US 20120096909A1

(19) United States
(12) Patent Application Publication
(10) Pub. No.: US 2012/0096909 A1
(43) Pub. Date: Apr. 26, 2012
Hart et al.

(54) ELECTRONIC LOCKING SYSTEM AND METHOD

(76) Inventors: **Jason Hart**, Fremont, CA (US); **Matthew Herscovitch**, Fremont, CA (US); **Sotoudeh Hamedi Hagh**, Fremont, CA (US)

(21) Appl. No.: **13/318,526**

(22) PCT Filed: **May 3, 2010**

(86) PCT No.: **PCT/AU10/00508**

§ 371 (c)(1), (2), (4) Date: **Jan. 13, 2012**

(30) **Foreign Application Priority Data**

May 4, 2009 (AU) 2009201756

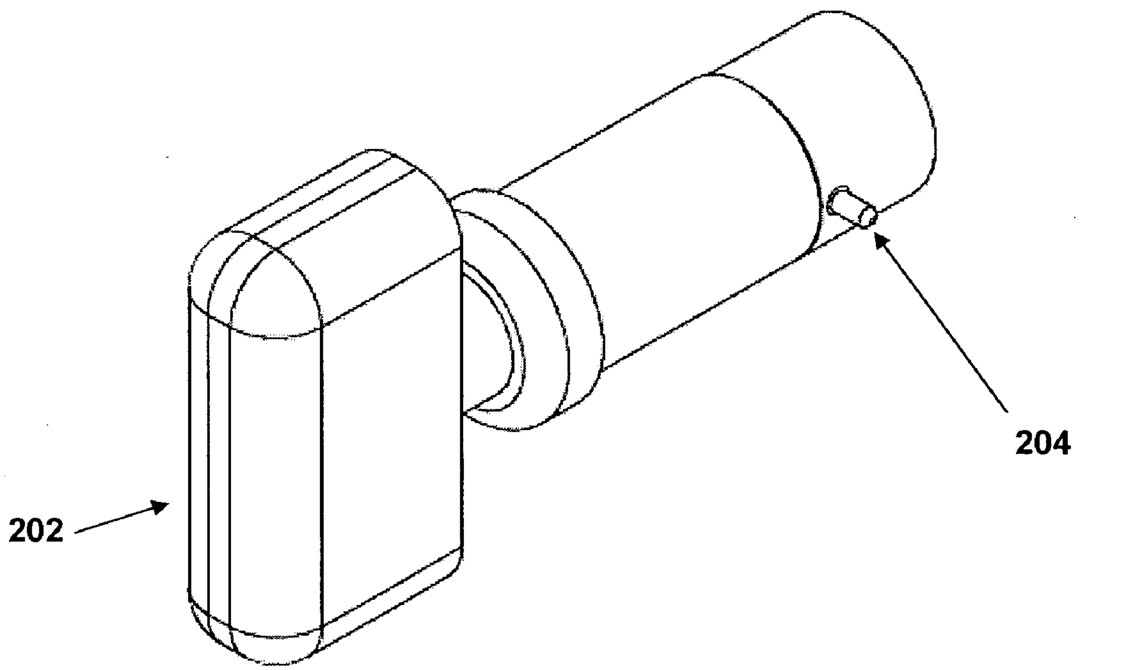
Publication Classification

(51) **Int. Cl.**
E05B 49/02 (2006.01)
G08B 29/00 (2006.01)
E05B 47/00 (2006.01)

(52) **U.S. Cl.** **70/278.1**; 70/280; 340/5.6

(57) **ABSTRACT**

The present invention provides an electronic locking system and method that includes a lock with a locking member and at least one antenna. A remote power source remotely powers the lock to actuate the locking member, using induction technology.



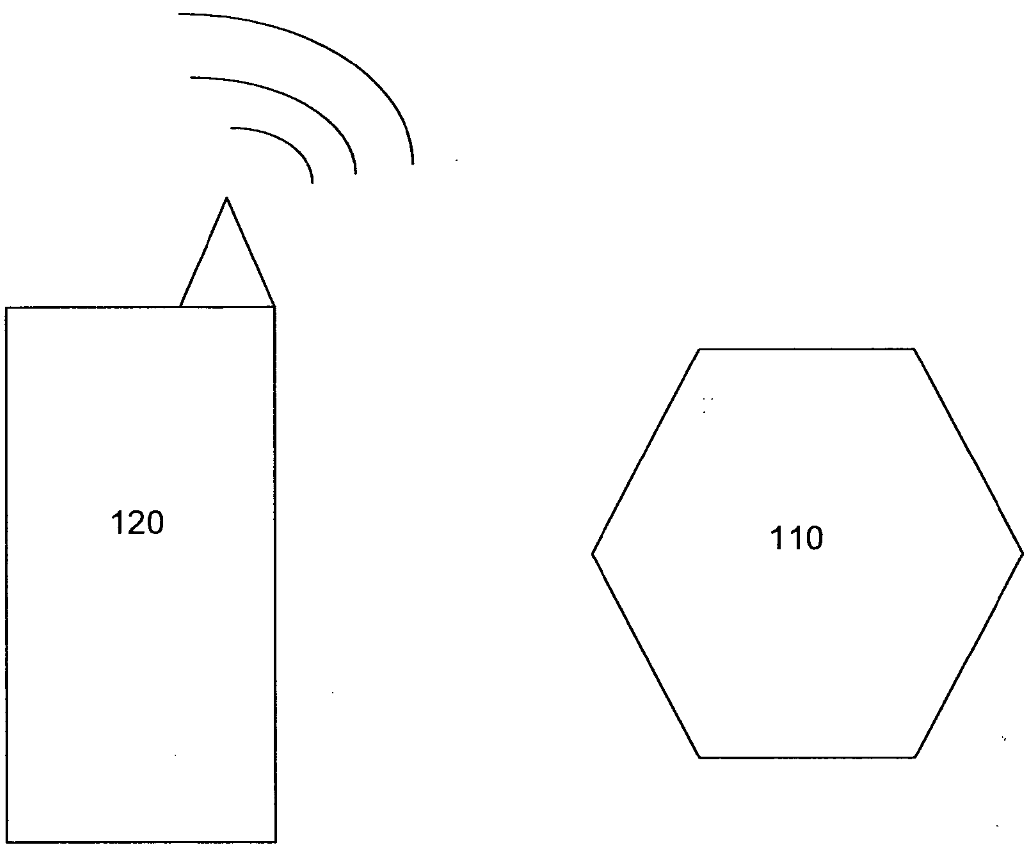


Figure 1.

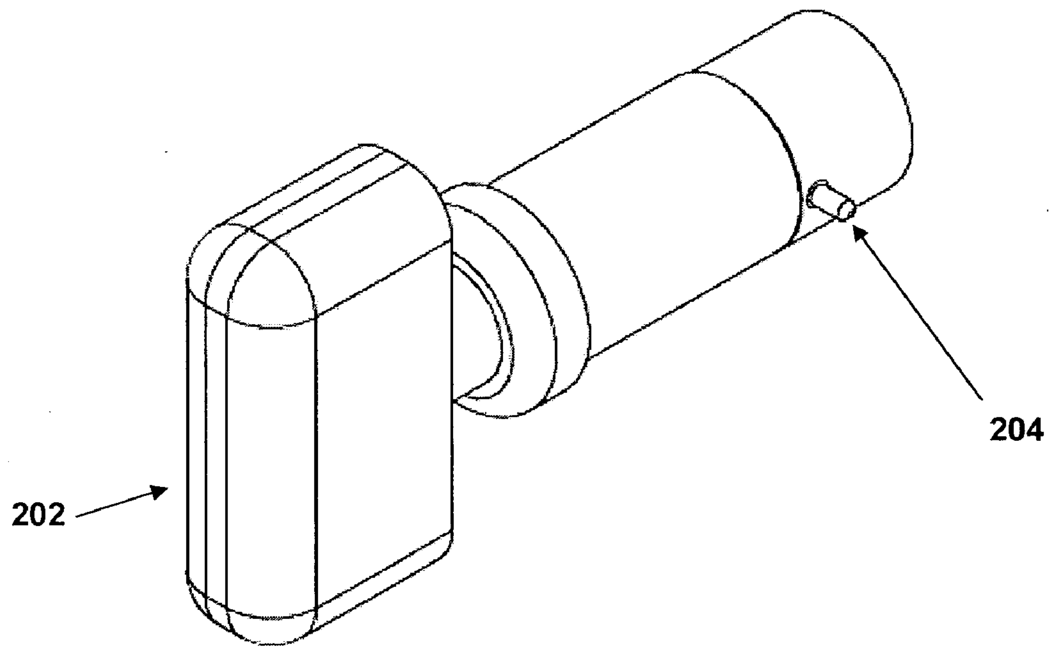


Figure 2.

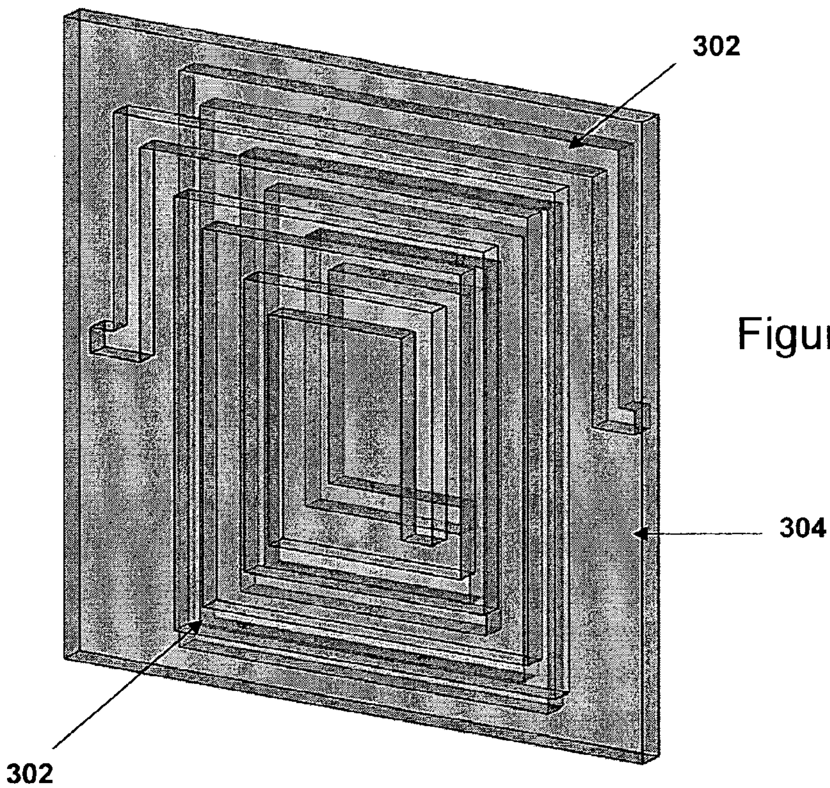


Figure 3a.

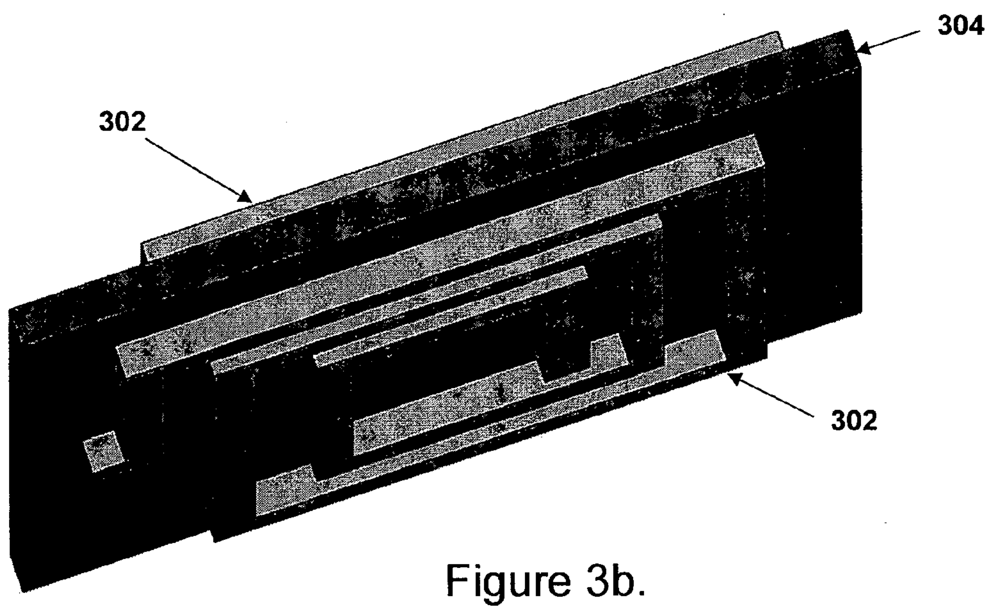


Figure 3b.

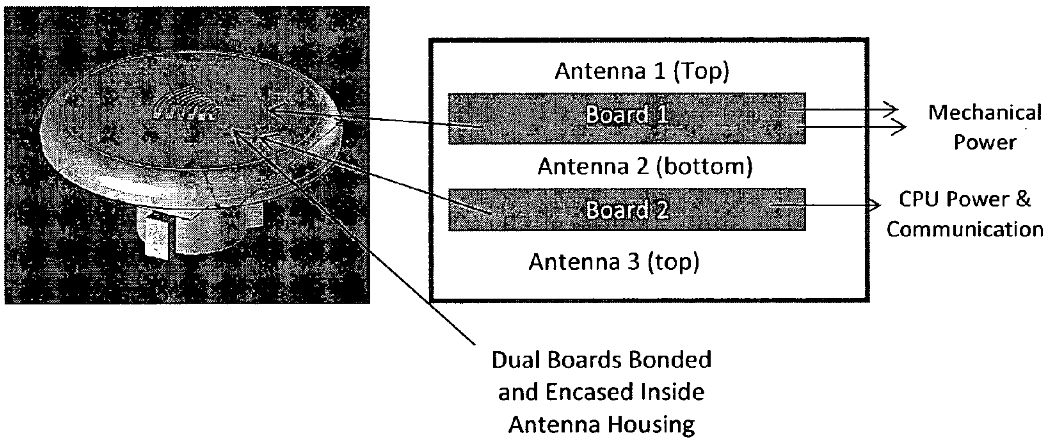

Antenna 1 (Top)
Board 1
Mechanical
Power
Antenna 2 (bottom)
Board 2
CPU Power &
Communication
Antenna 3 (top)
Dual Boards Bonded
and Encased Inside
Antenna Housing

Figure 4.

ELECTRONIC LOCKING SYSTEM AND METHOD

FIELD OF THE INVENTION

[0001] The present invention relates to an electronic locking mechanism. More particularly, it concerns a system and method for providing suitable power and actuating electronic locks using radio and induction technologies.

DESCRIPTION OF THE RELATED ART

[0002] Electronic locking systems requiring an electric current to engage/disengage a lock member are incorporated in a wide variety of environments where security is of importance. Electronic locking systems are generally preferred over traditional physical key-and-lock mechanisms given the increased functionality and greater security.

[0003] Increased functionality and security of electronic locks over traditional key locks is due to microprocessor technology being employed in the locking system. Microprocessor technology may allow selective access to a locking mechanism with greater confidence in the person or object requesting access, during certain times of the day, and even has the ability to create an audit log of the persons accessing the lock.

[0004] An additional advantage of electronic locking systems allows users to employ 'wireless' keys using a relatively simple RF transmitter and receiver. Basic security such as rolling or hopping code, may be implemented into this type of locking system.

[0005] However, in order for this functionality to be utilised, suitable power must be provided to the locking system. The current generated from a power source is required not only for the microprocessor in a lock to function, but also to engage/disengage the locking member. Further, a power source must be present in both a 'wireless' key and the locking member it actuates.

[0006] The present invention advantageously provides an alternative to existing electronic locking systems. The system and method according to certain embodiments of the present invention may advantageously be used to enhance functionality, while providing suitable power requirements in the electronic lock.

SUMMARY OF THE INVENTION

[0007] According to a first aspect of the invention, there is provided an electronic locking system that includes a lock with a locking member and a communication device. The communication device remotely powers the lock to actuate the locking member.

[0008] In accordance with a further aspect of the invention, there is provided an electronic lock. Power to actuate the locking member of the electronic lock is remotely supplied by a communication device.

[0009] According to still another aspect of the invention, there is provided a method for actuating a locking member of an electronic lock. The method includes the steps of receiving a RF induction field that is remotely supplied by a communication device, via an antenna communicably attached to the electronic lock. The locking member is actuated by power received from the RF induction field.

[0010] In accordance with a further aspect of the invention, the electronic lock includes at least one microprocessor, at least one solenoid, at least one antenna, and at least one capacitor. The lock further includes at least one battery, wherein the communication device remotely provides power to the lock to supplement the power supplied by the at least one battery.

[0011] The remote powering of the lock is enabled by radio field inductive technology, including ISO 14443, or ISO 15693, or RFID, or Near Field Communication technology. Further, the actuating of the locking member is subject to authentication of the communication device. The authentication includes public key cryptography or symmetrical key cryptography.

[0012] According to a further aspect of the invention, there is provided an electronic locking system that includes a lock with a locking member and at least one antenna. Suitable power to actuate the locking member is delivered through the at least one antenna received from a remote power source.

[0013] In accordance with a further aspect of the invention, there is provided an electronic lock. Power to actuate the locking member of the electronic lock is received by at least one antenna communicably attached to the electronic lock, from a remote power source.

[0014] According to still another aspect of the invention, there is provided a method for actuating a locking member of an electronic lock. The method includes the steps of receiving, via at least one antenna communicably attached to the electronic lock, an induction field, remotely supplied by a power source. The locking member is actuated by power received from the induction field.

[0015] In accordance with a further aspect of the invention, the electronic lock includes at least one microprocessor, at least one solenoid or DC motor or servo, and at least one capacitor. Further, the at least one antenna is a multi-layer antenna.

[0016] The remote power source is a communication device, and the lock further includes at least one internal power supply that may supplement the power supplied by the remote power source. The lock further includes a recharging device to recharge the at least one internal power supply.

[0017] The remote powering of the lock is enabled by radio field inductive technology, including ISO 14443, or ISO 15693, or RFID, or Near Field Communication technology. Further, the actuating of the locking member is subject to user authentication. The authentication includes public key cryptography or symmetrical key cryptography or at least one One Time Password.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] The invention will now be described in a non-limiting manner with respect to a preferred embodiment in which:—

[0019] FIG. **1** is an overview of a preferred embodiment of the present invention.

[0020] FIG. **2** is a locking mechanism according to a preferred embodiment of the present invention.

[0021] FIGS. **3***a* and **3***b* show an antenna with off-set layers according to a preferred embodiment of the present invention.

[0022] FIG. **4** is an antenna configuration according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0023] In the following discussion and in the claims that follow, the terms "including" and "includes" or "comprising" and "comprise" are used, and are to be read, in an open-ended fashion, and should be interpreted to mean "including, but not limited to . . . ".

[0024] Additionally, in the following discussion and in the claims that follow, the terms "electronic lock" and "electronic locking mechanism" are to be given a broad meaning, and refer to any locking device that is actuated (engages and/or disengages) by means of an electric current. An electronic lock or electronic locking mechanism in accordance with the present invention may or may not include a microprocessor.

[0025] Further, in the following discussion and in the claims that follow, the term "key" is to be given a broad meaning, and generally refers to any device that actuates the electronic lock or electronic locking mechanism. A key in accordance with the present invention may or may not include a microprocessor.

[0026] An exemplary embodiment of the system of the preset invention is shown in FIG. **1**, where there is provided an electronic lock **110**. The lock **110** preferably includes a locking member (not shown) that is movable between a closed (engaged) position and an open (disengaged) position. Preferably, the locking member is an electromagnetic latch.

[0027] The electronic lock **110** may include a power supply, preferably a soft battery, to provide power to the mechanism and actuate the locking member from an open (disengaged) position to a closed (engaged) position, or vice versa. However, in a preferred embodiment of the present invention, the electronic lock **110** does not have a traditional power supply.

[0028] The electronic lock **110** further preferably includes at least one antenna, capable of drawing power transmitted from a remote power source, such as a near field communication device **120**. The antenna is preferably a 13.56 MHz (or higher) compact antenna.

[0029] It will be appreciated that the antenna of the electronic lock may be capacitively loaded using resonant coupling to form tuned LC circuits in order to receive power.

[0030] However, such conventional configurations have traditionally not been suitable to receive an adequate and reliable amount of power to actuate a physical mechanism, such as a locking member.

[0031] Accordingly, in a particularly preferred embodiment of the present invention, the at least one antenna of the electronic lock is a multi-layer antenna that maximises electromagnetic field coupling, providing a relatively large inductance in a small area.

[0032] The electronic lock **110** in accordance with the present invention preferably further includes a microprocessor electrically connected to the locking member. The microprocessor is preferably a low power cryptographic secured processor which uses less than 5V DC and 60 mA. The microprocessor is preferably a self contained package including memory, ROM, and a power regulator in a miniature package that can be embedded inside various lock configurations, such as a locking cylinder, for example. It is to be understood that the components of the microprocessor are communicably attached to the electronic lock.

[0033] Further, it is to be understood that the electronic lock may be placed in a variety of casings in accordance with desired use. The electronic lock in accordance with the present invention may be implemented in suitable lock casings including, but not limited to, safe locks, filing cabinets, lockers, padlocks, door locks, cash boxes, vending machines, vehicle locks and deadlocks. A particularly preferred embodiment of the electronic lock mechanism is shown in FIG. **2**. Rotating turn knob **202** preferably physically moves the locking member **204** once relevant power is received and the user associated with the communication device is authenticated.

[0034] The system of the present invention further includes a remote power source. The remote power source is preferably a near field communication (NFC) enabled device **120** that is self powered by means of a battery unit (or similar), and capable of building a NFC field in close proximity. It will be appreciated however, that NFC technology need not be implemented, and any short-range communication technology capable of communicating via magnetic field induction may be used. Non-limiting examples of which may include ISO 14443, or ISO 15693, or RFID technology.

[0035] The NFC-enabled communication device **120** acting as the remote power source is preferably a mobile phone (such as those currently produced by Nokia®, BENq® and Samsung®), or a phone enabled with MicroSD NFC memory cards. Alternatively, the remote power source may be a single press-button transmitter or a transmitter with a PIN pad, such as a fob (also referred to as a ring) suitably attached to a key chain, with other/additional communication functionality.

[0036] In use, the communication device **120** of the present invention delivers power to its antenna, where a current is induced and transmitted to the electronic lock **110**, to be received by the at least one antenna. The microprocessor of the electronic lock **110** and the communication device **120** communicate with each other by modulating an established RF field. It is to be understood that the electronic lock and the communication device are preferably remote from each other. That is, the power delivered from the communication device to the electronic lock is remotely (wirelessly) delivered.

[0037] Preferably, an authentication exchange then takes place between the communication device **120** and the electronic lock **110**. The microprocessor of the electronic lock **110** controls a solenoid or other actuating mechanism, such as a DC motor, to actuate (engage/disengage) the locking member. It will be appreciated that the actuating mechanism may be any suitable mechanical device and may also include a servo with suitable torque characteristics.

[0038] The actuating mechanism draws its power from one or more capacitors associated with the at least one antenna within the electronic lock **110**, which is received from the RF field remotely generated by the remote power source.

[0039] Preferably, the at least one antenna of the electronic lock **110** is a multi-layer antenna, using a plurality of conductors, with off-set layers to reduce inherent parasitic capacitance associated with conventional stacked, single layer solenoids or flat spirals. A particularly preferred embodiment of the off-set layers of the antenna is shown in FIGS. **3***a* and **3***b*.

[0040] In order to further reduce the parasitic capacitance between antenna layers, each antenna is preferably applied on a Printed Circuit Board (PCB) with a thickness of approximately 0.05-0.08 inches (0.125-0.2 centimetres), with a preferred thickness of 0.062 inches (0.155 centimetres). The preferred thickness and the offset layout configuration maximises the quality factor and the self-resonance frequency of the antenna for proper operation at 13.56 MHz.

[0041] The antenna is preferably designed using suitable metal top and bottom layers **302** on a FR**4** PCB **304**, as shown in FIGS. **3***a* and **3***b*. As will be appreciated, if the PCB **304** is thin, the distance between the top and bottom off-set metal layers **302** is reduced and their capacitance increases. Accordingly, the overall inductance becomes insubstantial and the self-resonance frequency decreases. It is the self-resonance frequency of the antenna characteristic that becomes capacitive instead of being inductive.

[0042] Furthermore, additional layers (not shown)—such as ferrite layers, for example—can be added to the top and/or bottom layers **302** of the antenna to boost the electromagnetic fields passing through. This further adds to the multi-layer configuration, and increases the inductance and current of the antenna.

[0043] Traditionally, resonant coupling employs capacitively loaded coils to form matched LC circuits. However, in a particularly preferred embodiment of the present invention, a single capacitor is used to tune and match the at least one antenna to the NFC operating frequency of the communications device acting as the remote power source. It will be appreciated that, in the case of multiple antennas, each antenna will require its own corresponding tuning circuit facilitated by a corresponding single capacitor.

[0044] The use of a single capacitor, instead of using multiple inductor and capacitor components in an LC ladder circuit configuration, decreases the number of components required for matching and therefore reduces the need for a greater area of components on the PCB.

[0045] An antenna using an inductor L has a series resistance R due to its resistive metal inductors. Adding a series capacitance C creates a series RLC circuit with an input impedance Z_1 given by

$$Z_1 = \frac{1}{j\omega C} + j\omega L + R = R + j\omega L\left(1 - \frac{\omega_0^2}{\omega^2}\right)$$

where ω_0 is the resonant frequency defined as

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

[0046] When $\omega=\omega_0$, the input impedance becomes minimum and equal to resistance R and the output voltage across R becomes equal to the input voltage of the antenna. At the resonance frequency, the voltage across the capacitor C and the inductor L cancel each other and are given by

$$V_C = \frac{1}{j\omega_0 C} I_1 = \frac{1}{j\omega_0 C}\frac{V_1}{R} = -jQV_1$$

and

$$V_L = j\omega_0 L I_1 = j\omega_0 L\frac{V_1}{R} = jQV_1$$

where Q is defined as the quality factor. If Q is much larger than 1, then the voltage across matching capacitor C can increase to a larger value than the voltage at the antenna.

[0047] The at least one antenna may also preferably include an adjustable regulator circuit to assist in the prevention of voltage drop and power loss, providing constant voltage over the required time to actuate the locking member. Additionally, the communication device preferably periodically initializes communication with the electronic lock to ensure a robust power connection.

[0048] The at least one multi-layer antenna of the present invention is preferably a dual layer antenna. However, it will be appreciated that a three or more layer antenna could be adapted for use, as shown in FIG. **4**. As will be appreciated, the electronic lock may include various functions that require power, in addition to the actuating mechanism. For example, the electronic lock may include additional processor circuits to control a LCD screen, or a small illuminating device to assist the user in identifying the location of the lock. The antenna design of the present invention may be adapted to accommodate the additional power requirements of a CPU, without resorting to a hard-wired power source, or supplementary battery.

[0049] Further, and as demonstrated in FIG. **4**, the multi-layer design of the at least one antenna of the present invention advantageously allows for the provision of particular layers to draw power for the mechanism and other relevant functionality as mentioned above, while other layers may be used to transmit and receive data.

[0050] The at least one antenna preferably includes a hollow spiral structure, or other suitable design, to concentrate the electromagnetic field into the desired position, such as the centre of the antenna, to maximise the received power. It will be appreciated that the width of the spirals may be variously adapted to enhance received power and minimise ohmic losses. Each antenna may also be embedded inside suitable magnetic materials, such as ferrite for example, to boost the electromagnetic fields crossing the antenna. The current generation and performance of the antenna are enhanced with such a configuration.

[0051] It will be appreciated that the disengaging of the locking member may itself allow access to the desired room/compartment/facility etc. Alternatively, an authorised person may be required to physically turn a handle-type arrangement to gain access once the electronic lock is disengaged.

[0052] As described above, and in accordance with a particularly preferred embodiment of the present invention, the electronic lock does not include a power supply, such as a replaceable battery. The electronic lock remotely draws the required power to actuate the locking member from an RF field generated by a remote power source such as a communication device. There is no physical electrical connection required to actuate the lock.

[0053] However, it will be appreciated that certain lock configurations may require some form of internal or attached power supply, such as a battery. In this regard, and in accordance with an embodiment of the present invention, the RF field generated by a communication device may supplement the power supply of the electronic lock. The internal or attached power supply of this configuration may be suitable to provide all of the necessary power to engage/disengage the locking member, or may only provide a portion of the necessary power which can be 'topped up' by the RF field generated by the communication device. Such a configuration may be used on emergency doors, for example.

[0054] In a particularly preferred embodiment of this aspect of the invention, the electronic lock further includes a recharging device. The recharging device receives power via the at least one antenna of the electronic lock, and recharges the internal or attached power supply. Preferably, the communication device, acting as the remote power supply, is placed in the vicinity of the lock in accordance with the relevant radio technology field distance (for example, in the range of approximately 10 centimetres for NFC devices), for a longer period of time than would usually be required to actuate the locking member. The electronic lock would preferably inform the user of the communication device by means of an alarm or display for example, that the internal power supply requires recharging.

[0055] To enhance the security and credibility of the system, an authentication process is desired. In accordance with a particularly preferred embodiment of the present invention, the authentication process is based on the concept of public/private keys.

[0056] Preferably the electronic lock contains a cryptographic secure (smartcard-like) processor which has been provisioned with an authentication certificate. It is capable of validating engage or disengage requests based on a customer signature and is also preferably capable of uniquely identifying itself as a customer lock, for example, using mutual PKI (Public Key Infrastructure) authentication.

[0057] Further, the processor is preferably capable of validating One Time Password authentication requests based on relevant industry standards. It will be appreciated that the microcode is updatable, in similar regard to a smartcard, to evolve with industry standards. Additionally, the cryptographic data is updatable in the field to evolve with cryptographic key length requirements and processing power of attacking systems.

[0058] As discussed above, the communication device according to the present invention may be any suitable device, such as a mobile phone or a customised radio transmitter in the form of a key fob. Further, the communication device may also be a support device for a passive instrument, such as a smartcard or microprocessor identity card. The support device in the form of a badge holder for example, is preferably configured to include an internal power source that can provide suitable power to actuate a locking member in the manner described above.

[0059] Additionally, and in a particularly preferred embodiment of this aspect of the invention, the badge holder can also provide suitable power to the smartcard or other microprocessor identity card inserted into it. In this manner, the badge holder functions as a smartcard reader that may connect to a computing device and be used for smartcard functionality, such as PKI facilities.

[0060] As will be appreciated from the foregoing, the communication devices are preferably equipped with a secure storage area and their own private cryptographic key, or may act as a suitable reader in the form of a badge holder to retrieve/translate this information. The devices are capable of receiving configuration and cryptographic information from a Central Cryptographic Key Management security Server (CCKMS).

[0061] The CCKMS manages the provisioning of communication devices and the management of access control of these devices to the electronic locks.

[0062] For example, when a new lock is added to a person's account inside the CCKMS and that lock is associated with one or multiple communication devices, an access control file is cryptographically signed by the CCKMS and encrypted with the communication devices' key. The data block is transmitted to the communication device via suitable means, such as text message, download, Over-the-Air update, manual file etc.

[0063] When the communication device receives a data block it is able to decrypt it using its private key. The device further validates that the data block and contents were signed by the CCKMS. The data is then accepted and stored preserving the digital signatures from the CCKMS. An access control file contains the permissions that respective communication devices have to specific locks and specific user groups.

[0064] Once the communication device is presented to an electronic lock, and power via induction is remotely provided, the lock transmits its identifying information and the communication device determines if it has permission to actuate the locking member.

[0065] If the communication device determines that the electronic lock is valid and it has previously established a symmetrical key pair with the lock, it begins an authentication process request and may skip the establishment step.

[0066] For a new relationship between an electronic lock and a communication device, an establishment procedure of symmetrical keys and access privileges occurs. Preferably, the communication device transmits access control data that it has received from the CCKMS to the electronic lock. The lock in turn determines if it has a more current version of that access control data, and if the data is new it accepts it and validates the CCKMS signature.

[0067] The electronic lock then receives the public key of the communication device and validates that it was correctly signed with the CCKMS private key. The lock subsequently prepares a symmetric encryption key and a unique identifying number for the communication device, encrypts the key and number with the public key of the communication device, and then transmits it to the communication device.

[0068] The communication device decrypts the symmetric key and unique identifying number using its private key. The symmetric key is then used to generate a One Time Password and transmits that to the electronic lock with the unique identifying number of the communication device.

[0069] Finally, the electronic lock internally looks up the identifying number, the access control list and the unique symmetric key for that device. Once the One Time Password provided is validated, the locking member may be actuated.

[0070] Whilst public key infrastructure has been described as the authentication process for the present invention, it will be appreciated that other cryptographic secure authentication processes may be employed.

[0071] It will be appreciated that embodiments of the present invention may be used to access locking mechanisms that require the presentation of two or more electronic keys. Two or more communication devices may be presented simultaneously to the electronic lock. In this instance, each device is recognised and communicated with individually.

[0072] Alternatively, a first communication device is presented to the electronic lock and provides suitable power as described above. The electronic lock may or may not authenticate the device, but will inform the user of the first communication device that a second communication device is required. Once the first communication device is removed, the electronic lock powers down. The locking member of the electronic lock may be actuated once the second communication device is presented and authenticated.

[0073] It will be further appreciated that an unauthorised user may gain access to a particular environment, where an authorised user provides authority. The authority may be provided through a suitable service to generate a four to twelve digit one time access code, for example. The access code is based on a unique symmetrical key that is preinstalled in the electronic lock.

[0074] The authorised person would preferably provide the one time access code to the unauthorised person over a suitable secure link to the unauthorised user's communication device. Alternatively, the one time access code could be provided over an unsecure network, such as by telephone or email. Once the unauthorised user presents their communication device to the electronic lock, the one time access code is extracted/provided to gain a single access to actuate the locking member. Further security measures to enhance the integrity of the system will be apparent to those of skill in the art. For example, the time the access code was generated by the service may be embedded inside the transmitted code to determine validity.

[0075] There are a number of advantages using cryptographic keys to determine access to electronic locking mechanisms. For example, such keys are not duplicated, and may be provisioned or revoked securely and easily. That is, if a communication device is lost or stolen, it can be revoked from the system. Another trusted communication device may be employed which can deliver an updated payload from the CCKMS to respective electronic locks. The payload may include a list of authorized communication devices, as well as a time stamp. This time stamp is validated for all new establishment requests to ensure that an expired or de-authorized communication device cannot be re-established with an electronic lock.

[0076] Another advantage of using the keys of the present invention is relevant persons may access an audit log of the electronic lock. In accordance with an embodiment of the present invention, the audit log of a particular electronic lock may be accessed and read on a person's communication device, via the RF field.

[0077] The electronic lock stores an audit trail, and upon the request of an authorized communication device, the lock transmits the information from its storage to the device. The communication device can then display the audit trail on its screen and/or transmit the information to another storage location, such as a web site or data base.

[0078] A further advantage of the present invention allows administrators to gather/group users and assign multiple locks to be part of one group. Access privileges may be based on any number of considerations; for example, time of day per lock or group.

[0079] An additional advantage of the present invention allows authorized communication devices to provide Over-the-Air configuration and software updates to the electronic lock.

[0080] It is to be understood that the above embodiments have been provided only by way of exemplification of this invention, and that further modifications and improvements thereto, as would be apparent to persons skilled in the relevant art, are deemed to fall within the broad scope and ambit of the current invention described and claimed herein.

1. An electronic locking system, including:
an electronic lock with a locking member; and
a communication device,
wherein the communication device remotely powers the electronic lock to actuate the locking member.

2. The electronic locking system according to claim **1**, wherein the electronic lock further includes:
at least one microprocessor;
at least one solenoid;
at least one antenna; and
at least one capacitor.

3. The electronic locking system according to claim **1**, wherein the electronic lock further includes:
at least one microprocessor;
at least one DC motor;
at least one antenna; and
at least one capacitor.

4. The electronic locking system according to claim **1**, wherein the electronic lock further includes:
at least one microprocessor;
at least one servo motor;
at least one antenna; and
at least one capacitor.

5. The electronic locking system according to claim **2**, wherein the electronic lock further includes at least one battery.

6. The electronic locking system according to claim **5**, wherein the communication device remotely provides power to the electronic lock to supplement the power supplied by the at least one battery.

7. The electronic locking system according claim **1**, wherein the remote powering is enabled by radio field inductive technology.

8. The electronic locking system according to claim **7**, wherein the radio field inductive technology is ISO 14443, or ISO 15693, or RFID, or Near Field Communication technology.

9. The electronic locking system according to claim **1**, wherein the actuating of the locking member is subject to authentication of the communication device.

10. The electronic locking system according to claim **9**, wherein the authentication includes public key cryptography.

11. The electronic locking system according to claim **9**, wherein the authentication includes symmetrical key cryptography.

12. (canceled)

13. A method for actuating a locking member of an electronic lock, the method comprising:
receiving, via an antenna communicably attached to the electronic lock, a RF induction field, remotely supplied by a communication device;
wherein the locking member is actuated by power received from the RF induction field.

14. The method according to claim **13**, further including authenticating the communication device.

15. The method according to claim **14**, wherein the authentication includes public key cryptography.

16. The method according to claim **14**, wherein the authentication includes symmetrical key cryptography.

17. An electronic locking system, including:
an electronic lock with a locking member; and
at least one antenna,
wherein power to actuate the locking member is delivered through the at least one antenna received from a remote power source.

18. The electronic locking system according to claim **17**, wherein the electronic lock further includes:
at least one microprocessor;
at least one solenoid; and
at least one capacitor.

19. The electronic locking system according to claim **17**, wherein the electronic lock further includes:
at least one microprocessor;
at least one DC motor; and
at least one capacitor.

20. The electronic locking system according to claim **17**, wherein the electronic lock further includes:

at least one microprocessor;

at least one servo; and

at least one capacitor.

21. The electronic locking system according to claim **17**, wherein the at least one antenna is a multi-layer antenna.

22. The electronic locking system according to claim **17**, wherein the electronic lock further includes at least one internal power supply.

23. The electronic locking system according to claim **22**, wherein the electronic lock further includes a recharging device to recharge the at least one internal power supply.

24. The electronic locking system according to claim **17**, wherein the remote power source is a communication device.

25. The electronic locking system according to claim **24**, wherein the communication device is a mobile phone, key fob, or support device.

26. The electronic locking system according to claim **17**, wherein remote powering is enabled by radio field inductive technology.

27. The electronic locking system according to claim **26**, wherein the radio field inductive technology is ISO 14443, or ISO 15693, or RFID, or Near Field Communication technology.

28. The electronic locking system according to claim **17**, wherein the actuating of the locking member is subject to user authentication.

29. The electronic locking system according to claim **28**, wherein the user authentication includes public key cryptography.

30. The electronic locking system according to claim **28**, wherein the user authentication includes symmetrical key cryptography.

31. The electronic locking system according to claim **28**, wherein the user authentication includes the use of at least one One Time Password.

32. A method for actuating a locking member of an electronic lock, including the steps of:

receiving, via at least one antenna communicably attached to the electronic lock, an induction field remotely supplied by a power source;

wherein the locking member is actuated by power received from the induction field.

33. The method for actuating a locking member of an electronic lock according to claim **32**, wherein the at least one antenna is a multi-layer antenna.

34. The method for actuating a locking member of an electronic lock according to claim **32**, wherein the remotely supplied power source is provided from a communication device.

35. The method for actuating a locking member of an electronic lock according to claim **34**, wherein the communication device is a mobile phone, key fob, or support device.

36. The method for actuating a locking member of an electronic lock according to claim **32**, wherein remote powering is enabled by radio field inductive technology.

37. The method for actuating a locking member of an electronic lock according to claim **36**, wherein the radio field inductive technology is ISO 14443, or ISO 15693, or RFID, or Near Field Communication technology.

38. The method for actuating a locking member of an electronic lock according to claim **32**, wherein the actuating of the locking member is subject to user authentication.

39. The method for actuating a locking member of an electronic lock according to claim **38**, wherein the user authentication includes public key cryptography.

40. The method for actuating a locking member of an electronic lock according to claim **38**, wherein the user authentication includes symmetrical key cryptography.

41. The method for actuating a locking member of an electronic lock according to claim **38**, wherein the user authentication includes the use of at least one One Time Password.

42. An electronic lock, wherein power to actuate a locking member of the electronic lock is supplied from a remote power source.

* * * * *