 12 is in register with one of the access openings 22. It will be appreciated that, upon positioning of each key 12 on its respective bar 46, the tag 50 of each key 12 is read by the tag reader 48, and the position of each key 12 is stored in a memory forming part of the control unit 38. Thus, at any time, the positions of the respective keys 12 on the chain 40 are known, so that the shortest route can be followed to move a requested key 12 into the correct dispensing bay 30.

Once the requested key 12 is positioned in one of the dispensing bays 30, the barrier plate 26 is displaced such that the access opening 22 of the dispensing bay 30 in which the requested key 12 is positioned is unobstructed. The user can then insert his hand into the opened dispensing bay 30 and remove the requested key 12. The shield 32 prevents someone from requesting one key 12 but inserting his hand into the safe 20 through the opened access opening 22 and taking a key 12 other than the one which has been requested.

The tag reader 48 reads the tag 50 of the dispensed key 12, and a date and time stamp is added to a record in the logging database 58. The logging database thus records the date and time of removal of each key 12, as well as recording the identity of the person who removed the key 12.

After the key 12 has been removed, the dispensing bay 30 is automatically
closed by movement of the barrier plate 26 such that the apertures 28 in the plate 26 are out of register with the access openings 22.

The printer 54 automatically prints a pass which serves as evidence that dispensing of the key 12 was authorised. This pass can be used for security purposes at an exit from the compound.

Although not illustrated in this example, the system 10 is in electronic communication with an automated access control system to the compound. Upon dispensing of a particular key 12, the access control system is advised of authorised dispensing of that key 12. When a vehicle is driven out of the compound, a driver of the vehicle is required to submit the tag 50 of the key 12 of that vehicle to a tag reader at an exit station. The vehicle will only be permitted to leave the compound if the read tag 50 is of a key 12 which has been dispensed in an authorised manner from the safe 20.

After the key 12 has been used, it is returned to the safe 20 in a procedure which is effectively the reverse of the authorised dispensing of the key 12. After a user has identified himself by means of a biometric reading and the entry of a PIN, one of the dispensing bays is opened and the key 12 is hung on one of the bars 46. Thereafter, the dispensing bays 30 are closed again.

Details of return of each key 12, i.e. the date and time at which the key 12 is returned, and the person by whom the key 12 is returned, is stored on the logging database 58.

The computer software on the PC 18 has an application for producing detailed reports on the usage of keys 12 dispensed from the safe 20. For instance, a report can be generated in respect of the key usage of a particular person, the use of keys for particular types of vehicle, the use of a key of a particular vehicle, etc.

Although not included in this example, the system 10 can include an alarm arrangement for notifying appropriate persons of unauthorised removal of a key 12 from the safe 20. In one embodiment, the alarm arrangement can be arranged for sending an SMS-notification to a cellular telephone of a responsible person in case of
unauthorised access to the contents of the safe 20.

It is an advantage of the system 10 explained with reference to Figures 1 – 5 that it provides for the secure storage of the keys 12, preventing access by unauthorised persons to the keys 12. However, the keys 12 are individually accessible by authorised persons. An important feature of the system 10 is that it provides for accurate auditing of the dispensing and return of the keys 12, so that it facilitates effective management and control of the keys 12.

The system 10 can also be used for stock-taking purposes, as it can be assumed that all vehicles of which the keys 12 are in the safe 20, are in the compound at that time. As the system 10 is always aware of what keys 12 are in the safe, it can easily be established which vehicles are currently in the compound.

In Figure 6 of the drawings, reference numeral 70 generally indicates a further embodiment of a system for managing the use of a plurality of keys, in accordance with the invention. Like reference numerals indicate like parts in Figures 1-5 and in Figure 6, unless otherwise indicated.

In this example, the system 70 includes two of the secure storage device 16, the devices 16 being connected to a server computer 72 by means of a switch 74. The server 72 is also connected to a plurality of personal computers 76 in a local area network on site, each PC 76 being used by a respective car salesman.

The server computer 72 is in communication with the Internet 78 via a modem 80. This enables a remote computer 82 to access the server computer 72, via the Internet 78.

It is an advantage of the system described with reference to Figure 6 that any salesman can request the dispensing of a particular key 12 from the salesman's own PC 76. The salesman can also remotely establish which vehicles are currently available, by querying the server 72 to establish which keys 12 are currently stored in the storage devices 16. Fingerprint reading will still be required at the respective devices, before the keys 12 are issued.
Furthermore, the system 70 permits remote stock taking through the Internet 78, so that use of the keys 12, and therefore of the vehicles, can be monitored remotely.
CLAIMS

1. A key storage device which includes:
   a secure container having an interior for securely storing a plurality of keys; and
   a dispensing arrangement for dispensing a particular one of the keys upon request, to permit removal of that particular key from the secure container.

2. A device as claimed in claim 1, in which the secure container is a safe-type unit having a lockable theft-resistant door.

3. A device as claimed in claim 1 or claim 2, in which the storage device includes a tag reading means for reading key tags upon dispensing and/or replacement of any key, each tag being attached to a respective key.

4. A device as claimed in claim 3, in which the tag reading means is arranged for reading electronic tags on which are stored respective unique tag codes.

5. A device as claimed in claims 3 or claim 4, in which the tag reading means includes a tag reading device positioned at a dispensing bay where keys are dispensed from the secure container.

6. A device as claimed in claim 5, in which the container has a plurality of dispensing bays and the tag reading means comprises a plurality of tag reading devices associated respectively with the dispensing bays.

7. A device as claimed in any of claims 1 to 6 inclusive, in which the secure container includes a dispensing bay for dispensing requested keys, the dispensing arrangement including a conveyor for conveying a particular key which is to be dispensed to the dispensing bay.

8. A device as claimed in claim 7, in which the dispensing bay has an openably closable access opening for permitting access to a key held in the dispensing bay, the access opening being closed off by a barrier which is displaceable between an open position in which access to the dispensing bay, and hence to a key in the dispensing
bay, is permitted, and a closed position in which access to the dispensing bay is securely barred by the barrier.

9. A device as claimed in claim 8, in which the access opening is a cut-out in a wall of the container adjacent the dispensing bay, and the barrier is a plate which is mounted face-to-face with the wall of the container, the plate being slidably displaceable in a plane in which the plate lies, the plate having an access aperture which can be brought into register with the access opening in the wall of the container to permit access to the interior of the dispensing bay.

10. A device as claimed in claim 9, in which the container has a plurality of dispensing bays, said wall of the container having a corresponding number of cut-outs therein and the barrier plate having a corresponding number of access apertures.

11. A device as claimed in 10, in which the access apertures in the barrier plate and the cut-outs in said wall of the container are arranged such that the dispensing bays can be opened separately by appropriate sliding displacement of the barrier plate.

12. A device as claimed in any of claims 7 to 11 inclusive, in which the conveyor is an endless belt or chain drive to which key-holders are connected at regular intervals, each key-holder being arranged for removably holding at least one of the keys.

13. A device as claimed in claim 12 in which each key-holder is a bar which extends transversely to the belt or chain, so that two separate keys can be secured to opposite ends of each bar.

14. A device as claimed in any one of the preceding claims, which includes a control arrangement for authorising dispensing of particular keys from the secure container in response to requests for dispensing of the keys.

15. A device as claimed in claim 14, in which the storage device includes a biometric identification device for reading a biometric parameter of a person to whom a key is to be dispensed, the biometric identification device being in communication with the control arrangement.
16. A device as claimed in claim 15 in which the control arrangement is configured to dispense a key upon request only if the measured biometric parameter of a person requesting dispensing of a particular key is matched with a pre-stored biometric parameter associated with a person who is authorised to use that particular key.

17. A device as claimed in any one of the preceding claims, which includes a printer mounted on the container for producing a printed document upon issuing and/or returning of a key.

18. A device as claimed in any of the preceding claims, which includes a visual display mounted on the container.

19. A system for managing use of a plurality of keys, which system includes: a key storage device as claimed in any one of claims 1 to 18; and a control means in communication with the secure storage device to control the dispensing of keys from the storage device upon request.

20. A system as claimed in claim 19, in which the control means includes an electronic processor which is in communication with the dispensing arrangement forming part of the secure storage device, the electronic processor being configured for controlling operation of the dispensing arrangement.

21. A system as claimed in claim 20, in which the electronic processor is provided by a computer positioned adjacent the secure storage device, the computer providing a user interface for requesting the dispensing of keys from the device.

22. A system as claimed in claim 19 or claim 20, in which the secure storage device is connected to a network of computers, so that a user can request the dispensing of a particular key at any one of a plurality of computers on the network.

23. A system as claimed in any of claims 19 to 22 inclusive, which includes an information database on which is stored identification data associated with persons who are authorised to remove respective keys from the secure storage device.
24. A system as claimed in claim 23, in which the information database includes data indicative of a personal identification code associated with the respective authorised persons.

25. A system as claimed in claim 23 or claim 24, in which the information database includes data indicative of a biometric parameter associated with the respective authorised persons.

26. A system as claimed in claim 24 or claim 25, which includes a verification arrangement for verifying whether or not dispensing of a particular key to a person requesting dispensing of that key is authorised.

27. A system as claimed in claim 26, in which the verification arrangement is configured for checking whether or not an entered identification code corresponds to a stored identification code on the information database.

28. A system as claimed in claim 26 or claim 27, in which the verification arrangement is configured for reading a biometric parameter of a person requesting dispensing of a particular key, and for verifying whether or not the measured biometric parameter corresponds to a biometric parameter associated in the information database with a person authorised to remove the requested key.

29. A system as claimed in any of claims 19 to 28 inclusive, in which the control means provides a request arrangement for permitting the entry of a request for dispensing of a particular key.

30. A system as claimed in claim 29, in which the request arrangement is configured for requiring the entry of an identification code on an input means connected to the secure storage device, as well as for prompting the entry of an indication of which key is required.

31. A system as claimed in claim 30, in which computer equipment in communication with the storage device is arranged to receive and store information from a tag reading means incorporated in the storage device for reading electronic tags connected to the
respective keys, the computer equipment being configured for generating and storing a record of the time at date at which respective keys were removed from the storage device, the record including the identification code which was entered for dispensing of each key.

32. A system as claimed in any one of claims 19 to 31 inclusive, in which the system is configured for managing the use of keys which are for operating respective vehicles, the system including an interface for connection to an access control system of a compound on which the vehicles are resident, the system being arranged for permitting the exit of a particular one of the vehicles from the compound only if the respective key of the particular vehicle has been dispensed from the secure storage device to an authorised person.

33. A method of managing the use of a plurality of keys, which method includes: securely storing the keys in a secure storage device and automatically dispensing a particular key to an authorised person upon request.

34. A method as claimed in claim 33, which includes the step of verifying whether or not dispensing of a particular key to a person requesting dispensing of that key is authorised.

35. A method as claimed in claim 34, in which the verification step includes requiring the input of an identification code, the key which has been requested being dispensed only if the entered code corresponds with a pre-established identification code associated with the requested key.

36. A method as claimed in claim 34 or claim 35, in which the verification step includes measuring a biometric parameter of a person who is positioned at the secure storage device, and dispensing the key to that person only if the measured biometric parameter corresponds to a pre-authorised biometric parameter.

37. A method as claimed in claim 36, in which measuring a biometric parameter of the person comprises reading a fingerprint of the person and dispensing the requested key only if the fingerprint reading corresponds to a stored fingerprint associated with the
identified person on an information database.

38. A method as claimed in any of claims 33 to 37 inclusive, which includes keeping a record of particulars of the dispensing of keys from the secure storage device and the return of keys to the secure storage device.

39. A method as claimed in claim 38, in which each key is uniquely associated with an electronic tag which is connected to the key, the tag being read by the secure storage device upon dispensing from and return of the respective keys to the secure storage device, to monitor movement of the keys.

40. A method as claimed in claim 38 or claim 39, which includes identifying each person to whom one of the keys is dispensed, and noting and recording the date and time at which each key is dispensed.

41. A method as claimed in any of claims 33 to 40 inclusive, in which the keys are for operating respective vehicles, the method including permitting the exit of any one of the vehicles from a compound on which the vehicles are resident only if the respective key of the particular vehicle has been dispensed from the secure storage device to an authorised person.

42. A method as claimed in claim 41, in which an access control system of the compound requires reading of each tag at an exit from the compound, any vehicle being permitted to exit the compound only if the associated key, as indicated by the tag, has been dispensed from the secure storage device.

43. A device as claimed in claim 1, substantially as herein described and illustrated.

44. A system as claimed in claim 19, substantially as herein described and illustrated.

45. A method as claimed in claim 33, substantially as herein described and illustrated.
INTERNATIONAL SEARCH REPORT

IB2005/051086

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07F7/00 G07F7/06 E05B19/00 G07F11/58

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F E05B G07C

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>FR 2 729 066 A (FITOUSSI DANIEL) 12 July 1996 (1996-07-12) the whole document</td>
<td>1-45</td>
</tr>
<tr>
<td>X</td>
<td>WO 92/0127 A (COMPUTER DETECTION SYSTEMS PTY. LTD) 23 January 1992 (1992-01-23) abstract page 1, paragraph 1-3 page 6, paragraph 2 - page 8, paragraph 4 page 10, paragraph 4 - page 11, paragraph 2 page 15, paragraph 3 figures</td>
<td>1-45</td>
</tr>
</tbody>
</table>

Further special categories of cited documents:

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

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

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

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

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

Date of the actual completion of the international search

13 May 2005

Date of mailing of the international search report

24/05/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5815 Patentlaan 2 NL - 2280 HV Rijswijk
Tel: (+31-70) 940-2040, Tx: 31 651 epos nl, Fax: (+31-70) 340-3016

Authorized officer

Breugelmans, J

Form PCT/ISA/210 (second sheet) (January 2004)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>
| X        | US 2002/130180 A1 (STOBBE ANATOLI)  
19 September 2002 (2002-09-19)  
abstract  
paragraphs '0002!', '0042! - '0047!  
figures | 1-45 |
| X        | SCHAFFER B: "MORSE WATCHMAN: KEYWATCHER"  
LOCKSMITH LEDGER INTERNATIONAL, LOCKSMITH  
PUB. CORP., PARK BRIDGE, IL, US,  
vol. 56, no. 4, 1 March 1996 (1996-03-01),  
pages 62-65, XP0000585286  
ISSN: 1050-2254  
the whole document | 1-45 |
| A        | US 6 195 005 B1 (MALONEY WILLIAM C)  
27 February 2001 (2001-02-27)  
abstract  
figures | 1-45 |
| A        | US 6 505 754 B1 (KENNY THOMAS A ET AL)  
14 January 2003 (2003-01-14)  
abstract  
column 1, lines 6-9  
column 1, line 56 - column 2, line 45  
figures | 1-45 |
| A        | US 5 172 829 A (DELLICKER, JR. ET AL)  
22 December 1992 (1992-12-22)  
abstract  
figures | 1-45 |
| A        | EP 0 291 614 A (KEY-MATIC INDUSTRIES INC)  
abstract  
figures | 1-45 |
| A        | US 4 812 985 A (HAMBRECK ET AL)  
14 March 1989 (1989-03-14)  
abstract  
figures | 1-45 |
| A        | EP 1 223 566 A (JOFEMAR, S.A)  
17 July 2002 (2002-07-17)  
abstract  
figures | 1-45 |
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>WO 9201273 A1</td>
<td>23-01-1992</td>
</tr>
<tr>
<td>US 2002130180</td>
<td>19-09-2002</td>
<td>DE 10113072 A1</td>
<td>02-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1241635 A2</td>
<td>18-09-2002</td>
</tr>
<tr>
<td>US 6195005</td>
<td>27-02-2001</td>
<td>AU 5916899 A</td>
<td>03-04-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2343411 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002044055 A1</td>
<td>18-04-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0016282 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003184437 A1</td>
<td>02-10-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004113785 A1</td>
<td>17-06-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2001009397 A1</td>
<td>26-07-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5916799 A</td>
<td>03-04-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5924599 A</td>
<td>03-04-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 6031499 A</td>
<td>03-04-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 6032699 A</td>
<td>03-04-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2343404 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2343412 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1121812 A1</td>
<td>08-08-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002075154 A1</td>
<td>20-06-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0016564 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0016280 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0016281 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0016284 A1</td>
<td>23-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002145520 A1</td>
<td>10-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002153418 A1</td>
<td>24-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003052782 A1</td>
<td>20-03-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6232876 B1</td>
<td>15-05-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6427913 B1</td>
<td>06-08-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6262664 B1</td>
<td>17-07-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6204764 B1</td>
<td>20-03-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003201321 A1</td>
<td>30-10-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004021670 A1</td>
<td>05-02-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004095241 A1</td>
<td>20-05-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2001004235 A1</td>
<td>21-06-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004172554 A1</td>
<td>02-09-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 200106368 A1</td>
<td>05-07-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2001022552 A1</td>
<td>20-09-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2005040232 A1</td>
<td>24-02-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002014961 A1</td>
<td>07-02-2002</td>
</tr>
<tr>
<td>US 6505754</td>
<td>14-01-2003</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>US 5172829</td>
<td>22-12-1992</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AT 48171 T</td>
<td>15-12-1989</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 3761027 D1</td>
<td>28-12-1989</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 4681504 A</td>
<td>21-07-1987</td>
</tr>
<tr>
<td>US 4812985</td>
<td>14-03-1989</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>

Form PCT/ISA/210 (patent family annex) (January 2004)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP 1223566 A</td>
<td></td>
<td>BR 0010278 A</td>
<td>23-04-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2362823 A1</td>
<td>07-09-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002125266 A1</td>
<td>12-09-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0165504 A1</td>
<td>07-09-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZA 200106599 A</td>
<td>12-08-2002</td>
</tr>
</tbody>
</table>