(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/102625 A2

(51) International Patent Classification:
G06K 5/00 (2006.01)

(21) International Application Number:
PCT/US2006/010910

(22) International Filing Date: 24 March 2006 (24.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/665,043 24 March 2005 (24.03.2005) US

(71) Applicant *(for all designated States except US)*: **PRIVARIS, INC.** [US/US]; 675 Peter Jefferson Parkway, Suite 150, Charlottesville, Virginia 22911 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CANNON, Charles** [US/US]; 710 Battle Mountain Road, Amissville, Virginia 20106 (US). **REIGLE, Thomas** [US/US]; 12573 Colgate Court, Woodbridge, Virginia 22192 (US).

(74) Agent: **CHASTEEN, Kimberly**; 721 Lakefront Common, Suite 200, Newport News, Virginia 23606 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 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, LV, 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:
— *without international search report and to be republished upon receipt of that 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.

WO 2006/102625 A2

(54) Title: BIOMETRIC IDENTIFICATION DEVICE WITH SMARTCARD CAPABILITIES

(57) Abstract: A smartcard-enabled BPID Security Device integrates a smartcard reader with a biometric authentication component to provide secured access to electronic systems. The device allows for an individual to insert a smartcard into an aperture in the physical enclosure of the BPID Security Device, allowing the smartcard and the BPID Security Device to electronically communicate with each other. The smartcard-enabled BPID Security Device is based on a custom application specific integrated circuit that incorporates smartcard terminals, such that the BPID Security Device can communicate directly with an inserted smartcard. In an alternative embodiment of the invention, the smartcard-enabled BPID Security Device is based on a commercial off-the-shelf microprocessor, and may communicate with a commercial off-the-shelf microprocessor smartcard receiver using a serial, USB, or other type of communication protocol. The device allows for enrolling a user's credentials onto the smartcard-enabled BPID Security Device. The device also allows for authenticating an individual using the smartcard-enabled BPID Security Device.

BIOMETRIC IDENTIFICATION DEVICE WITH SMARTCARD CAPABILITIES

RELATED U.S. APPLICATION DATA

[01] This application claims priority under 35 U.S.C. 119(e) of provisional patent application Ser. No. 60/665,043 filed March 24, 2005, entitled, "Biometric Identification Device with Smartcard Capabilities," which is hereby incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION:

Field of the Invention:

[02] This invention relates to the field of portable, electronic personal identification and authentication devices. This invention relates more specifically to electronic devices using biometric and/or smartcard authentication technologies.

Related Art:

[03] U.S. Patent No. 6,991,174 to Zuili discloses a method and apparatus for authenticating a shipping transaction. The disclosed apparatus, which is not covered by the claims of the patent, is a portable smartcard reader incorporating a number of different authentication mechanisms, including a personal identification number (PIN), asymmetric cryptographic keys, and/or biometrics. The apparatus may be used autonomously or in conjunction with other electronic devices, such as a personal digital assistant (PDA), cellular telephone, or remote control. The apparatus is designed for use in a variety of applications, including computer networks, televisions and cable access, and payment transactions. The patented invention is a method of specifically authenticating a shipping transaction by using a smartcard and a smartcard reader, acquiring biometric information and shipping information from a customer, encrypting the shipping information using the biometric information,

storing the encrypted shipping information on the smartcard and in a database, permitting the customer to access the database in order to change the shipping information, and requiring the customer to resubmit biometric information in order to authenticate the shipping transaction.

[04] U.S. Patent No. 6,016,476 to Maes, et al., discloses a portable PDA with biometric authentication capability. The PDA is further capable of reading and writing information to smartcards, magnetic stripe cards, optical cards and/or electronically alterable read-only memory (EAROM) cards. The PDA is intended for use in payment transactions, and can communicate with other electronic devices, such as a point of sale terminal, through either wired or wireless transceivers.

[05] Research In Motion, Ltd. (RIM) produces and sells a device called "The BlackBerry® Smart Card Reader," which is a portable smartcard reader that provides two-factor authentication, symmetric cryptographic keys and the smartcard, for users attempting to access or use BlackBerry devices. Once the smartcard and the cryptographic key has been processed on the device, the device communicates via Bluetooth wireless technology with the BlackBerry device, enabling users to transmit secure e-mail. The device does not include biometric authentication.

[06] Key Ovation produces the "Goldtouch ErgoSecure Smart Card and Biometric Keyboard SF2.4." This device is a standard ergonomic computer keyboard, which incorporates both a smartcard reader and an Authentec fingerprint sensor. It is not portable, nor does it appear to possess wireless technology.

NECESSITY OF THE INVENTION:

[07] Companies, governments, and other organizations possess a variety of physical and digital resources, which are often valuable and must be protected. Some of these resources are physical, such as particular buildings, offices, or grounds, while others are more intangible, such as databases, computer files, or other digital data. As a natural consequence of wishing to protect the resource, organizations either implicitly or explicitly develop an associated security policy or structure that specifies rules for access to the resource. When an individual wants access to a protected resource, the organization's security policy will – again implicitly or explicitly – require the individual to identify himself in an acceptable manner, and will then authenticate the identified individual against the security policy. If the identified and authenticated individual has privileges to the resource he is permitted access.

[08] Both government agencies and private industry have developed a number of different technologies to implement these security policies. One such technology is the "proximity card," commonly used to secure physical access to commercial buildings and offices. The proximity card is typically the size of a credit card, and contains electronics sufficient to both store and wirelessly transmit a unique identifier to a receiver located at the access point. The proximity card gains its name from its characteristic type of wireless transmission, allowing the user to simply hold the card close (typically within a few inches) to the access point, without inserting the card into a reader. When a proximity card is issued to an individual, a centralized database associates the unique identifier on the card with that individual; when the individual provides the proximity card to gain access to the resource, the identifier is transmitted to the access point, and the association is verified. Once the unique identifier has been programmed onto the proximity card, it cannot be altered, nor can additional data be added to the card.

[09] Developers have been equally prolific in generating authenticating technologies for access to computers, networks, and other digital resources. The simplest examples are passphrases or personal identification numbers (PINs) that the individual must supply before being granted access to the resource. Virtually all e-mail systems are protected this way; another common example is the Windows® log-in process, which prompts the user to enter a username and password. In more advanced systems, individuals may be provided cryptographic keys, such as one half of a public key/private key pair, or a digital certificate. These technologies similarly rest on an individual's previous association with the particular credential, such as the passphrase or cryptographic key.

[10] One technology frequently used to accomplish one or both objectives of physical and digital access is the "smartcard." Similar to the proximity card, the smartcard is in the form-factor of a credit card. The smartcard, however, generally contains a small integrated circuit with sufficient processing power to perform a number of different tasks, including cryptography and two-way transmission. The smartcard can store unique identifiers, such as cryptographic keys, passphrases, and other user data, as well as be transported and used to obtain access to physical resources. One smartcard can provide storage and authentication for a number of different resources, each of which may have a different identifier. Rather than wirelessly transmitting credentials, such as the proximity card, the smartcard uses contact-based transmission, and requires the user to insert the smartcard into a reader at the access point. Smartcard readers may be attached to electronic resources, such as a computer or network terminal, or physical resources, such as doors, gates, etc. Because of the two-way transmission capability, the data stored on a smartcard may be altered or updated through the smartcard reader. Smartcards are extremely popular; for example, the Department of Defense (DoD) currently uses the smartcard-based Common Access Card (CAC) to grant access to its organizations and resources. The CAC retains all of the functions and features of the

traditional smartcard, and incorporates a photograph of the bearer on the outside of the card, to allow for both visual and electronic identification and authentication.

[11] Each of these security technologies, while very useful, is susceptible to use by an impostor. If an individual loses his proximity card or smartcard, anyone who picks it up may use it to access the resource. Biometric technology, which authenticates an individual by use of physical characteristics such as fingerprints, can largely eliminate this risk. In the case of fingerprint recognition, an individual's fingerprint is electronically scanned and stored as a numeric template. When the individual wishes to access the resource, the finger is rescanned and digitally compared to the stored fingerprint to determine a match. Biometrics offer a clear advantage over previous technology – while a smartcard may be easily stolen and used by an unauthorized individual, an electronic forgery of a fingerprint is much more difficult to achieve.

[12] The Privaris® BPID™ Security Device is one type of authentication device based on biometric technology, and is much younger technology than the smartcard. The BPID Security Device is a handheld, portable electronic device, containing a fingerprint scanner, two-way wireless communications, memory, and sufficient processing power to perform cryptographic functions and on-device fingerprint authentication algorithms. Much like the smartcard, the BPID Security Device can store unique identifiers, including cryptographic keys and passphrases, and can be used to authenticate an individual to a number of different resources. The BPID Security Device, however, possesses significantly more processing power and memory than the traditional smartcard, in part because of the fingerprint template storage and comparisons done on-board the device. Furthermore, the BPID Security Device is based on wireless technology, so it can use the same protocols as used in proximity cards, newer standards like the Bluetooth® protocol, or both. Data on the BPID Security Device can be transmitted or received without inserting the device into a reader, which, for example,

allows individuals to authenticate faster at a physical access point than they could using a smartcard.

[13] Since the advent of the smartcard, a number of organizations have attempted to create an identification system common to multiple organizations that utilized common information contained on the smartcard, while at the same time increasing the security of this information, and insuring positive identification of the individual using the smartcard, prior to granting access to approved resources. Shortage of memory, limited range for contactless applications, the need for multiple cards to accommodate existing building access systems, the need for reliable biometric authentication, and the difficulties associated with updating the data on the card all became issues. While the BPID Security Device can largely address these concerns, it does not possess the form-factor of the smartcard, and therefore does not lend itself to the visual identification component of the CAC. Nor does the BPID Security Device contain a contact-based transmission mechanism allowing it to interact with systems currently using smartcard readers. What is needed is an apparatus and methods that combines the visual identification aspect of the smartcard with the biometric and wireless components of the BPID Security Device, which can allow reversion to a contact-based smartcard system when necessary.

SUMMARY OF THE INVENTION:

[14] The present invention discloses apparatuses and methods for integrating smartcard and BPID Security Device technology. The primary apparatus of the invention, hereinafter termed a "smartcard-enabled BPID Security Device," integrates a smartcard reader with the BPID Security Device such that an individual may insert the smartcard into an aperture in the physical enclosure of the BPID Security Device, allowing the smartcard and the BPID Security Device to electronically communicate with each other. In one primary embodiment

of the invention, the smartcard-enabled BPID Security Device is based on a custom application specific integrated circuit (ASIC) that incorporates smartcard terminals, such that the BPID Security Device can communicate directly with an inserted smartcard. In an alternative embodiment of the invention, the smartcard-enabled BPID Security Device is based on a commercial off-the-shelf (COTS) microprocessor, and may communicate with a COTS smartcard receiver using a serial, USB, or other type of communication protocol. The first method of the invention is a process for enrolling a user's credentials onto the smartcard-enabled BPID Security Device. The second method of the invention is a process for authenticating an individual using the smartcard-enabled BPID Security Device.

[15] DETAILED DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts the smartcard-enabled BPID Security Device
100 – BPID Smartcard Security Device
101 – physical enclosure
102 – aperture for receiving a smartcard
110 – strap
310 – fingerprint sensor of the BPID Security Device

Fig. 2 depicts a smartcard being inserted into the smartcard-enabled BPID Security Device
100 – BPID Smartcard Security Device
101 – physical enclosure
102 – aperture for receiving a smartcard
200 – smartcard

Fig. 3 depicts a smartcard inserted into the smartcard-enabled BPID Security Device
100 – BPID Smartcard Security Device
101 – physical enclosure
102 – aperture for receiving a smartcard
200 – smartcard

Fig. 4 is a schematic representation of the smartcard-enabled BPID Security Device
100 – BPID Smartcard Security Device
210 – smartcard reader
211 – smartcard terminal
212 – external device terminal
300 – biometric authentication component

DETAILED DESCRIPTION OF THE INVENTION:

[16] The following detailed description is of the best presently contemplated mode of carrying out the invention. This description is not to be taken in a limiting sense, but is made merely for the purpose of illustrating general principles of embodiments of the invention.

[17] The primary apparatus of the invention is called a "smartcard-enabled BPID Security Device." As seen in Fig. 1, the BPID Smartcard Security Device 100 may be attachable to a strap 110, so that it may be worn around an individual's neck or used in some other convenient carrying method. The BPID Smartcard Security Device 100 comprises a physical enclosure 101 with an aperture 102 for receiving a smartcard, a biometric authentication component 300 (see Fig. 4), and a smartcard reader 210 (see Fig. 4). The fingerprint sensor 310 of the BPID Security Device is made externally available through the physical enclosure 101. As seen in Figs. 2 and 3, the aperture 102 may be oriented in the physical enclosure 101 such that a picture or photograph on the outside of a smartcard 200, such as the CAC, is easily visible to all approaching the individual.

[18] Fig. 4 is a schematic representation of the smartcard-enabled BPID Security Device, without the physical enclosure and aperture. The smartcard reader 210 may be any existing technology that incorporates contact-based terminals 211 for receiving and transmitting electronic data smartcards (hereinafter "smartcard terminal"), and at least one additional terminal 212 for transmitting and receiving data to an external device (hereinafter "external device terminal"). The biometric authentication component 300 and the smartcard reader 210 are located within the physical enclosure 101, such that a smartcard 200 inserted into the aperture 102 will physically contact the smartcard terminal 211 and may use existing smartcard protocols to transmit information to and from the smartcard reader 210. The smartcard reader 210 is physically coupled to the biometric authentication component 300, such that the external device terminal 212 allows the smartcard reader 210 to communicate with the biometric authentication component 300.

[19] In the first embodiment of the apparatus, the biometric authentication component 300 may communicate with the external device terminal 212 over a standard communications protocol, such as, but not limited to, RS232 (now known as EIA232) or Universal Serial Bus (USB). In an alternative embodiment of the apparatus, the biometric authentication component 300 and the smartcard reader 210 will coexist on a secure microprocessor (hereinafter "BPID Security Device /reader"), such that communications between the external device terminal 212 and the biometric authentication component 300 will be physically and electronically located on the same ASIC. In this embodiment of the invention, the BPID Security Device /reader will be located within the physical enclosure 101 such that a smartcard 200 inserted into the aperture 102 of the physical enclosure 101 will directly contact the smartcard terminal 211 of the BPID Security Device /reader. This creates enhanced security for the BPID Smartcard Security Device 100, as the ASIC may be physically and electronically secured.

[20] The first method of invention permits an individual with a smartcard to enroll himself into the BPID Smartcard Security Device 100. First, the individual places a smartcard 200 into the aperture 102 of the physical enclosure 101 such that the smartcard 200 contacts the smartcard terminal 211 of the reader 210. The individual then activates power to the smartcard-enabled BPID Security Device 101 and the smartcard reader 210 reads the smartcard's serial number. The smartcard reader 210 transmits the serial number to the biometric authentication component 300 using the external device terminals 212. The biometric authentication component 300 verifies that it has not previously been enrolled with the specific smartcard 200. The biometric authentication component 300 then connects to a BPID Security Device enrollment station and enrolls the individual pursuant to its regular procedure. During the enrollment procedure, the biometric authentication component 300 stores the individual's biometric data and a PIN, which are then associated in the memory of

the biometric authentication component 300 with the smartcard's 200 serial number. The biometric authentication component 300 also transmits the individual's biometric data and the PIN to the smartcard reader 210 via the external device terminals 212, and the smartcard reader 210 writes the biometric data and the PIN to the smartcard 200 via the smartcard terminal 211. The BPID Smartcard Security Device 100 is now enrolled and the user may remove the smartcard from the aperture 102 of the physical enclosure 101.

[21] The second method of the invention permits an individual to authenticate himself to a BPID Smartcard Security Device 100 he has previously enrolled in. First, the individual places a smartcard 200 into the aperture 102 of the physical enclosure 101 such that the smartcard 200 contacts the smartcard terminal 211 of the reader 210. The individual then activates power to the smartcard-enabled BPID Security Device 101 and the smartcard reader 210 reads the smartcard's serial number. The smartcard reader 210 transmits the serial number to the biometric authentication component 300 using the external device terminals 212. The biometric authentication component 300 verifies that it has previously been enrolled with the specific smartcard 200 and requests the individual to authenticate himself to the biometric authentication component 300 according to its standard procedure. If the biometric authentication component 300 successfully authenticates the individual, the biometric authentication component 300 locates the PIN associated with the smartcard's 200 serial number and transmits the PIN via the external device 212 to the smartcard reader 210. The smartcard reader 210 then transmits the PIN to the smartcard 200 via the smartcard terminal 211.

[22] If the smartcard 200 possesses "match-on-card" capabilities, i.e. the smartcard is capable of matching fingerprint templates to those stored on the card, the biometric authentication component 300 locates the fingerprint template associated with the smartcard's 200 serial number and transmits the template via the external device 212 to the smartcard

reader 210. The smartcard reader 210 then transmits the template to the smartcard 200 via the smartcard terminal 211. If the smartcard 200 matches both the transmitted PIN and fingerprint template to its stored PIN and template, it 200 transmits its stored electronic data to the smartcard reader 210 via the smartcard terminal 211, which subsequently transmits the stored electronic data to the biometric authentication component 300 via the external device terminal 212. The biometric authentication component 300 may now use the electronic data stored on the smartcard 200 as necessary.

[23] If the smartcard 200 does not possess "match-on-card" capabilities, the smartcard 200 will only match the transmitted PIN to its stored PIN. It 200 will then transmit the stored fingerprint template to the smartcard reader 210 via the smartcard terminal 211, which in turn transmits the fingerprint template to the biometric authentication component 300 via the external device terminal 212. The biometric authentication component 300 locates the fingerprint template associated with the smartcard's 200 serial number and compares the stored template to the template transmitted from the smartcard 200. If the two match, the biometric authentication component 300 prompts the smartcard reader 210 to transmit its stored electronic data to the smartcard reader 210 via the smartcard terminal 211. The smartcard reader 210 then transmits the stored electronic data to the biometric authentication component 300 via the external device terminal 212. As above, the biometric authentication component 300 may now use the electronic data stored on the smartcard 200 as necessary.

[24] Those having ordinary skill in the art will recognize that the precise sequence of steps may be altered such that they result in the same functional outcome. Many improvements, modifications, and additions will be apparent to the skilled artisan without departing from the spirit and scope of the present invention as described herein and defined in the following claims.

CLAIMS:

We claim,

1. An autonomous, portable apparatus for identifying and authenticating electronic user credentials, comprising:
    a. a physical enclosure with an aperture for receiving a smartcard;
    b. a reading/writing means for reading and writing to a smartcard, such that when a smartcard is placed into said aperture of said physical enclosure, the smartcard connects to said reading/writing means such that the smartcard can be read or written; and
    c. a personal authentication device comprising an authentication means for biometric authentication, a wireless transceiver, a communication means for communicating with said reading/writing means, and a processing means for electronic data processing and storage, located inside said enclosure and coupled to said reading/writing means.
2. The apparatus of Claim 1, wherein said physical enclosure is tamper-evident.

3. The apparatus of Claim 1, wherein said physical enclosure is tamper-resistant.

4. The apparatus of Claim 1, wherein said aperture of said physical enclosure is oriented such that when a smartcard is inserted into said aperture, the external surface of the smartcard is visible.

5. The apparatus of Claim 1, wherein said reading/writing means and said personal authentication device are implemented together on an application-specific integrated

circuit, such that communications between said reading/writing means and said personal authentication device are secure and tamper-resistant.

6. The apparatus of Claim 1, wherein said reading/writing means and said personal authentication device communicate using serial communications.

7. The apparatus of Claim 1, wherein said reading/writing means and said personal authentication device communicate using a Universal Serial Bus.

8. A method for associating a user with an autonomous, portable apparatus for identifying and authenticating electronic user credentials, comprising the steps of:
    a. providing the autonomous, portable apparatus which comprises:
        i. a physical enclosure with an aperture for receiving a smartcard;
        ii. a reading/writing means for reading and writing to a smartcard, such that when a smartcard is placed into said aperture of said physical enclosure, the smartcard connects to said reading/writing means such that the smartcard can be read or written; and
        iii. a personal authentication device comprising an authentication means for biometric authentication, a wireless transceiver, a communication means for communicating with said reading/writing means, and a processing means for electronic data processing and storage, located inside said enclosure and coupled to said reading/writing means;
    b. placing a smartcard into said aperture formed in said physical enclosure of the autonomous, portable apparatus;
    c. using said reading/writing means to read said a serial number assigned to said smartcard;
    d. transmitting said serial number to said personal authentication device;
    e. verifying that said personal authentication device has not previously enrolled said smartcard using said serial number;
    f. connecting said personal authentication device to an external enrollment station;
    g. using said external enrollment station to acquire a biometric template and a personal identification number from the user;

h. transmitting said biometric template and said personal identification number to said personal authentication device;

i. storing said biometric template and said personal identification number to said personal authentication device;

j. associating said serial number with said biometric template and said personal identification number in said personal authentication device;

k. transmitting said biometric template and said personal identification number from said personal authentication device to said smartcard; and

l. storing said user's biometric template and personal identification number on said smartcard.

9. A method for authenticating a user to a device using an autonomous, portable apparatus for identifying and authenticating electronic user credentials, comprising the steps of:

    a. providing the autonomous, portable apparatus which comprises:

        i. a physical enclosure with an aperture for receiving a smartcard;

        ii. a reading/writing means for reading and writing to a smartcard, such that when a smartcard is placed into said aperture of said physical enclosure, the smartcard connects to said reading/writing means such that the smartcard can be read or written; and

        iii. a personal authentication device comprising an authentication means for biometric authentication, a wireless transceiver, a communication means for communicating with said reading/writing means, and a processing means for electronic data processing and storage, located inside said enclosure and coupled to said reading/writing means;

    b. placing a smartcard into said aperture formed in said physical enclosure of the autonomous, portable apparatus;

    c. acquiring a biometric sample and a personal identification number from the user using the personal authentication device;

    d. comparing said acquired biometric sample and personal identification number to a previously stored biometric sample and personal identification number; and

    e. authenticating the user if said acquired biometric sample and personal identification number match said previously stored biometric sample and personal identification number.

10. The method of Claim 9 wherein the comparison step is performed on the smartcard.

11. The method of Claim 9, wherein the comparison step is performed on the personal authentication device.

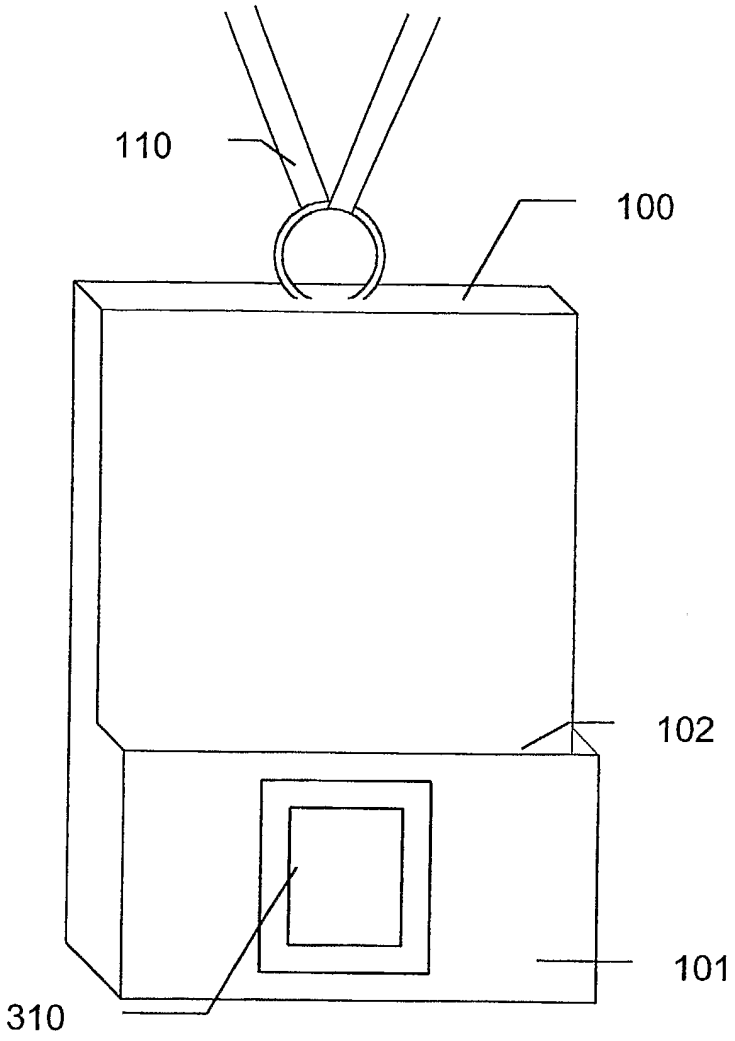

FIG. 1

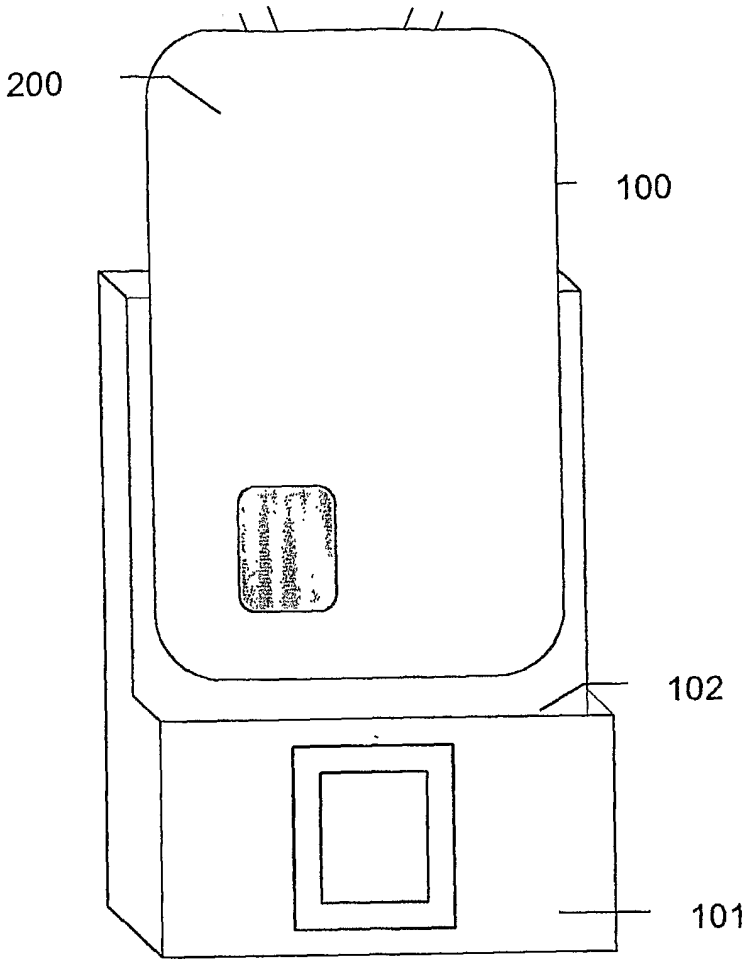

FIG. 2

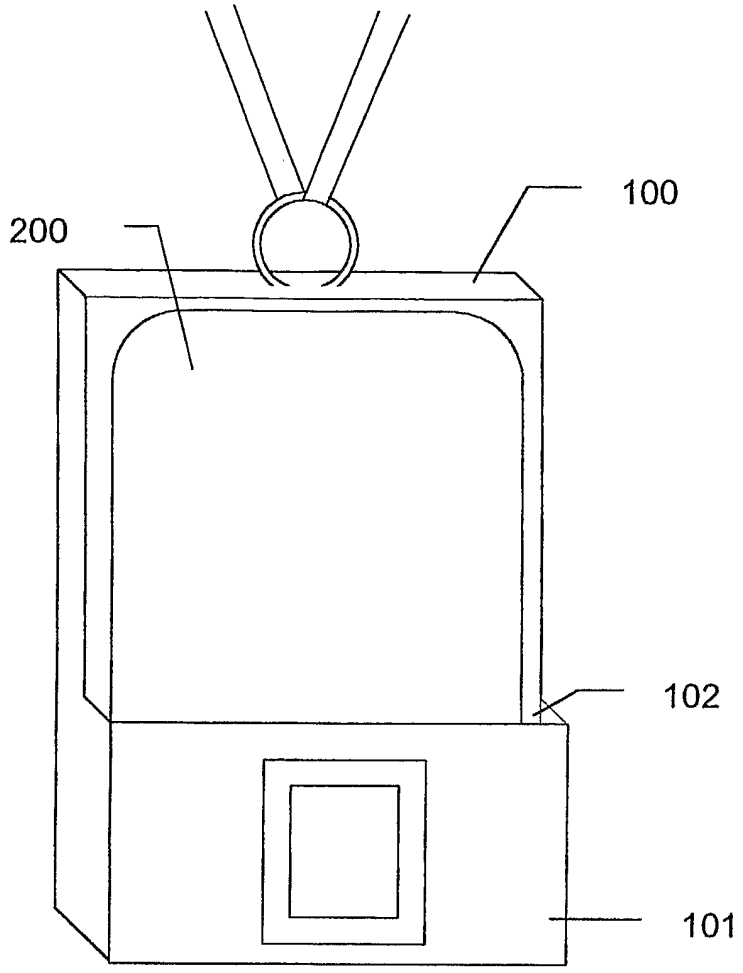

FIG. 3

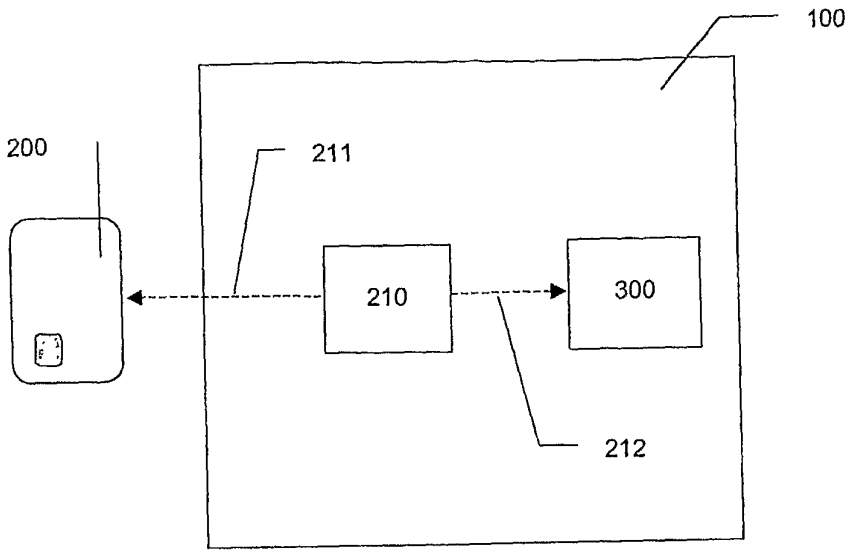

FIG. 4