

Description

Title Of Invention: LOCK POSITION AUTHENTICATING BATTERY CONTAINER AND METHOD

Technical Field

[0001] The present invention relates generally to a battery container, more particularly, a battery container that is capable of, and a method for, authenticating that a cover of the battery container is at a lock position.

Background

[0002] In standard process of electrical vehicle battery swap in a swap station, potential asset losses can occur during practical use as users may maliciously press a pressure-based sensor using a small rod to deceive the device to mistakenly determine that the cover or door of the battery container is closed and locked well, and then take out the inserted battery at any time they want.

[0003] Currently, some of the swap station service provider provides functions to check the state of the sensor twice to double confirm the lock state of the door. However, this could still prevent some check pass from accident and the malicious users can still get through the multiple checks by some way, for example by adhibiting the sensor with a tape.

[0004] There is thus a need for a new lock position authenticating battery container and method that is able to authenticate that the door/cover is what triggers the sensor and forbid a malicious user from interfering with the sensor and deceiving the door locking check.

[0005] Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

Summary

[0006] In a first aspect, the present disclosure provides a battery container comprising: a body with an opening through which a battery can be inserted and extracted, the body comprising a lock and first circuitry, wherein the first circuitry is configured to generate a request signal

based upon a receipt of a signal from a lock sensor indicating a lock pin is secured to the lock; and a cover comprising a lock pin and second circuitry, wherein the second circuitry is configured to generate a response signal based upon a receipt of the request signal; wherein the cover is movable onto a lip portion of the body adjacent to the opening into a lock position to close the opening and secure the lock pin to the lock, and the first circuitry is further configured to process the response signal and switch a status of the lock from an unlock state to a lock state based on a result of the processing of the response signal.

[0007] In a second aspect, the present disclosure provides a method for authenticating that a cover of a battery container is at a lock position, comprising: receiving a signal from a lock sensor indicating a lock pin of the cover of the battery container is secured to a lock of a body of the battery container; generating, by a first circuitry of the body, a request signal; generating, by a second circuitry of the cover, a response signal; processing, by the first circuitry, the response signal; and switching a status of the lock from an unlock state to a lock state based on a result of the processing of the response signal.

[0008] Additional benefits and advantages of the disclosed embodiments will become apparent from the specification and drawings. The benefits and/or advantages may be individually obtained by the various embodiments and features of the specification and drawings, which need not all be provided in order to obtain one or more of such benefits and/or advantages.

Brief Description of the Drawings

[0009] Embodiments and implementations are provided by way of example only, and will be better understood and readily apparent to one of ordinary skill in the art from the following written description, read in conjunction with the drawings, in which:

[0010] Figure 1 shows a flowchart illustrating a method implemented by a system comprised in a battery container for authenticating that a cover of the battery container is at a lock position according to an embodiment of the present disclosure.

[0011] Figure 2 shows a flowchart showing an operation flow carried out in a cover and a body of a battery container, respectively, according to an embodiment of the present disclosure.

[0012] Figure 3 shows a front view a battery container according to an embodiment of the present disclosure.

[0013] Figure 4 shows side view of a battery container according to an embodiment of the present disclosure.

[0014] Figure 5a shows a plan view an IC unit comprised in a cover of a battery container according to an embodiment of the present disclosure.

[0015] Figure 5b shows a side view of an IC unit comprised in a cover of a battery container according to an embodiment of the present disclosure.

[0016] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

Detailed Description

[0017] The following detailed description is merely exemplary in nature and is not intended to limit the invention or the application and uses of the invention. Furthermore, there is no intention to be bound by any theory presented in the preceding background of the invention or the following detailed description. It is the intent of this invention to present a lock position authenticating battery container and method.

[0018] Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

[0019] It is to be noted that the discussions contained in the "Background" section and that above relating to prior art arrangements relate to discussions of devices which form public knowledge through their use. Such should not be interpreted as a representation by the present inventor(s) or the patent applicant that such devices in any way form part of the common general knowledge in the art.

[0020] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the

substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0021] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “calculating”, “determining”, “updating”, “generating”, “initializing”, “outputting”, “receiving”, “retrieving”, “identifying”, “dispensing”, “authenticating” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0022] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0023] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[0024] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with

a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0025] In a standard process of electrical vehicle battery swap in an unmanned swap station, the following steps are executed:

1. Open a door (or cover) of an empty battery container on the station;
2. Insert the battery they hold into the container;
3. Close and lock the door of the container;
4. Validate the battery which is inserted;
5. Open a door of a battery container on station which contains an available;
6. Take out the available battery; and
7. Close and lock the door of the second container.

[0026] As mentioned above, the above steps could face a potential asset (battery) loss during practical use. A malicious user can interfere with a door sensor, e.g., a pressure-based sensor, which is used on step 3 to detect whether the door/cover is closed, by pressing it or trigger with a small rod to deceive the sensor mistakenly determining that the door is closed and locked well. Then, after all steps, the user can take out the inserted battery at any time they want and lead to the battery loss.

[0027] Conventionally, functions such as double checking the state of the sensor to determine the lock state of the door are used. However, there are still ways to get through those multi-time check by some way such as adhibit the sensor with a tape.

[0028] According to the present disclosure, an organically integrated system is introduced, comprising position checking, authentication and anti-disassembly, to ensure locking check of the cover (or door) of the battery container will pass if and only if the cover is closed onto the body of the batter container properly, or in other words, only if the lock pin on the cover is secured to the lock in the body of the container. An authentication mechanism is introduced by using an integrated circuit (IC) on the cover working in connection with a controller on the body. Through the interactions between the IC and the controller as well as related operation flow, it is able to authenticate whether the cover is at a lock position triggering the lock sensor. Further related protectional designs on the battery container to prevent this authentication mechanism from bypassing are also provided in embodiments below.

[0029] Figure 1 shows a flowchart 100 illustrating a method implemented by a system comprised in a battery container for authenticating that a cover of the battery container is at a lock position according to an embodiment of the present disclosure. In step 102, a step of receiving a signal from a lock sensor indicating a lock pin of a cover of a battery container is secured to a lock of a body of the battery container. In step 104, a step of generating a request signal is carried out by a first circuitry (e.g., controller) of the body. In step 106, a step of generating a response signal is carried out by a second circuitry (e.g., integrated circuit) of the cover. In step 108, a step of processing the response signal received in step 106 is further carried out by the first circuitry of the body. In step 108, a step of switching a status of the lock from an unlock state to a lock state is carried out based on a result of the processing of the response signal.

[0030] Figure 2 shows a flowchart 200 showing an operation flow carried out in a cover (herein referred to as container door 202) and a body (herein referred to as container body 222) of a battery container, respectively, according to an embodiment of the present disclosure. According to the embodiment, the container door 202 comprises a lock pin 204, an integrated circuitry (IC) chip 206 and an IC Antenna 208 whereas the container body 222 comprises a lock 224, a lock sensor 226, a controller 228 and a controller antenna 230. Each of the IC antenna 208 and controller antenna 230 can function as a transceiver (or comprises a receiver and a transmitter separately) to receive a signal from and transmit a signal to the other antenna. The operation flow can be divided to 11 chronological operation steps, as follows:

1. A lock pin 204 on the container door 202 is physically secured to a lock 224 on the container body 222;
2. A lock sensor 226 detects the lock pin 204 is secured to the lock 224 and is triggered upon detection of the lock pin 204;
3. The trigger lock sensor 226 signals a controller 228 to initiate the authentication process;
4. The controller 228 generates a request signal comprising a digitally signed one time authentication request and sends the signal to a controller antenna 230;
5. The controller antenna 230 transmits the request signal wirelessly via near-field communication to the container door 202;
6. An IC antenna 208 of the container door receives the request signal and sends the authentication request to an IC chip 206 in the container door 202;
7. The IC chip 206 processes the authentication request with pre-integrated logic and an authentication key;
8. The IC chip 206 generates a response signal comprising a digitally signed authentication response and sends to the IC antenna 208;

9. The IC antenna 208 transmits the response signal wirelessly via near-field communication to the container body 222'
10. The controller 228 antenna 230 receives the response signal and sends the authentication response to the controller 228; and
11. The controller 228 processes the authentication response and evaluates it with an expected result to identify if the container door is closed and switch the lock status from the unlock state to the lock state based on a result of the evaluation/processing.

[0031] Figures 3 and 4 show a front view and a side view of a battery container according to an embodiment of the present disclosure. The battery container comprises a container body and a container door (cover). The container body has an opening configured to through which a battery can be inserted and extracted and comprises a lock on a lip portion adjacent to the opening. The lip portion is illustrated as the top, right and bottom side of the container body. The lock is configured to receive a lock pin, and in this embodiment, it is located at the right side of the container body. The container body further comprises circuitry (controller), a lock sensor and a transceiver (controller antenna). The controller connects to the lock sensor and the controller antenna through wires, and is located behind (or at the bottom surface opposite the opening of) the container. A skilled person would appreciate that the controller can be located at any other surface of the container or inside the container inaccessible by the user of the battery container.

[0032] The container door comprises a lock pin attached to a rear surface of the container door and extended out from the rear surface and an IC unit. The IC unit is a contained hardware component with an IC chip and an IC antenna. The container door is movable onto the lip portion of the container body. The location of the lock pin on rear surface of the container door matches to the location of the lock on the lip portion of the container body such that when the container door is moved onto the lip portion of the container body and cause the rear surface of the container door and the lip portion of the container body to come towards each other, the lock pin is moved together with the container door, and at the end of the movement, the lock pin is inserted into the lock and is able to be secured to the lock, and the container door sits on the lip portion of the container body, closes the opening and encloses the battery container. Such position between the container door and the container body when the lock pin is secured to the lock and the container door closes the opening to enclose the battery container is referred to as "lock position" in various embodiments of the present disclosure.

[0033] In one example, the IC unit is physically located within the container door such that the IC unit is not visible to a user. In another embodiment, the IC antenna is in electrical

communication with the IC unit and located within the container door such that the IC antenna is also not visible to the user. Preferably, the container door is constructed such that the IC unit and the IC antenna are hidden within the container door such that a user is not able to obtain physical access to the IC unit and the IC antenna. The controller antenna is located within the side wall of the container body such that it is not visible to a user or physically accessible to a user. The IC antenna and controller antenna should touch each other or be close enough with each other when the door is well closed at the lock position in order to ensure communication distance can be set less enough to prevent IC unit from receiving signals from the controller antenna if the door is not at the lock position (not closed). In other words, the IC antenna is located within a signal range of the controller antenna to receive/transmit any signal from/to the controller antenna only when the cover is at the lock position.

[0034] In one embodiment, the IC unit is located at a side of the door where it will be the last contact with the container body when the door is closed at the lock position. For example, if the door is closed from the left side to the right side, and the door covers the right side of the container body last, the IC unit should be put at the right side of the door as shown in Figure 3.

[0035] If the door is locked appropriately at the lock position, that is, the lock pin is secured to the lock and the container door closes the opening to enclose the battery container, the lock sensor in the container body sends a signal to the controller to initiate the authentication process. Due to the distance between IC Antenna and Controller Antenna being close enough to be within a signal range with each other, the authentication request will be sent to the IC Unit by NFC and excite the IC Chip to process the corresponding authentication response. After the received authentication response is sent back to the container body and confirmed by the controller. The door can be considered as successfully locked and the controller is then configured to switch the lock status of the battery container from an unlock state to a lock state.

[0036] The lock sensor can be integrated within the container body or external to the battery container connecting to the lock or lock pin through a wire or wirelessly. In this embodiment, the lock sensor is located within the container body and is configured to be triggered to send a signal to the controller when the lock pin is physically inserted into the lock.

[0037] If someone triggers the lock sensor by another object rather than the lock pin. The lock sensor may send a signal to the controller to initiate the authentication process. However, because the object will block lock pin (and the cover) to lock at the lock position, there will be cause a gap between antenna units to block the NFC. The IC antenna cannot receive the request signal transmitted by the controller antenna and/or the controller antenna cannot receive the response signal transmitted by the IC antenna. As a result, the controller cannot get the expected authentication response, and does not switch the lock status. The door can be considered as failing to lock.

[0038] In one embodiment, the digitally signed request signal generated by the controller comprises a controller identifier which can be used to identify and verify the source of the signal (i.e., the controller) by the circuitry receiving and processing the signal (i.e., the IC chip). Similarly, the digitally signed response signal generated by the IC chip also comprises an IC chip identifier which can be used to identify and verify the source of the signal (i.e., IC chip) by the circuitry receiving and processing the signal (i.e., the controller). This is to ensure that a malicious user will not be able to a signal source other than the respective intended circuitries located at the container body and the container door to complete the authentication process.

[0039] In another embodiment, the IC chip process the response signal by retrieving an authentication key stored in a memory or database (not shown) in connection with the IC chip and use the authentication key (alone or in combination with the pre-configured logic) to generate the response signal from the request signal. The authentication key can be an analogy signal or a digital signal such as binary sequence. On the other hand, the controller also generates an expected response signal (or expected authentication response) by retrieving a related authentication key stored in a memory or databased (not shown) in connect with the controller and use the related authentication key to generate the expected response signal. The controller then evaluates the response signal received from the IC chip by comparing it against the expected response signal on its side. If the response signal matches the expected result, the controller then determines that the door is successfully lock at the lock position and switch the lock status from the unlock state to the lock state.

[0040] In yet another embodiment, the request signal generated by the controller to initiate the authentication process and sent to the IC chip to process is a single-use one-time request signal generated in response to the most recent signal received from the lock sensor, the single-use request signal being different from one or all previous request signals generated by the controller for the authentication process. For example, if a digital signal is used, the

single-use one time request signal can be a random fixed length binary stream. This is to ensure that the IC chip generates the response signal comprising the authenticate response based on that single-use signal that is unique and specific to the most recent lock from the lock pin. This again is to ensure that the authentication process is unique every time when it is based on a single-use signal and a malicious user is not able to deceive the controller or the IC chip using a previously used signal to complete the authentication process. In other words, if a device is used to impersonate the IC Unit by replaying an authentication response. Because the IC Chip has an encrypted signature, and the control side sends a one-time verification request, the replay history response is invalid. The door can be considered as failing to lock.

[0041] In one implementation, if a device is used to impersonate the IC Unit by copying the IC data. It prevents copying the encrypted area data, and the IC Unit only returns the processed data rather than the original data on the IC Unit which participated in the calculation.

[0042] In an additional implementation, beside the signal from the lock sensor, the authentication process may be triggered when the controller receives another signal from a battery sensor (not shown in any figure) indicating that a battery is present in the container body. If, for example, the battery sensor detects that the container body does or does not contain a battery, a signal is generated and sent to the controller, and the controller will initiate the authentication process and generate the request signal further based on such signal received from the battery sensor on top of the signal from the lock sensor.

[0043] Figures 5a and 5b show a plan view 500 and a side view 520 of an IC unit located within a container door (cover) of a battery container according to an embodiment of the present disclosure, respectively. In this embodiment, the container door (cover) is a shell enclosing the IC unit.

[0044] In this embodiment, the IC unit is attached to the container door through a junction on chip unit and located within the container door, hence the IC unit is separated by the rear surface 505 of the container door from the container body when the container door is at the lock position). The IC unit comprises an antenna unit acting as a transceiver and a chip unit acting as circuitry which works together with a controller and a transceiver at the container body to provide functions to authenticate the container door is at the lock position triggering the lock sensor, covering the opening of the container body and enclosing the battery container. The antenna unit comprises an antenna circle (IC antenna), a wire(s), contacts and

a shell enclosing the antenna circle, wire(s) and contacts. The chip unit comprises an IC chip, contacts and a shell enclosing the IC chip and the contacts. The contacts of the antenna unit and the chip unit are electrically connected to each other such that electrical signals can be transmitted between the antenna circle and the IC chip through the wire and the contacts.

[0045] In one embodiment, the wire comprises a wire structure which acts as a weak point. The weak point is designed such that when a pulling force is applied to the wire (e.g., by exerting pressure to the container door shell or the antenna unit shell), causing the length of the wire extended beyond a threshold length, the weak point will break and cause the electrical connection between the antenna circle and the IC chip to break or that the antenna circle and the IC chip become very hard to connect back with each other unless the container door shell is removed to reconnect the wire. In other words, if a malicious user tries to bring the antenna circle out from the antenna unit shell or from the container door shell by force and extend the wire beyond the threshold length when the container door is opened, for example, to put the antenna circles of the container door and the container body within their radio ranges and deceive the system that the container door is at the lock position to switch the lock status from unlock status to lock status maliciously, the wire structure of the wire will break, causing the chip unit to be disconnected from the antenna unit and disallowing any switching of the lock status.

[0046] Similarly, if someone wants to extend the IC unit, they need to expose the wire in the antenna unit, and due to the wire structure, this will break the antenna unit into two parts from the weak point and let the broken wire hide in the door and the IC unit to disconnect from the antenna unit. Unless the door shell is removed, the wire is hard to connect back again.

[0047] In one configuration, the shell of the container door is made out of a signal shielding material that is capable of blocking the near-field communication signal. In such configuration, the rear surface 505 of the container door separating the IC unit from the container body has a window or opening which exposes the antenna circle to the counterpart antenna at the container body while the rear surface 505 blocks any signal from transmitting through the signal shielding material directly from/to the chip unit located within the container door shell. This is to ensure that the signal can only be transmitted to and received from the counterpart antenna at the container body and the antenna circle at that window.

[0048] The foregoing describes only some embodiments of the present disclosure, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

CLAIMS

1. A battery container comprising:

a body with an opening through which a battery can be inserted and extracted, the body comprising a lock and first circuitry, wherein the first circuitry is configured to generate a request signal based upon a receipt of a signal from a lock sensor indicating a lock pin is secured to the lock; and

a cover comprising a lock pin and second circuitry, wherein the second circuitry is configured to generate a response signal based upon a receipt of the request signal;

wherein the cover is movable onto a lip portion of the body adjacent to the opening into a lock position to close the opening and secure the lock pin to the lock, and the first circuitry is further configured to process the response signal and switch a status of the lock from an unlock state to a lock state based on a result of the processing of the response signal.

2. The battery container of claim 1, wherein each of the body and the cover further comprises a transceiver which transmits/receives the request signal and the response signal.

3. The battery container of claim 2, wherein the transceiver of the cover is within a signal range of the transceiver of the body for the transceivers to receive the request signal and the response signal only when the cover is at the lock position.

4. The battery container of claim 3, wherein the transceiver of the body is located at a part of the lip portion of the body; and the second circuitry and the transceiver of the cover are located within the cover and movable together with the cover; and wherein moving the cover into the lock position causes the transceiver of the cover to move into the signal range of the transceiver of the body.

5. The battery container of 4, wherein the cover comprises a rear surface, wherein the rear surface is moved onto the remaining part of the lip portion of the body at the lock

position and comprises a signal shielding material that blocks the request signal or the response signal from transmitting through the rear surface of the cover, and wherein the rear surface further comprises a window exposing the transceiver of the cover to the transceiver of the body located at the part of the lip portion of the body and allowing the transceiver of the cover to receive the request signal from or transmit the response signal to the transceiver of the body.

6. The battery container of any one of claims 1-5, wherein the request signal comprises a first identifier identifying the first circuitry; and the second circuitry is further configured to verify that the request signal comprises the first identifier and generate the response signal further based on a result of the verification of the request signal.

7. The battery container of any one of claims 1-6, wherein the response signal comprises a second identifier identifying the second circuitry; and the first circuitry is further configured to verify that the response signal comprises the second identifier; and switch the status of the lock based on a result of the verification of the response signal.

8. The battery container of any one of claims 1-7, wherein the request signal comprises a single-use request signal and the second circuitry is configured to generate the response signal based on the single-use request signal.

9. The battery container of any one of claims 1-8, wherein the first circuitry is configured to generate an expected response signal and compare the response signal against the expected signal to process the response signal; and switch the status of the lock based on a result of the comparison.

10. The battery container of claim 9, wherein the second circuitry is configured to retrieve an authentication key stored in a second memory in connection with the second circuitry and use the authentication key retrieved from the second memory to generate the response signal from the request signal; and the first circuitry is configured to retrieve a related authentication key corresponding to the second circuitry stored in a first memory in

connection with the first circuitry and use the related authentication key retrieved from the first memory to generate the expected response signal from the request signal.

11. The battery container of any one of claims 1-10, wherein the cover further comprises a wire connecting the second circuitry and transceiver of the cover, the wire comprising a wire structure designed to disconnect the second circuitry and transceiver when a length of the wire is extended beyond a threshold length.

12. The battery container of any one of claims 1-11, wherein the first circuitry is configured to generate the request signal further based upon a receipt of another signal indicating a presence of a battery in the body.

13. A method for authenticating that a cover of a battery container is at a lock position, comprising:

receiving a signal from a lock sensor indicating a lock pin of the cover of the battery container is secured to a lock of a body of the battery container;

generating, by a first circuitry of the body, a request signal;

generating, by a second circuitry of the cover, a response signal;

processing, by the first circuitry, the response signal; and

switching a status of the lock from an unlock state to a lock state based on a result of the processing of the response signal.

14. The method of claim 13, further comprising:

transmitting, by a first transceiver of the body, the request signal generated by the first circuitry to the cover;

receiving, by a second transceiver of the cover, the request signal;

transmitting, by the second transceiver, the response signal generated by the second circuitry to the body; and

receiving, by the first transceiver, the response signal.

15. The method of claim 13 or 14, further comprising:

verifying, by the second circuitry, that the request signal comprises a first identifier identifying the first circuitry; wherein the generation of the response signal is further based on a result of the verification of the request signal.

16. The method of any one of claims 13-15, wherein the processing of the response signal comprises:

verifying that the response signal comprises a second identifier identifying the second circuitry, and the switching of the status of the lock is based on a result of the verification of the response signal.

17. The method of any one of claims 13-16, wherein the request signal comprises a single-use request signal, and the generation of the response signal is based on the single-use request signal.

18. The method of any one of claims 13-17, wherein the processing of the response signal comprises:

generating an expected response signal,

comparing the response signal against the expected signal, wherein the switching of the status of the lock is based on a result of the comparison.

19. The method of claim 18, wherein the generation of the response signal comprises:

retrieving an authentication key stored in a second memory in connection with the second circuitry; and

generating the response signal from the request signal using the authentication key retrieved from the second memory; and

wherein the generation of the expected response signal comprises:

retrieving a related authentication key corresponding to the second circuitry stored in a first memory in connection with the first circuitry; and

generating the expected response signal from the request signal using the related authentication key retrieved from the first memory.

20. The method of any one of claims 13-16, further comprising:

receiving another signal from a battery sensory indicating a presence of a battery in the body; and the generation of the request signal is further based upon the receipt of the other signal.