159159

WEB ENABLED KEY MANAGEMENT SYSTEM

DESCRIPTION

Technical Field

1. The invention relates to a key management security system, and in particular, a device to monitor and manage keys using security hardware and computer software.

Background Art

2. Pursuant to conventional key management systems, keys are usually kept in a manual key press and monitored by way of manual logs being kept on the retrieving and the return of keys.

3. Pursuant to the manual key press system, when a user wishes to retrieve a key, he would complete a manual written log, which includes the date and time the key is retrieved together with a description of the key he intends to retrieve and the identity of the person retrieving the key. Thereafter, using the key press master key, he will open the locked key press and retrieve the key that he had indicated in the log that he was retrieving.

4. When the user wishes to return the key, he would use the key press master key and open the locked key press and return the key that he had retrieved in the position where the key is indicated to have been located. The user would then record in the log the date and time the key was returned.

5. The problems with the conventional key management systems would include the following:

    a. inaccuracy in the date and time for the retrieval and the return of keys;

    b. possibility of persons retrieving keys without proper authorisation and record;

    c. problems with the monitoring of the location of keys.

G00002

Disclosure of the Invention

6. The present invention is directed to ensuring the keys retrieved and returned to a key press is properly managed and monitored. This substantially obviates one or more of the problems due to limitations and disadvantages in the conventional key management system.

7. An object of the present invention is to provide proper logging of the date and time that keys are retrieved and replaced in the key press.

8. Another object of the present invention is to ensure that only authorised persons who may retrieve the associated authorised keys are able to do so.

9. Another object of the present invention is to allow the users to monitor the retrieval and the replacement of the keys to the key press, the persons retrieving and replacing the keys and the frequency of the retrieval and replacement.

10. Further object of the present invention is that the same allows appointed persons to be notified of any unauthorised retrievals or attempts for the retrieval of keys from the key press using internet based technology, smart messaging technology, global messaging technology.

11. Additional features and advantages of the present invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the present invention will be realised and attained by the structure particularly pointed out in the written description and claims thereof as well as the appended drawings.

12. According to the features of the invention, the user is able to specify:

    a. the persons who may have access to the keys held by the invention;

    b. the keys the person has access to; and

    c. the time and dates the keys the person has access to.

13. Further, the user is able to monitor through internet based systems:

a. the dates and times each individual key was retrieved from the invention;

b. the person who retrieved or returned each individual key; and

c. the frequency of the retrieval of each key.

14. Further, the invention allows the user to be informed via internet systems, smart messaging systems and global messaging systems, if an attempt has been made to remove keys which a particular person is not authorised to remove and any attempt to force open the invention in order to reach the keys held by the invention.

Brief Description of Drawings

15. The accompanying drawings, which are included to provide a further understanding of the present invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention. Figure 1 is a schematic front view of the cabinet unit of the Web Enabled Key Management System.

Carrying Out the Invention

16. Hereinafter, the present invention will be described in detail with reference to the accompanying drawings.

17. The embodiments and the drawings of the present invention have been described and illustrated in order only to easily explain the present invention, which could not limit the scope of the present invention.

18. Therefore, it will be apparent to those skilled in the art that various modifications and variations can be made therein without departing from the spirit and scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention that come within the scope of the appended claims and their equivalent.

19. The cabinet unit (the 'Cabinet Unit') (see Figure 1) is made of about 1.5 mm steel plate with the front door embedded with a tampered proof glass window. The front door is fitted with a door contact sensor and a back door tamper switch to aid in the

security in the event that an attempt to force open the front door is made. A master key is provided in the event that an emergency release of the keys is required.

20. The Cabinet Unit includes a key storage unit (the 'Key Storage Unit') and a controller housing unit (the 'Controller Housing Unit') (see Figure 1).

21. The Key Storage Unit is constructed and may hold up to 128 individual key rings, which are tampered for security reasons. Individual key rings are attached to a key distribution controller, which would include a Flash-based 8-bit CMOS Microcontroller with a Solenoid, Infra Red Position Sensor and LED State indicator.

22. The Controller Housing Unit includes the Main Controller Unit, the LCD Display and Keypad panel, the Key Distribution Interface and the Power Supply Unit with Battery Charger.

23. The Main Controller Unit would include a microprocessor with a specification of 29.4 MHz and 512K Flash and/or RAM. The Main Controller Unit would further include a 16M Serial Flash Memory Card, a serial communication port and battery backup.

24. The LCD Display and Keypad panel shall be attached to the Main Controller Unit of which the same shall include a Central Processing Unit enhanced with a Flash Microcontroller, communication ports, a 24 character LCD Display, numerical keypad with 10 numerical keys and 4 function keys, a buzzer alarm with LED indicators.

25. The Key Distribution Interface shall be attached to the LCD Display and Keypad panel and the Main Controller Unit. The Key Distribution Interface shall include a Central Processing Unit enhanced with a Flash Microcontroller, communication ports, an address decoder and a key state collector.

26. The Power Supply Unit would include a supply of at least 12V DC. A rechargeable 12V battery shall be included in the Power Supply Unit with systems to detect a power down, to ensure that the battery takes over in the event of a power down, to ensure that the battery is recharged and continuously readily available in the event of a power down.

27. Further, the Cabinet Unit may be installed with a picture recorder, various card readers or a modem so as to enhance the security in the management and monitoring of keys.

28. The Main Controller Unit is configured and controlled by way of embedded software, the software application of which may be readily accessible by the internet or through the Keypad panel. The software application provides for the following:

    a. allows the user to change the time on the system, create new user profiles and user pin passwords, edit the particulars of existing user profiles and to change existing pin passwords;

    b. allows the user to change the timing and schedule and the persons authorised to access the individual keys;

    c. to monitor the retrieval and replacement of keys; and

    d. to check the log records for the retrieval and replacement of keys.

WEB ENABLED KEY MANAGEMENT SYSTEM

CLAIMS

1. A web enabled key management system to ensure the security of keys by restricting the persons authorised to access individual keys and to control the time and schedule persons are able to access individual keys.

2. A web enabled key management system to allow the monitoring of the use and access of keys and the tracking of the movement of keys by way of internet based systems.

3. The web enabled key management system according to claim 1, wherein individual keys are secured under individual key rings, the access to the individual key rings of which are controlled by a Main Controller Unit which is controlled by the user through web based interface systems.

4. The web enabled key management system according to claim 2, wherein the release of the keys from the individual key rings are logged by the Main Controller Unit and published through web based interface systems to the user.