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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 April 2009 (30.04.2009)

PCT

(10) International Publication Number
WO 2009/052548 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06K 9/62* (2006.01)

(21) International Application Number:
PCT/AU2008/001490

(22) International Filing Date: 8 October 2008 (08.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007905760 22 October 2007 (22.10.2007) AU
2008900672 13 February 2008 (13.02.2008) AU

(71) Applicant *(for all designated States except US)*: **MICROLATCH PTY LTD** [AU/AU]; Unit 13, 145-147 Forest Road, Hurstville, NSW 2220 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BURKE, Christopher, John** [AU/AU]; 48 Margate Street, Ramsgate, NSW 2217 (AU).

(74) Agent: **SPRUSON & FERGUSON**; GPO Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) **Title:** A TRANSMITTER FOR TRANSMITTING A SECURE ACCESS SIGNAL

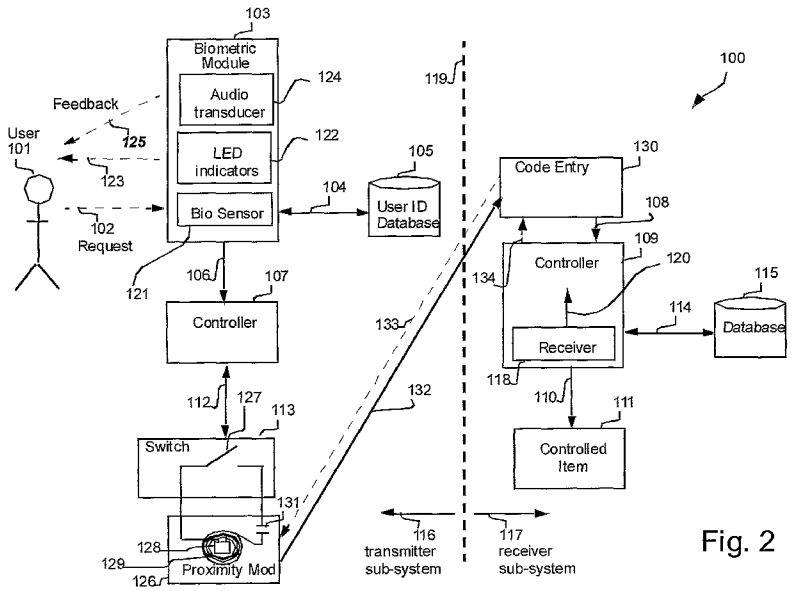

Fig. 2

(57) **Abstract:** A transmitter (116) for transmitting a secure access signal to a system (117) for providing secure access to a controlled item (111) is disclosed. The access is dependent on information contained in the secure access signal. The transmitter (116) comprises a biometric sensor (121) for receiving a biometric signal and a processor (1005) for matching the biometric signal against members of a database (105) of biometric signatures. The transmitter (116) comprises enabling means (e.g., 127) for enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system (117) upon the inductive circuit being placed within range of a radio frequency field emitted by the system (117).

WO 2009/052548 A1

A TRANSMITTER FOR TRANSMITTING A SECURE ACCESS SIGNAL

Field of the Invention

The present invention relates to secure access systems and, in particular, to systems for remote entry access.

Background

Fig. 1 shows a conventional arrangement for providing secure access. A user 401 makes a request, as depicted by an arrow 402, directed to a code entry module 403. The module 403 is typically mounted on the external jamb of a secure door. The request 402 is typically a secure code of some type which is compatible with the code entry module 403. Thus, for example, the request 402 can be a card number stored within a conventional proximity card used to direct the request 402 to a card reader 403. Alternatively, the request 402 can be a sequence of secret numbers directed to a keypad 403. The request 402 can also be a biometric signal from the user 401 directed to a corresponding biometric sensor 403. One example of a biometric signal is a fingerprint. Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, palm configuration and so on.

The code entry module 403 conveys the request 402 by sending a corresponding signal, as depicted by an arrow 404, to a controller 405 which is typically situated in a remote or inaccessible place. The controller 405 authenticates the security information provided by the user 401 by interrogating a database 407 as depicted by an arrow 406. If the user 401 is authenticated, and has the appropriate access privileges, then the controller 405 sends an access signal, as depicted by an arrow 408, to a device 409 in order to provide the desired access. The device 409 can, for example, be the locking mechanism of a secure door, or can be an electronic lock on a personal computer (PC) which the user 401 desires to access.

Current systems as depicted in **Fig. 1** utilise a communication protocol called "Wiegand" for communication between the code entry module 403 and the controller 405. The Wiegand protocol is a simple one-way data protocol that can be modified by increasing or decreasing the bit count to ensure uniqueness of the protocol among different security companies. The Wiegand protocol does not secure the information being sent between the code entry module 403 and the controller 405.

More advanced protocols such as RS 485 have been used in order to overcome the vulnerability of the Wiegand protocol over long distance routes. RS 485 is a duplex protocol offering encryption capabilities at both the transmitting and receiving ends, ie. the code entry module 403 and the controller 405 respectively in the present case. The length of the path 404 nonetheless provides an attack point for the unauthorised person.

Proximity cards have become a popular means for emitting the request 402, since proximity cards are cheap, easy to use and convenient to carry for the user 401. Typically, proximity cards comprise an inductive circuit including an integrated circuit (IC), a capacitor, and a coil, which are connected in series within the card. When a proximity card 410 is placed within range of the code entry module 403 (or "card reader"), the code entry module 403 presents a field that excites the coil and charges the capacitor, which in turn energizes the IC on the proximity card 410. The IC then transmits a card number stored within the IC, via the coil as transmit antenna, to the code entry module 403. The field emitted by the code entry module 403 for older proximity cards is typically around 125 kHz. The field emitted by the code entry module 403 for newer proximity cards is typically around 13.56 MHz. These newer proximity cards are typically in the form of contactless RFID cards which are also known as "contactless smartcards". Proximity cards have a communication range of 0-80 mm in most instances, allowing the user to place the card 410 within 80 mm of the code entry module 403 in

order for the card to be read by the code entry module 403. The term "communication range" refers, in the described example, to the distance to within which the proximity module 126 and the code entry module 130 must be brought in order for their respective transmit/receive antennas to be able to achieve satisfactory communications.

Conventional proximity cards (e.g., 410) used for emitting the request 402 may be lost by the user 401, and the lost proximity card 410 may be used by an unauthorised person to gain the desired access. In fact, there has been a high incidence of such fraudulent activity with conventional proximity cards where unauthorised persons steal the cards. As a result many users have looked to upgrade their proximity card secure access systems with other more secure systems. However, the cost of such up-grades is high due to the necessity to re-wire buildings and facilities to implement the upgrades.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

According to a first aspect of the present invention there is provided a transmitter for transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the transmitter comprising:

a biometric sensor for receiving a biometric signal;

a processor for matching the biometric signal against members of a database of biometric signatures; and

enabling means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the

system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

According to another aspect of the present invention there is provided a method of transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the method comprising:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures; and

enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the program comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures; and

code for enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

According to still another aspect of the present invention there is provided a system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures; and

means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying information upon the inductive circuit being placed within range of a radio frequency field; and

a receiver sub-system comprising;

means for emitting the radio frequency field;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the controlled item dependent upon said information.

According to still another aspect of the present invention there is provided a transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for emitting a radio frequency field, means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures; and

means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying said information upon the inductive circuit being placed within range of the radio frequency field.

According to still another aspect of the present invention there is provided a receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures, and means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying information; wherein the receiver sub-system comprises:

means for emitting a radio frequency field;

means for receiving the transmitted secure access signal from the transmitter sub-system upon the inductive circuit being placed within range of a radio frequency field; and

means for providing conditional access to the controlled item dependent upon said information.

According to still another aspect of the present invention there is provided a system for providing secure access to one of a plurality of controlled items, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for determining if the received biometric signal matches a member of the database of biometric signatures;

a plurality of proximity modules associated with the plurality of controlled items;

means for selecting one of said plurality of proximity modules; and

means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module; and

a receiver sub-system comprising;

means for emitting said radio frequency field adapted to activate the selected proximity module;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the selected controlled item dependent upon said information.

According to still another aspect of the present invention there is provided a transmitter for transmitting a secure access signal to a system for providing secure access to one of a plurality of controlled items, said access being dependent on information contained in the secure access signal, the transmitter comprising:

a biometric sensor for receiving a biometric signal;

means for determining if the received biometric signal matches a member of a database of biometric signatures;

a plurality of proximity modules associated with the plurality of controlled items;

means for selecting one of said plurality of proximity modules; and

means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

According to still another aspect of the present invention there is provided a receiver sub-system in a system for providing secure access to one of a plurality of controlled items, the system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, means for determining if the received biometric signal matches a member of the database of biometric signatures, a plurality of proximity modules associated with the plurality of controlled items, means for selecting one of said plurality of proximity modules, and means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module; said receiver sub-system comprising:

means for emitting said radio frequency field adapted to activate the selected proximity module;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the selected controlled item dependent upon said information.

According to still another aspect of the present invention there is provided a system for performing a secure transaction, the system comprising:

a database of one or more biometric signatures;

a first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating a first password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing funds available; and

a second sub-system comprising;

means for receiving the first password;

means for determining the funds available based on the received password; and

means for performing the transaction based on the available funds.

According to still another aspect of the present invention there is provided a first sub-system for operating in a system for performing a secure transaction, the system comprising a database of biometric signatures, a second sub-system comprising means for receiving a password, and means for performing the secure transaction based on available funds dependent upon the password, the first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating the password dependent upon said authentication signal, wherein said password is generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing said funds available.

According to still another aspect of the present invention there is provided a system for performing a secure transaction over a network using a card, the system comprising:

a database of one or more biometric signatures;

a first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing said magnetic stripe card; and

a second sub-system comprising;

means for reading the card;

means for receiving the password;

means for authenticating the received password based on the card number encrypted within password; and

means for performing the transaction based on the authentication.

According to still another aspect of the present invention there is provided a method of transmitting a secure access signal to a system for providing secure access to

one of a plurality of controlled items, said access being dependent on information contained in the secure access signal, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal to a member of a database of biometric signatures;

selecting one of a plurality of proximity modules, the selected proximity module being associated with at least one of the plurality of controlled items; and

enabling the selected proximity module, if the received biometric signal matches a member of the database of biometric signatures, the enabled selected proximity module being configured for transmitting a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

According to still another aspect of the present invention there is provided a method for performing a secure transaction over a network using a card, the method comprising:

matching a biometric signal against members of a database of biometric signatures to thereby determine an authentication signal; and

generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said password comprising an encrypted number representing said card;

reading the card to determine said card number from said card;

authenticating a received password based on the card number encrypted within password; and

performing the transaction based on the authentication.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer

program recorded therein for transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the program comprising:

code for receiving a biometric signal;

code for matching the biometric signal to a member of a database of biometric signatures;

code for selecting one of a plurality of proximity modules, the selected proximity module being associated with at least one of the plurality of controlled items; and

code for enabling the selected proximity module, if the received biometric signal matches a member of the database of biometric signatures, the enabled selected proximity module being configured for transmitting a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

According to still another aspect of the present invention there is provided a computer program product having a computer readable medium having a computer program recorded therein for performing a secure transaction over a network using a card, the program comprising:

code for matching a biometric signal against members of a database of biometric signatures to thereby determine an authentication signal; and

code for generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said password comprising an encrypted number representing said card;

code for reading the card to determine the card number from said card;

code authenticating a received password based on the card number encrypted within password; and

code for performing the transaction based on the authentication.

Other aspects of the invention are also disclosed.

Brief Description of the Drawings

Some aspects of the prior art and one or more embodiments of the present invention are described with reference to the drawings, in which:

Fig. 1 shows a conventional arrangement for providing secure access;

Fig. 2 is a functional block diagram of a system for providing secure access according to an exemplary embodiment of the present invention;

Fig. 3 shows an example of a method of operation of a transmitter sub-system of the system of **Fig. 2**;

Fig. 4 shows an example of a method of operation of a receiver sub-system of the system of **Fig. 2**;

Fig. 5A shows an example of a method of operation of the transmitter sub-system of **Fig. 2** where the IC is a smart card chip;

Fig. 5B shows an example of a method of operation of the receiver sub-system of **Fig. 2** where the IC is a smart card chip;

Fig. 6 is a schematic block diagram of the system in **Fig. 2**;

Figs. 7A and **7B** show an alternate arrangement for enabling the proximity module in **Fig. 2**;

Fig. 8 shows how the secure access system of **Fig. 2** can support multiple selectable proximity modules;

Fig. 9 shows an example of a method of operation of the arrangement of **Fig. 8**;

Fig. 10 shows an example of a method of making an online payment using the arrangement of **Fig. 8**;

Fig. 11 is a functional block diagram of a general purpose computer system upon which the method of **Fig. 10** may be implemented;

Fig. 12 shows an example of a method of debiting an amount of funds from an account stored within the transmitter sub-system of **Figs. 2** and **8;**

Fig. 13 shows how the secure access system of **Fig. 2** can support one or more conventional proximity modules according to another embodiment; and

Fig. 14 shows an example of a method of performing a secure transaction using the arrangement of **Fig. 13.**

Detailed Description including Best Mode

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

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.

Fig. 2 is a functional block diagram of a system 100 for providing secure access according to the exemplary embodiment. A user 101 makes a request, as depicted by an arrow 102, to a biometric module 103. The biometric module 103 includes a biometric sensor 121 and the request 102 takes the form of a biometric signal which corresponds to the nature of the sensor 121 in the module 103. In the embodiments described herein, the biometric sensor 121 in the module 103 is a fingerprint sensor and the request 102

typically takes the form of a thumb press on a sensor panel (not shown) on the module 103. Alternatively, the biometric sensor 121 may be responsive to one or more of voice, retinal pattern, iris pattern, face pattern and palm configuration.

The module 103 interrogates, as depicted by an arrow 104, a user identity database 105. Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains one or more members in the form of biometric signatures for authorised users against which the request 102 can be authenticated. If the identity of the user 101 is authenticated successfully, then the biometric module 103 sends a signal 106 to a controller 107. Upon receiving the signal 106, the controller 107 sends a signal, as depicted by an arrow 112, to a switch module 113 comprising a "normally open" switch 127. Any suitable mechanical or electronic (e.g., semiconductor) switch may be used to implement the switch 127.

As seen in **Fig. 2**, the switch module 113 is connected to a proximity module 126. The proximity module 126 comprises an inductive circuit formed from an IC 128, a coil 129 and a capacitor 131, which are connected in series. The IC 128 has information in the form of a unique card number stored within a memory of the IC 128. The switch 127 of the switch module 113 is connected in series with the IC 128, the coil 129 and the capacitor 131 of the proximity module 126. Accordingly, the proximity module 126 is similar to that used in conventional proximity cards such as those provided by financial institutions such as VISA®, MASTERCARD®, AMERICAN EXPRESS® and so on. However, the switch module 113 is configured to close and open the circuit formed by the IC 128, the coil 129 and the capacitor 131, thereby enabling and disabling the proximity module 126, respectively.

Upon receiving the signal 112 from the controller 107, the switch module 113 closes the normally open switch 127 for a predetermined period of time (e.g., four to five

seconds). Within this period the inductive circuit in the proximity card module 126 is enabled and may be placed by the user 101 within range of a radio frequency field being emitted by a code entry module 130. The field emitted by the code entry module 130 excites the coil 129 and charges the capacitor 131, which in turn energizes the IC 128 and thus activates the proximity module 126. The IC 128 then transmits, as depicted by an arrow 132, a secure access signal, via the coil as transmit antenna, to the code entry module 130. Accordingly, the secure access signal 132 is transmitted via the inductive circuit. The secure access signal 132 is configured for conveying information including the card number stored within the memory of the IC 128.

The switch 127 is preferably implemented in the form of a flip/flop arrangement where upon receiving the signal 112 the switch 127 will close but will automatically return to the normally open position at the end of the predetermined period. Accordingly, if the proximity card module 126 is not placed within the range of the code entry module 130 within the predetermined period, then the field emitted by the code entry module 130 will not charge the capacitor 131 as the switch 127 has opened the circuit formed by the IC 128, coil 129 and capacitor 131. In this instance, the user 101 again makes the request 102 in order to enable the proximity module 126.

Upon receiving the secure access signal 132 including the card number from the proximity card module 126, the code entry module 130 sends a signal, as depicted by an arrow 108, including the card number to a controller 109. The controller 109 tests the card number received from the code entry module 130 against a database 115 of card numbers, this testing being depicted by an arrow 114. If the incoming card number received from the code entry module 130 is found to be legitimate, then the controller 109 sends a command, as depicted by an arrow 110, to a controlled item 111. The controlled item 111 can be a door locking mechanism on a secure door, or an electronic lock (or key

circuit) on a personal computer (PC) that is to be accessed by the user 101. Accordingly, access to the controlled item 111 is dependent on the information (e.g., the card number) contained in the secure access signal 132. The system 100 provides conditional access to the controlled item 111 dependent upon the information contained in the secure access signal 132.

It is noted that the controller 109 contains a receiver 118 that receives the signal 108 including the card number and converts the signal 108 into a form, as depicted by an arrow 120, that the controller 109 can use.

The biometric module 103 also incorporates at least one mechanism for providing feedback to the user 101. This mechanism can, for example, take the form of one or more Light Emitting Diodes (LEDs) 122 which can provide visual feedback, depicted by an arrow 123 to the user 101. Alternately, or in addition, the mechanism can take the form of an audio signal provided by an audio transducer 124 providing audio feedback 125. Similarly, the code entry module 130 may also incorporate one or more mechanisms for providing feedback to the user 101.

The transmitter sub-system (or transmitter) in **Fig. 2** falling to the left hand side, as depicted by an arrow 116, of a dashed line 119 may be implemented in a number of different forms. The transmitter sub-system 116 (or transmitter), including the biometric module 103, the switch module 113, the user ID database 105, the controller 107 and the proximity module 126, may for example be incorporated within a remote fob (which is a small portable device carried by the user 101) or even a mobile (cell) telephone. The biometric module 103 may be powered by an internal battery of the fob or telephone.

Similar to the transmitter sub-system 116, the code entry module 130, the controller 109, database 115 and the controlled item 111 form a receiver sub-system 117 as seen in Fig. 2.

The code entry module 130 may be mounted in a protected enclosure on the outside jamb of a secured door. In this instance, the channel used by the signal 108 typically uses a wired medium. However, the code entry module 130 may communicate with the controller 109 via a wireless communication channel used by the signal 108.

The controller 109, database 115 and controlled item 111 are typically located in an inaccessible area such as a hidden roof space or alternately in a suitable protected area such as an armoured cupboard. In the case that a wireless communication channel is used by the signal 108, the location of the controller 109 is of course consistent with reliable reception of the wireless signal 108.

In the case that the code entry module 130 communicates with the controller 109 via a wireless communication channel, the signal 108 may be based upon rolling code. However, it is noted that this is merely one arrangement, and other secure codes can equally be used. Thus, for example, either of the Bluetooth™ protocol, or the Wi Fi™ protocols may be used.

Rolling codes provide a substantially non-replayable non-repeatable and encrypted radio frequency data communications scheme for secure messaging. These codes use inherently secure protocols and serial number ciphering techniques which may be used to hide clear text values required for authentication.

Rolling codes may use a different code variant each time the transmission of the signal 108 occurs. This is achieved by encrypting the data from the code entry module 130 with a mathematical algorithm, and ensuring that successive transmissions of the signal 108 are modified using a code and/or a look-up table known to both the code entry module 130 and the receiver sub-system 117. Using this approach, successive transmissions are modified, resulting in a non-repeatable data transfer, even if the information from the code entry module 130 remains the same. The modification of the

code in the signal 108 for each transmission significantly reduces the likelihood that an intruder can access the information and replay the information to thereby gain entry at some later time.

The biometric signature database 105 is shown in **Fig. 2** to be part of the transmitter sub-system 116. The sub-system 116 may comprise a memory 1006 (see Fig. 6) containing the database 105 of biometric signatures. As described above, the transmitter sub-system 116 including the database 105 may be implemented as a remote fob, where the fob incorporates the biometric (e.g. fingerprint) authentication arrangement. However, in an alternate arrangement, the biometric signature database 105 can be located in the receiver sub-system 117 together with the controller 109, in which case the communication 104 between the biometric module 103 and the signature database 105 can also be performed over a secure wireless communication channel. In the event that the secure access system 100 is being applied to providing secure access to a PC, then the secured PC can store the biometric signature of the authorised user in internal memory, and the PC can be integrated into the sub-system 117 of **Fig. 1**.

The combination of the biometric verification and proximity module 126 in a remote fob provides a particularly significant advantage over current proximity card systems. If the remote fob is lost by the user 101, the lost remote fob may not be used by an unauthorised person to gain the desired access. Further, the security of conventional proximity card systems may be improved without the need to upgrade existing infrastructure.

Fig. 3 shows the method 200 of operation of the transmitter sub-system 116 of **Fig. 2**. The method 200 commences with a testing step 201 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 200 is directed in accordance with a NO

arrow back to the step 201 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 200 is directed in accordance with a YES arrow to a step 202. The step 202 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101 of the transmitter sub-system 116.

A subsequent testing step 203 checks whether the comparison in the step 202 yields the desired authentication. If the biometric signature matching is authenticated, then the method 200 is directed in accordance with a YES arrow to a step 204. In the step 204 the controller 107 sends the signal 112 to the switch module 113 to close the normally open switch 127 to allow the coil 129 to be excited when the proximity card module 126 is placed within range of the code entry module 130. Then at the next step 205, upon the proximity card module 126 being placed within the field of the code entry module 130, the coil 129 is excited and charges the capacitor 131, which in turn energizes the IC 128. The IC 128 then transmits, as depicted by an arrow 132, the card number stored within the IC 128, via the coil, to the code entry module 130. The method 200 is then directed in accordance with an arrow 206 back to the step 201.

Returning to the testing step 203, if the signature comparison indicates that the biometric signal 102 is not authentic, and has thus not been received from the proper user, then the method 200 is directed in accordance with a NO arrow back to the step 201. In an alternate arrangement, the NO arrow from the step 203 could lead to a disabling step which would disable further operation of the transmitter sub-system 116, either immediately upon receipt of the incorrect biometric signal 102, or after a number of attempts to provide the correct biometric signal 102.

Fig. 4 shows the method of operation of the receiver sub-system 117 of **Fig. 2**. The method 300 commences with a testing step 301 which continuously checks whether

the signal 108 including the card number has been received from code entry module 130. The step 301 is performed by the controller 109. As long as the signal 108 is not received the method 300 is directed in accordance with a NO arrow in a looping manner back to the step 301. When the signal 108 is received, the method 300 is directed from the step 301 by means of a YES arrow to a step 302. In the step 302, the controller 109 compares the card number received by means of the signal 108 with one or more card numbers stored in the database 115. A subsequent testing step 303 is performed by the controller 109. In the step 303 if the card number received on the signal 108 is successfully matched against a card number stored in the database 115 then the method 300 is directed in accordance with a YES arrow to a step 304.

In the step 304 the controller 109 sends the control signal 110 to the controlled item 111 (for example opening the secured door). The method 300 is then directed from the step 304 as depicted by an arrow 305 back to the step 301.

Returning to the testing step 303 if the card number received on the signal 108 is not successfully matched against card number stored in the database 115 by the controller 109 then the method 300 is directed from the step 303 in accordance with a NO arrow back to the step 301. As was described in regard to **Fig. 3**, in an alternate arrangement, the method 300 could be directed, if the card number match is negative, from the step 303 to a disabling step which would disable the receiver sub-system 117 if the incorrect card number where received once or a number of times.

In the exemplary embodiment described above, the IC 128 merely stores information in the form of a unique card number. In an alternative embodiment, the IC 128 may be a smart card chip which may be used to store one or more other values as well as the unique card number. Such an embodiment provides particular advantages where the transmitter sub-system 116 is being used to pay for a service. For example, the

IC 128 may further comprise a memory (not shown) containing a "stored value" representing an amount of money where the transmitter sub-system 116 is being used for paying the fare on a bus or other form of public transport.

Fig. 5A shows a method 500 of operation of the transmitter sub-system 116 of **Fig. 2** where the IC 128 is a smart card chip containing a stored value representing an amount of money, in accordance with the alternative embodiment. The method 500 commences with a testing step 501 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 500 is directed in accordance with a NO arrow back to the step 501 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 500 is directed in accordance with a YES arrow to a step 502. The step 502 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101 of the transmitter sub-system 116.

A subsequent testing step 503 checks whether the comparison in the step 502 yields the desired authentication. If the biometric signature matching is authenticated, then the method 500 is directed in accordance with a YES arrow to a step 504. In the subsequent step 504 the controller 107 sends the signal 112 to the switch module 113 to close the normally open switch 127 to allow the coil 129 to be excited when the proximity module 126 is placed within range of the code entry module 130. Then at the next step 505, upon the proximity module 126 being placed within the field of the code entry module 130, the coil 129 is excited and charges the capacitor 131, which in turn energizes the IC 128. The IC 128 then transmits, as depicted by the arrow 132, the card number stored within the IC 128, via the coil, to the code entry module 130.

At the next step 506, the proximity module 126 receives a signal, as depicted by the arrow 133, from the code entry module 130. In the described arrangement, the signal 133 is received via the coil 129 acting as a receive antenna. Then at the next step 507, the IC 128 decrements the stored value by a predetermined amount. This predetermined amount may represent the fare for a trip on a bus, for example. In another alternative embodiment, the signal 133 received from the code entry module 130 may include a value indicating an amount that needs to be decremented from the stored value in step 507. In this instance, the IC 128 decrements the stored value by the amount represented by the value received from the code entry module 130. Accordingly, the stored value is decremented by an amount (i.e., either predetermined or variable) depending on the information (such as the card number) contained in the secure access signal 132 and the proximity module 126 never has to leave the user's hand. Following step 507, the method 500 is then directed in accordance with an arrow 508 back to the step 501.

Fig. 5B shows a method 510 of operation of the receiver sub-system 117 of **Fig. 2** where the IC 128 is the smart card chip containing the stored value of **Fig. 5A**. The method 510 commences with a testing step 511 which continuously checks whether the signal 108 including the card number has been received from code entry module 130. The step 511 is performed by the controller 109. As long as the signal 108 is not received the process 510 is directed in accordance with a NO arrow in a looping manner back to the step 511. When the signal 108 is received, the method 510 is directed from the step 511 by means of a YES arrow to a step 512. In the step 512, the controller 109 compares the card number received by means of the signal 108 with the card numbers stored in the database 115. A subsequent testing step 513 is performed by the controller 109. In the step 513 if the card number received on the signal 108 is successfully matched against a card number stored in the database 115 then the method 510 is directed in accordance

with a YES arrow to a step 514. In the step 514, the controller 109 sends a signal, as represented by arrow 134 of Fig. 2, to the code entry module 130 indicating that the card number was successfully matched.

In the alternative embodiment of Fig. 5A, the amount by which the stored value should be decremented (i.e., the amount of the fare) is predetermined. However, in one arrangement, the amount by which the stored value should be decremented may be variable (e.g., where the fare is variable). In this instance, the signal 134 may include a value representing the value of the fare.

At step 515, if the code entry module 130 determines that the stored value is more than the fare, then the method 510 is directed by a YES arrow to a step 516. The code entry module 130 may read a particular memory address in the IC 128 to determine if the stored value is more than the fare.

At step 516, the code entry module 130 sends the signal 133 to the proximity module 126 to indicate that the stored value should be decremented by the predetermined amount. As described above, the signal 133 may include a value indicating an amount that needs to be decremented from the stored value. At step 516, the code entry module 130 may also send a further signal to the controller 109 which in turn sends a signal 110 to the controlled item 111. In this instance, the controlled item may merely produce an audible tone indicating that the fare has been paid. Alternatively, the controlled item 111 may open a gate or enable a turnstile. The method 510 is then directed from the step 516 as depicted by an arrow 517 back to the step 511.

Returning to the testing step 513 if the card number received on the signal 108 is not successfully matched against card number stored in the database 115 by the controller 109 then the method 510 is directed from the step 513 in accordance with a NO arrow back to the step 511. In this instance, the controller 109 may send a signal 110 to the

controlled item 111 which then sounds an audible alert to indicate that the fare has not been paid.

Returning to the testing step 515, if the code entry module 130 determines that the stored value is less than the fare, then the process 510 is directed from the step 515 in accordance with a NO arrow back to the step 511. Again, in this instance, the controller 109 may send a signal 110 to the controlled item 111 which then sounds an audible alert to indicate that the fare has not been paid.

In the embodiment of **Figs. 5A** and **5B**, the code entry module 130 may include a liquid crystal display (LCD) screen (not shown) for providing feedback to the user 101. In this instance, at step 515, the code entry module 130 may display the amount of the fare as well as the amount of the stored value representing the remaining amount of money on the proximity card module 126.

The transmitter sub-system 116 as described with reference to **Figs. 5A** and **5B** may also be configured to enable value to be added to the stored value. For example, a cash station similar to a train ticket vending machine may be configured with a card reader similar to the code entry module 130. In this instance, upon entering an amount of money into the vending machine (e.g., via a note collector) and providing a biometric request to the bio sensor 121, the proximity module 126 may be placed within the field of the card reader 130 of the vending machine. The card reader 130 may then send a signal to proximity module 126 indicating the value of the money entered into the vending machine and the corresponding amount by which the stored value is to be incremented.

The transmitter sub-system 116 including the switch module 113 and the proximity module 126 may also include an LCD screen (not shown) for providing feedback to the user 101. The LCD screen may be used for displaying information, such as the stored value, stored on the transmitter sub-system 116. In this instance, at step 507

of the method 500, the LCD of the transmitter sub-system 116 may display the amount of the fare as well as the amount of the stored value representing the remaining amount of money stored in the IC of the proximity module 126. In this instance, the LCD and the IC 128 included in the transmitter sub-system 116 may be powered by a battery (e.g., a battery incorporated within the remote fob). In this instance, the user 101 may determine the amount of money remaining on the transmitter sub-system 116 by presenting a biometric request. After the biometric has been authenticated in the manner described above, the amount of the stored value may be displayed on the LCD.

The IC 128 may also be used to store personal details, health records, account balances, personal identification numbers (PIN) and/or other pertinent data. Again, after a biometric has been authenticated in the manner described above, the personal details, medical records, account balances and/or PIN may be displayed on the LCD.

The IC 128 may also be used to store audit trail information so that a record is kept of the date and time that the user 101 attempted to gain access to the controlled item 111.

As will be described in detail below, the ICs such as the IC 128 may also be used to generate a one-time dynamic password for use in online banking applications or the like. If the identity of the user 101 is authenticated successfully upon the user presenting a particular biometric (e.g., an index finger), as described above, then the biometric module 103 sends the signal 106 to the controller 107. The controller 107 may then access a key stored in a key database 113 (not shown) and generate a one-time password using the key and the current time which the controller 107 determines from a clock (not shown). The password may be displayed on the LCD. The password may be generated using the RSA encryption algorithm. However, any suitable encryption algorithm may be used (e.g., Data Encryption Standard (DES), Blowfish, International Data Encryption

Algorithm (IDEA)). The user may then provide the generated password read from the LCD to an authentication server via a personal computer and communications network (see Fig. 11) in order to make an online banking transaction, for example.

The transmitter sub-system 116 of any of the described embodiments may be used in automotive applications where the controlled item 111 is the central locking of a car. The controlled item 111 may also activate or deactivate an engine immobiliser.

The transmitter sub-system 116 of any of the embodiments described may also be used in resort areas, hotels, theme parks or the like. In this instance, the internal operators of the resort areas, hotels and theme parks may issue the transmitter sub-system 116 incorporated within a remote fob, for example, to the user 101. The user 101 may then operate the transmitter sub-system 116 within the confines of the resort, hotel or theme park to enter their room or to have a go on a ride, where the code entry module 130 is mounted on a door jamb or near a gate, respectively.

Any suitable and secure method may be used for populating the user ID database 105 with biometric signatures. Biometric signatures may be added to the user ID database 105 or deleted from the database 105. For example, if a biometric signal has been received by the biometric module 103 and the user ID database 105 in **Fig. 2** is empty, then the received biometric may be treated as an "administrator." This would be the case, for example, if the biometric module 103 is new and has never been used, or if the user 101 has erased all the information in the database 105. The administrator may have the ability to amend data stored, for example, in the database 105. Another type of user may be termed an "ordinary user" and may not have the capability to amend the data stored in the database 105.

The first user of the biometric module 103, whether this is the user who purchases the module, or the user who programs the module 103 after all data has been

erased from the database 105, may be automatically categorised as an administrator. This first administrator may direct the system 100 to either accept further administrators, or alternately to only accept further ordinary users.

Fig. 6 is a schematic block diagram of the system 100' in **Fig. 2**. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in **Fig. 6** wherein the processes of **Figs. 3-5B and Figs. 9, 12** and **14** may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the sub-systems 116 and 117. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part performs the provision of secure access methods and a second part manages a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the sub-systems 116 and 117 from the computer readable medium, and is then executed under direction of the respective processor modules 107 and 109. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for provision of secure access.

The following description is directed primarily to the transmitter sub-system 116, however the description applies in general to the operation of the receiver sub-system 117. The computer system 100' is formed, having regard to the transmitter sub-system

116, by the controller module 107, input devices such as the bio sensor 121, output devices including the LEDs 122, the audio device 124 and the switch module 113.

The controller module 107 typically includes at least one processor unit 1005, and a memory unit 1006, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The controller module 107 also includes a number of input/output (I/O) interfaces including an audio-video interface 1007 that couples to the LED display 122 and audio speaker 124, an I/O interface 1013 for the bio-sensor 121 and the switch module 113. The switch module 113 is connected to the proximity module 126.

The components 1005, 1007, 1013 and 1006 of the controller module 107 typically communicate via an interconnected bus 1004 and in a manner which results in a conventional mode of operation of the controller 107 known to those in the relevant art.

Typically, the application program modules for the transmitter sub-system 116 are resident in the memory 1006 iROM, and are read and controlled in their execution by the processor 1005. Intermediate storage of the program and any data fetched from the bio sensor 121 and a network, for example, may be accomplished using the RAM in the memory 1006. In some instances, the application program modules may be supplied to the user encoded into the ROM in the memory 1006. Still further, the software modules can also be loaded into the transmitter sub-system 116 from other computer readable media (e.g., over a communications network). The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the transmitter sub-system 116 for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external

of the transmitter sub-system 116. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

Figs. 7A and **7B** show an alternate arrangement for enabling the proximity module in **Fig. 2**. **Fig. 7A** shows the proximity arrangement of **Fig. 2**, in which the control signal 112 from the controller 107 of the transmitter sub-system 116 is used to control the switch module 113. When the switch 127 is open, the series circuit comprising the IC 128, the coil 129 and the capacitor 131 is open, and thus the proximity module 126 is disabled and cannot operate when it is brought into the field emitted by the code entry module 130. When the switch 127 is closed, the series circuit comprising the IC 128, the coil 129 and the capacitor 131 is closed, and thus the proximity module 126 is enabled and can perform its designated functions when brought into the field emitted by the code entry module 130. In this arrangement, the control signal 112 can be a simple binary signal, in which for example one voltage level can cause the switch 127 to be in an open state, and another voltage level can cause the switch 127 to be in an open state.

Fig. 7B shows an alternate arrangement 702 in which a proximity module 704 has a series circuit comprising an IC 705, a coil 707 and a capacitor 706 that is permanently closed, and in this arrangement, a control signal 703 controls the operation of the IC 705 directly. In this arrangement, the control signal can in one example comprise a secure encrypted communication session, using multiple layers of security if desired, between the controller 107 (see **Fig. 2**) and the IC 705. In another simpler arrangement, the control signal 703 can be a simple binary signal which merely enables or disables the operation of the IC 705. Upon receiving the signal 112 from the controller 107, the IC 705 remains enabled for a predetermined period of time (e.g., four to five

seconds). Within this period the proximity module 704 is enabled and may be placed by the user 101 within range of a radio frequency field being emitted by a code entry module 130. Although the arrangement of **Fig. 7B** shows one series circuit for each IC 705, other arrangements may be used which share some of the components such as the coils and/or the capacitors.

The communication between the controller 107 and the IC 705 can be implemented using data and/or address bus communications, via a direct bus connection between the controller 107 and the IC 705. Alternatively, the communication between the controller 107 and the IC 705 can be implemented using a contactless communication interface comprising the series circuit of the IC 705, the coil 707 and the capacitor 706. The contactless communication interface between the controller 107 and the IC 705 is a software interface. Any suitable contactless communication interface may be used. In one example, the controller 107 may communicate with the IC 705 according to the Sliding Window Protocol (SWP).

Fig. 8 shows how the secure access system of **Fig. 2** can, using the proximity module arrangement of **Fig. 7B**, support multiple selectable proximity modules (e.g., 806A and 806B). **Fig. 8** shows the biometric module 103 of **Fig. 2** together with the audio transducer 124, the LED indicators 122 and the bio sensor 121. In this arrangement 800 however the biometric module 103 also has a set 801 of control selectors designated selectors 1-4 in the present example for selecting one or more control functions. A greater or smaller number of selectors can be incorporated as desired. Furthermore, the module 103 has an LCD display 802.

According to this arrangement, once the identity of the user 101 is authenticated successfully, the user may select one of the set 801 of the selectors such as the selector designated "1". In response to such a selection, the biometric module 103 sends a signal

803 to the controller 107. Upon receiving the signal 803, the controller 107 sends a control signal on a control line 807A to a corresponding proximity module 806A. Upon receiving the signal 807A from the controller 107, the proximity module 806A remains enabled for a predetermined period of time (e.g., four to five seconds). Within this period the proximity module 806A is enabled and may be placed by the user 101 within range of a radio frequency field being emitted by a code entry module 130. Again, the biometric module 103, the controller 107 and the plurality of the proximity modules (e.g., 806A, 806B) may, for example, be incorporated within a remote fob or mobile telephone, together with the switch module 113 and the user ID database 105. The arrangement of **Fig. 8** can be used to incorporate a number of different ICs (e.g., 705A, 705B) (being the service provider specific elements in the corresponding proximity modules) in a single transmitter sub-system 116, each IC and associated proximity module being associated with a different service provider (such as VISA®, MASTERCARD®, AMERICAN EXPRESS® and so on). This arrangement would enable the user 101, after biometric authentication, to select the appropriate service provider by pressing the appropriate selector in the set 801 of selectors, and to then bring the corresponding proximity module 806A into the field emitted by the code entry module 130. In fact, all of the proximity modules incorporated into the transmitter sub-system 116 are being brought into the field emitted by the code entry module 130 however only the desired proximity module 806A is enabled by the signal 803.

The LCD display 802 can show the user 101 which service provider has been selected, thereby confirming to the user that the desired service provider has been selected. The display 802 can be provided before the user places the proximity module (e.g., 806A) into the field emitted by the corresponding code entry module 130.

In a more general case, the various selectable proximity modules (e.g., 806A, 806B) can be associated with service providers from diverse fields, namely financial, security, automotive, individual identification and so on, and can have different interfaces with the respective code entry modules such as 130. Therefore, the ICs 705A, 705B configured within the proximity modules 806A, 806B may include a combination of ICs such as the known HID™ proximity IC, iCLASS IC, and Mifare™ IC, each for a distinct application and using a different interface. The user 101 may select the desired application using the set 801 of selectors, and optionally can receive feedback on the selection via the LCD display 802.

Security and payment functionality may be combined using one or more iterations of authentication and selection, thus facilitating operation with existing infrastructure. For example, the proximity module 806A and corresponding IC 705A may contain a stored unique number for use in secure access and the proximity module 806B and corresponding IC 705B may contain a stored value for use in making cashless payments as described above.

The controller 107 may also be configured to generate a one-time dynamic "time-dependent" or "event-synchronous" password. Upon authentication of a user's biometric as described above with reference to Fig 3, the controller 107 may access a key stored in a database (e.g., the database 115). The controller 107 may then generate a one-time time-dependent password using the key and the current time (as a dynamic input value), for example. The current time may be determined from a computer clock (not shown) configured within the arrangement 800 of Fig. 8. The password may be generated using the RSA encryption algorithm or any other suitable encryption algorithm (e.g., Data Encryption Standard (DES), Blowfish, International Data Encryption Algorithm (IDEA)).

Accordingly, a password may be generated using the current time as the input value to the encryption process. It is noted that this is merely one arrangement, and other input values such as a simple counter value or a random number may be used as with event-synchronous tokens and asynchronous challenge/response tokens. Further, other mathematical algorithms or codes can equally be used to generate the one-time password. For example, the password may be generated using a rolling code to generate a different code variant each time the password is generated. In this instance, successive passwords may be generated using a code and/or a look-up table known to both the code entry module 103 and receiver sub-system 117. Using this approach successive numbers are modified, resulting in a non-repeatable number.

The user 101 may make a payment (e.g., a VISA® payment) at a conventional (i.e., not using the proximity module) payment terminal or online by selecting the appropriate selector from the set 801, then pressing a suitable combination of the selectors 801 as guided by a display on the LCD screen 802 and waiting for a one-time password to be generated and shown on the display 802. The password may then be manually entered into the keyboard of the payment terminal or personal computer. This approach supports applications including business-to-business on line payments through to standard contact-less payments at existing payment terminals.

Fig. 9 shows a method 900 of operation of the arrangement 800 of **Fig. 8** according to one example. In the example of **Fig. 9**, the user 101 generates a dynamic password using the arrangement 800 of **Fig. 8**. The dynamic password may then be used for making an online payment to a business website. In the present example, the online payment is being made using a VISA® account. The example provides a secure scenario as a reference to a typical transaction. However, variations of the steps of the methods described below including input from the user 101, biometric reads, generation

of dynamic passwords, display of current account balances, can be used to conduct various transactions.

The method 900 of **Fig. 9** may be implemented as software, such as application program modules being controlled in their execution by the controller 107 and being resident in the memory 1006 of the controller 107. The method 900 commences with a testing step 901 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 900 is directed in accordance with a NO arrow back to the step 901 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 900 is directed in accordance with a YES arrow to a step 902. The step 902 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101.

A subsequent testing step 903 checks whether the comparison in the step 902 yields the desired authentication. If the biometric signature matching is authenticated, then the method 900 is directed in accordance with a YES arrow to a step 904. At step 904, the controller 107 detects selection of one of the selectors of the set 801. In the present example, the selector "1" of the set 801 is selected. In response to selection of the selector "1", at the next step 905, the controller 107 displays the value, stored on one of the ICs, representing available funds. In the present example, the IC 705A is a VISA® IC for making VISA® card payments and comprises the stored value. The value is displayed on the LCD 802. In the present example, the controller 107 displays $156.56 which represents the balance of the user's VISA™ account.

At the next step 906, if within a predetermined period of time (e.g., 30 seconds) the controller 107 again detects selection of the same selector (i.e., selector "1") of the set 801, then the method 900 is directed in accordance with a YES arrow to a step 907.

Otherwise, the method 900 is directed in accordance with a NO arrow to the step 901. At step 907, the controller 107 generates a dynamic password (i.e., a first dynamic password), using the RSA encryption algorithm, as described above. The dynamic password is displayed on the LCD 802.

In the present example, the dynamic password generated at step 907 is "2 3 4 9 8 7 8 9". The dynamic password will be different each time it is generated. The dynamic password may be a time-dependent password where the current time is used as the input value to the encryption process. The available funds and the unique token serial number are also preferably encrypted with the generated password. Alternatively, the dynamic password may be an event-synchronous password.

In accordance with the present example, the first dynamic password generated and displayed by the controller 107 at step 907 is entered into a computer module 1101 of a computer system 1100 as shown in Fig. 11, in order to make the online payment to the business website. The online payment is made in accordance with a method 1000 of making an online payment, which will be described in detail below with reference to Fig. 10. The method 1000 may be may be implemented using the computer system 1100, wherein the process of Fig. 10 may be implemented as software, such as one or more application programs executable within the computer system 1100. In particular, the steps of method 1000 may be effected by instructions in the software that are carried out within the computer system 1100. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part and the corresponding code modules performs the method 1000 and a second part and the corresponding code modules manage a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example.

One or more portions of the software may be stored within the computer module 1101 and also on a remote server 1150, as will be described below. The software is loaded into the computer system 1100 from the computer readable medium, and then executed by the computer system 1100. A computer readable medium having such software or computer program recorded on it is a computer program product as described above. The use of the computer program product in the computer system 1100 preferably effects an advantageous apparatus for implementing the method 1100.

As seen in Fig. 11, the computer system 1100 is formed by a computer module 1101, input devices such as a keyboard 1102 and a mouse pointer device 1103, and output devices including a printer 1115, a display device 1114 and loudspeakers 1117. An external Modulator-Demodulator (Modem) transceiver device 1116 may be used by the computer module 1101 for communicating to and from a communications network 1120 via a connection 1121. The network 1120 may be a wide-area network (WAN), such as the Internet or a private WAN. Where the connection 1121 is a telephone line, the modem 1116 may be a traditional "dial-up" modem. Alternatively, where the connection 1121 is a high capacity (e.g.: cable) connection, the modem 1116 may be a broadband modem. A wireless modem may also be used for wireless connection to the network 1120.

In accordance with the present example, a server 1150 hosting a payments website (e.g., a utility website such as the phone company or bank website) is connected to the network 1120.

The computer module 1101 typically includes at least one processor unit 1105, and a memory unit 1106 for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The module 1101 also includes an number of input/output (I/O) interfaces including an audio-video interface 1107 that couples to the

video display 1114 and loudspeakers 1117, an I/O interface 1113 for the keyboard 1102 and mouse 1103 and optionally a joystick (not illustrated), and an interface 1108 for the external modem 1116 and printer 1115. In some implementations, the modem 1116 may be incorporated within the computer module 1101, for example within the interface 1108. The computer module 1101 also has a local network interface 1111 which, via a connection 1123, permits coupling of the computer system 1100 to a local computer network 1122, known as a Local Area Network (LAN). As also illustrated, the local network 1122 may also couple to the wide network 1120 via a connection 1124, which would typically include a so-called "firewall" device or similar functionality. The interface 1111 may be formed by an Ethernet™ circuit card, a wireless Bluetooth™ or an IEEE 802.11 wireless arrangement.

The interfaces 1108 and 1113 may afford both serial and parallel connectivity, the former typically being implemented according to the Universal Serial Bus (USB) standards and having corresponding USB connectors (not illustrated). Storage devices 1109 are provided and typically include a hard disk drive (HDD) 1110. Other devices such as a floppy disk drive and a magnetic tape drive (not illustrated) may also be used. An optical disk drive 1112 is typically provided to act as a non-volatile source of data. Portable memory devices, such optical disks (e.g.: CD-ROM, DVD), USB-RAM, and floppy disks for example may then be used as appropriate sources of data to the system 1100.

The components 1105 to 1113 of the computer module 1101 typically communicate via an interconnected bus 1104 and in a manner which results in a conventional mode of operation of the computer system 1100 known to those in the relevant art. Examples of computers on which the described arrangements can be practised include IBM-PC's and

compatibles, Sun Sparcstations, Apple Mac™ or alike computer systems evolved therefrom.

Typically, the application program(s) implementing the method 1000 are resident on the hard disk drive 1110 and read and controlled in execution by the processor 1105. Intermediate storage of such programs and any data fetched from the networks 1120 and 1122 may be accomplished using the semiconductor memory 1106, possibly in concert with the hard disk drive 1110. In some instances, the application programs may be supplied to the user encoded on one or more CD-ROM and read via the corresponding drive 1112, or alternatively may be read by the user from the networks 1120 or 1122. Still further, the software can also be loaded into the computer system 1100 from other computer readable media. Computer readable media refers to any storage medium that participates in providing instructions and/or data to the computer system 1100 for execution and/or processing. Examples of such media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computer module 1101. Examples of computer readable transmission media that may also participate in the provision of instructions and/or data include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

The second part of the application programs and the corresponding code modules mentioned above may be executed to implement one or more graphical user interfaces (GUIs) to be rendered or otherwise represented upon the display 1114. Through manipulation of the keyboard 1102 and the mouse 1103, a user of the computer system

1100 and the application may manipulate the interface to provide controlling commands and/or input to the applications associated with the GUI(s).

The method 1000 may alternatively be implemented in dedicated hardware such as one or more integrated circuits performing the functions or sub functions of Fig. 10. Such dedicated hardware may include graphic processors, digital signal processors, or one or more microprocessors and associated memories.

The method 1000 begins at step 1010, where after receiving the first password entered by the user 101, the method 1000 proceeds to step 1011. At step 1011, the password is transmitted by the processor 1105 to the server 1150 hosting the payments website. Then at the next step 1012, the server 1150 verifies the password entered by the user 101 by generating another dynamic password and comparing the passwords. In order to generate the password, the server 1150 accesses a key (associated with the user 101 of the code module 103) stored in a key database 1151 and determines the current time from a system clock 1152. In the present example, the key database 1151 may be configured within a hard disk drive (not shown) of the server 1150. The server 1150 generates the password using the key and the current time determined by encrypting a value representing the current time, using the RSA encryption algorithm, which is the same encryption algorithm used by the controller 107. Also at step 1012, the server 1150 determines available funds (i.e. $156.56) by determining the amount from the password entered by the user 101.

Once the dynamic password is entered into the computer module 1101 and verified by the server 1150, the user 101 makes another request using the arrangement of **Fig. 8** in order to select the amount of funds wishing to be debited from their account. The amount of funds selected by the user 101 is then debited from the value stored on the

IC (e.g., 705A) corresponding to their account. **Fig. 12** shows a method 1200 of debiting an amount of funds from an account.

The method 1200 commences at step 1201, where the controller 107 detects selection of another one of the selectors of the set 801. In the present example, the selector "2" of the set 801 is selected. In response to selection of the selector "2", at the next step 1202, the controller 107 prompts the user 101 to enter the amount that they wish to pay which also represents the amount to be debited from their account (i.e. their VISA® account).

At the next step 1203, the controller 107 determines the amount wished to be payed based on an amount entered by the user 101 and displays this amount on the LCD 802. The user may enter the amount using the set of control selectors 801. For example, the controller 107 may display a generic amount and the user may select "3" of the set 801 to increase a displayed amount and "4" to decrease the displayed amount.

The next step 1204 is a testing step in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 1200 is directed in accordance with a NO arrow back to the step 1206 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 1200 is directed in accordance with a YES arrow to a step 1205. The step 1205 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received is that of the rightful user 101.

A subsequent testing step 1206 checks whether the comparison in the step 1205 yields the desired authentication. If the biometric signature matching is authenticated, then the method 1200 is directed in accordance with a YES arrow to a step 1207. At step 1207, the controller 107 generates a second dynamic password, using the RSA encryption

algorithm with the current time being used as the input value to the encryption process, as described above. The dynamic password is displayed on the LCD 802. In the present example, the dynamic password generated at step is "5 6 8 8 8 1 8 9". Again, the second dynamic password is a time-dependent password. However, the second password may also be an event-synchronous password. The amount determined at step 1203 representing the amount of funds to be payed is also encrypted within the dynamic password. The method 1200 concludes at the next step 1208, where the amount of funds entered by the user at step 1203 is deducted from the value stored on the IC 705A.

In accordance with the present example, the second dynamic password generated and displayed by the controller 107 at step 1207 is entered into the computer module 1101 to complete the online payment to the business website.

Returning to **Fig. 10**, at the next step 1013, after receiving the second dynamic password entered by the user 101, the method 1000 proceeds to step 1014. At step 1014, the second password is transmitted by the processor 1105 to the server 1150 hosting the payments website. Then at the next step 1015, the server 1150 verifies the password entered by the user 101 by generating still another dynamic password and comparing the passwords as described above. In order to generate this still further password, the server 1150 accesses the key (associated with the user 101 of the code module 103) stored in the key database 1151 and determines the current time from the system clock 1152, as described above. Also at step 1015, the server 1150 determines the amount to be paid by decrypting the amount from the second password entered by the user 101.

The method 1000 concludes at the next 1016, where the payment is processed by the server 1150. The payment transaction can be reconciled to the customer in a monthly statement.

Variations on the methods described above can also be used for secure access, for example, to gain entry to a building. For example, the dynamic password generated at step 907 may be entered into a keypad located on a door jamb and being connected to a building security system. In this instance, rather than representing an account balance, the stored value encrypted within the dynamic password can be a personal identification number (PIN) stored with the transmitter sub-system 116. The building security system then verifies the password entered by the user 101 by generating another dynamic password and comparing the passwords. Thus, the PIN used for secure access is enhanced through the need of a biometric signature.

The dynamic passwords generated at step 907 may have other user information encrypted within the dynamic password including a serial number related to the transmitter sub-system (configured within a telephone or fob), time of access, type of account and validated finger (e.g., middle finger).

The arrangement of **Fig. 8** comprises multiple selectable proximity modules (e.g., 806A, 806B) each configured in accordance with the arrangement of **Fig. 7B**. In an alternative arrangement, one antenna (e.g., 707) may be associated with multiple ICs (e.g., all connected in parallel with the antenna). Again, in this instance, each of the ICs may be separately selectable using separate control lines (e.g., 807A, 807B).

Fig. 13 shows how the secure access system of **Fig. 2** can, using one or more conventional proximity modules, be used to perform a secure transaction. **Fig. 13** shows the biometric module 103 of **Fig. 2** together with the audio transducer 124, the LED indicators 122 and the bio sensor 121, and a set 1301 of control selectors designated selectors 1-4 in the present example for selecting one or more control functions. The module 103 also has an LCD display 802. The arrangement 1300 also has a proximity

module 1306. The proximity module 1306 comprises the coil 129, the capacitor 131 and an IC 1307.

In the arrangement 1300 of **Fig. 13**, the proximity module 1306 is configured to be constantly available to be activated, upon being placed within the field of the code entry module 130 in a conventional manner, without the need for a control signal such as the control signal 803. That is, no biometric verification is required in the arrangement 1300 in order to activate the proximity module 1306.

The arrangement 1300 may also be used to perform secure transactions or the like, including an online transaction. Rather than the biometric verification being needed in order to activate the proximity module 1306, the generation of a dynamic password, as described above, may be utilised to provide an additional security layer, as will be described below.

A method 1400 of performing a transaction using the arrangement 1300 of **Fig. 13** will now be described with reference to **Fig. 14**. The method 1400 begins with a testing step 1401 in which the biometric sensor 121 in the code entry module 103 checks whether a biometric signal 102 is being received. If this is not the case, then the method 1400 is directed in accordance with a NO arrow back to the step 1401 in a loop. If, on the other hand, the biometric signal 102 has been received, then the method 1400 is directed in accordance with a YES arrow to a step 1402. The step 1402 compares the received biometric signal 102 with information in the biometric signature database 105 in order to ensure that the biometric signal received 102 is that of the rightful user 101.

A subsequent testing step 1403 checks whether the comparison in the step 1402 yields the desired authentication. If the biometric signature matching is authenticated, then the method 1400 is directed in accordance with a YES arrow to a step 1404 where the match is indicated to the user 101 on the display 802. Also at step 1404, the controller

107 detects selection of one of the selectors of the set 801. In the present example, the selector "1" of the set 801 is selected by the user 101. In response to selection of the selector "1", at the next step 1405, the controller 107 generates a dynamic password, using the RSA encryption algorithm, as described above, and displays the dynamic password on the LCD 802. The dynamic password is generated based on a card number (associated with the user) stored on the IC 1307. In the present example, the dynamic password generated at 1405, is entered into a keypad or the like (not shown) associated with the code entry module 130. The card number may be encrypted within the dynamic password.

Then at the next step 1406, upon the proximity module 1306 being placed within the field of the code entry module 130, the coil 129 is excited and charges the capacitor 131, which in turn energizes the IC 1307. The IC 1307 then transmits, as depicted by an arrow 1332, the card number stored within the IC 1307, via the coil 1306, to the code entry module 130. A controller (e.g., 109) associated with the code entry module 130 then uses the card number to verify the dynamic password as described above. In particular, the controller of the code entry module 130 generates a dynamic password, using the RSA encryption algorithm, using the card number, and compares the generated password to the password entered by the user 101. Again, the passwords generated at step 1405 and by the controller may be time-dependent or event-synchronous.

At the next step 1406, the proximity module 1306 receives a signal, as depicted by the arrow 1333, from the code entry module 130. Then at the next step 1407, the IC 1307 decrements the stored value by a predetermined amount. This predetermined amount may represent a payment for a trip on a bus, for example. In another alternative embodiment, the signal 1333 received from the code entry module 130 may include a value indicating an amount that needs to be decremented from the stored value in step

1407. In this instance, the IC 1307 decrements the stored value by the amount represented by the value received from the code entry module 130. Accordingly, the stored value is decremented by an amount (i.e., either predetermined or variable) depending on the information (such as the card number) contained in the secure access signal 132 and the proximity module 126 never has to leave the user's hand. Following step 1407, the method 1400 is then directed in accordance with an arrow 1408 back to the step 1401.

Accordingly, in the example of **Figs. 13** and **14**, the dynamic password generated on the basis of a valid biometric reading, is used to verify the user of the arrangement 1300. Although in the example of **Figs. 13** and **14**, the dynamic password was generated first, in alternative arrangements the dynamic password may follow or accompany a payment.

The arrangements described above, including the arrangement 1300 of **Fig. 13**, may also be used with automatic teller machines (ATMs) or point of sale (POS) devices where a personal identification number (PIN) has conventionally been used to verify the validity of a card (i.e., magnetic stripe card or smart card) owner. The dynamic password generated on the basis of a valid biometric reading may be used to replace such a PIN, without affecting a conventional transaction. For example, in the case of an ATM transaction or electronic funds transfer point of sale (EFTPOS) transaction, a user inserts their magnetic stripe card (or smart card) into the ATM or swipes the card using an EFTPOS terminal. A card number corresponding to the magnetic stripe card is stored on the IC 1307. At the same time as inserting or swiping their card, the user may use the arrangement 1300 described above to generate a time-dependent or event-synchronous dynamic password based on a valid biometric reading. Again, the card number corresponding to the magnetic stripe card may be encrypted within the generated

password. The user then enters the generated dynamic password into the ATM or EFTPOS terminal. The dynamic password is then verified by a back-end host server (e.g., associated with a bank) in the manner described above based on the card number.

The arrangements described above, including the arrangement 1300 of **Fig. 13**, may also be used for making an online payment. Again, the dynamic password may be used to replace the user's password which has conventionally been used. At the same time as logging into a banking website, for example, the user may use the arrangement 1300 described above to generate a time-dependent or event-synchronous dynamic password based on a valid biometric reading. Again, a user identification number corresponding to the user may be encrypted within the generated password. The user then enters the generated dynamic password into a personal computer. The dynamic password is then verified by a back-end host server (e.g., associated with a bank) connected to the personal computer in the manner described above based on the user's identification number encrypted with the entered password.

The arrangements described above, including the arrangement 1300 of **Fig. 13** may stop intruders from stealing credit and debit cards for later fraudulent use in ATM and POS devices. The owner or user of a magnetic stripe card would also require the fob or mobile telephone with the card number corresponding to the magnetic stripe card stored thereon. A new dynamic password could then be generated for each ATM or EFTPOS transaction. The dynamic password overcomes the inherent weaknesses in PIN type inputs, due to the dynamic nature of the password and requirement to validate the owner or user biometrics prior to generating that password. If an intruder views a dynamic password input, they cannot replicate it a next time as the password is constantly changing.

Although the arrangement 1300 of **Fig. 13** has been described as including the proximity module 1307, the arrangement 1300 may not necessarily include such proximity module 1307. An arrangement without a proximity module may also be used to perform the transactions described above including ATM, EFTPOS and online transactions merely by generating a dynamic password as described above.

The arrangements described above allow biometric security to be easily integrated with existing infrastructure for payment or access systems. The arrangements are simple and effective for secure proof of identity. The user does not need to remember a code, number, name or combination. The arrangements may be used online or offline. The described arrangements may also be used in wireless systems, alarm panel activation, garage control, door access, boom-gate access and anywhere long distance secure transmissions are required.

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the security industry.

The foregoing describes only some embodiments of the present invention, 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.

The system 100 can also be used to provide authorised access to lighting systems, building control devices, exterior or remote devices such as air compressors and so on. The system 100 may also be used to gain access to online applications. For example, as described above, the transmitter sub-system 116 may be used to generate a one-time dynamic password for use in online banking applications or the like. The concept of "secure access" is thus extendible beyond mere access to restricted physical areas.

Although the present specification has described communication between the transmitter sub-system 116 and the receiver sub-system being performed using RF, other communication modes such as capacitive coupling or infra-red could also be used.

The arrangements described above may comprise a "duress" or "alarm" feature. This feature may be activated using a different predetermined biometrics. For example, typically the user may present a particular finger (e.g., their thumb) for verification prior to enabling the proximity module (e.g., 126) or generating a dynamic password. If the valid user is under duress by an intruder, the valid user can use an alternate finger (e.g., their index finger) to enable the proximity module and/or generate a dynamic password, for example. Use of the alternate finger may automatically activate an alarm, thereby bringing emergency services to the situation. Alternatively, the dynamic password generated based on the alternate finger may include an encrypted alarm notification. In this instance, when the generated password is entered into a keypad, keyboard or the like, an alarm will be automatically activated by a backend controller or server, again bringing the emergency services to the location.

Generating different dynamic passwords based on the verification of different biometrics may also be used where multiple access areas are selectable from a single point. For example, the arrangements described above (e.g., the arrangement 1300) may be configured so that a user's thumb may be read and verified, as described above, in order to generate a first dynamic password. The first password may be entered into a keypad, for example, to allow the user to enter a first door "1". The user may then present a different finger (e.g., the person's index finger) which once verified may result in the generation of a second dynamic password. The second password may be entered into a keypad, for example, to allow the user to enter a second door "2".

Claims:

1. A transmitter for transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the transmitter comprising:

a biometric sensor for receiving a biometric signal;

a processor for matching the biometric signal against members of a database of biometric signatures; and

enabling means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

2. The transmitter according to claim 1, further comprising a memory containing the database of biometric signatures.

3. The transmitter according to claim 1, wherein the database of biometric signatures is located in the system for providing secure access to the controlled item.

4. The transmitter according to any one of claims 1 to 3, further comprising the inductive circuit.

5. The transmitter according to claim 4, wherein the inductive circuit further comprises a capacitor.

6. The transmitter according to any one of claims 4 or 5, wherein the inductive circuit further comprises an integrated circuit.

7. The transmitter according to any one of claims 1 to 6, wherein the secure access signal is transmitted via the inductive circuit.

8. The transmitter according to any one of claims 1 to 7, further comprising a display for displaying information stored on the transmitter.

9. The transmitter according to any one of claims 1 to 8, further comprising a memory for storing a value.

10. The transmitter according to claim 9, wherein the stored value is decremented by an amount depending on the information.

11. The transmitter according to any one of claims 1 to 10, wherein the transmitter further comprises means for populating the database of biometric signatures.

12. The transmitter according to any one of claims 1 to 11, wherein the biometric sensor is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration.

13. The transmitter according to any one of claims 1 to 12, wherein the controlled item is a locking mechanism of a door

14. The transmitter according to any one of claims 1 to 12, wherein the controlled item is an electronic lock on a Personal Computer (PC).

15. The transmitter according to any one of claims 1 to 14, wherein the transmitter is incorporated within a fob.

16. A method of transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the method comprising:

receiving a biometric signal;

matching the biometric signal against members of a database of biometric signatures; and

enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

17. The method according to claim 16, further comprising the step of storing a value associated with the inductive circuit.

18. The method according to claim 17, further comprising the step of decrementing the stored value by an amount depending on the information.

19. The method according to claim 17, further comprising the step of providing conditional access to the controlled item dependent upon said information.

20. A computer program product having a computer readable medium having a computer program recorded therein for transmitting a secure access signal to a system for providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the program comprising:

code for receiving a biometric signal;

code for matching the biometric signal against members of a database of biometric signatures; and

code for enabling an inductive circuit, based on the matching of the biometric signal, to transmit the secure access signal conveying the information to the system upon the inductive circuit being placed within range of a radio frequency field emitted by the system.

21. A system for providing secure access to a controlled item, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures; and

means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying information upon the inductive circuit being placed within range of a radio frequency field; and

a receiver sub-system comprising;

means for emitting the radio frequency field;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the controlled item dependent upon said information.

22. A transmitter sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a receiver sub-system comprising means for emitting a radio frequency field, means for receiving a secure access signal transmitted by the transmitter sub-system, and means for providing conditional access to the controlled item dependent upon information conveyed in the secure access signal; wherein the transmitter sub-system comprises:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures; and

means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying said information upon the inductive circuit being placed within range of the radio frequency field.

23. A receiver sub-system for operating in a system for providing secure access to a controlled item, the system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, means for matching the biometric signal against members of the database of biometric signatures, and means for enabling an inductive circuit, based on the matching of the biometric signal, to transmit a secure access signal conveying information; wherein the receiver sub-system comprises:

means for emitting a radio frequency field;

means for receiving the transmitted secure access signal from the transmitter sub-system upon the inductive circuit being placed within range of a radio frequency field; and

means for providing conditional access to the controlled item dependent upon said information.

24. A system for providing secure access to one of a plurality of controlled items, the system comprising:

a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor for receiving a biometric signal;

means for determining if the received biometric signal matches a member of the database of biometric signatures;

a plurality of proximity modules associated with the plurality of controlled items;

means for selecting one of said plurality of proximity modules; and

means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module; and

a receiver sub-system comprising;

means for emitting said radio frequency field adapted to activate the selected proximity module;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the selected controlled item dependent upon said information.

25. The system according to claim 24, wherein the means for enabling the selected proximity module comprises means for communicating an enabling signal to the integrated circuit of the proximity module.

26. The system according to claim 24, wherein said transmitter sub-system further comprises means for generating a dynamic password.

27. The system according to claim 26, wherein access to the controlled item is dependent upon the dynamic password being authenticated by the receiver sub-system.

28. The system according to claim 24, wherein the transmitter sub-system is configured within a fob.

29. The system according to claim 24, wherein the transmitter sub-system is configured within a mobile telephone.

30. The system according to claim 24, wherein the receiver sub-system is a payment system.

31. The system according to claim 30, wherein the payment system is an online payment system.

32. A transmitter for transmitting a secure access signal to a system for providing secure access to one of a plurality of controlled items, said access being dependent on information contained in the secure access signal, the transmitter comprising:

a biometric sensor for receiving a biometric signal;

means for determining if the received biometric signal matches a member of a database of biometric signatures;

a plurality of proximity modules associated with the plurality of controlled items;

means for selecting one of said plurality of proximity modules; and

means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

33. The transmitter according to claim 32, further comprising a memory containing the database of biometric signatures.

34. The transmitter according to claim 32, further comprising means for generating a dynamic password.

35. The transmitter according to claim 34, wherein access to at least one of the controlled items is dependent upon the dynamic password being authenticated.

36. The transmitter according to claim 32, wherein the transmitter is configured within a fob.

37. The transmitter according to claim 32, wherein the transmitter is configured within a mobile telephone.

38. A receiver sub-system in a system for providing secure access to one of a plurality of controlled items, the system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, means for determining if the received biometric signal matches a member of the database of biometric signatures, a plurality of proximity modules associated with the plurality of controlled items, means for selecting one of said plurality of proximity modules, and means for enabling, if the received biometric signal matches a member of the database of biometric signatures, the selected proximity module which can consequently transmit a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module; said receiver sub-system comprising:

means for emitting said radio frequency field adapted to activate the selected proximity module;

means for receiving the transmitted secure access signal upon the radio frequency field being emitted; and

means for providing conditional access to the selected controlled item dependent upon said information.

39. A system for performing a secure transaction, the system comprising:

a database of one or more biometric signatures;

a first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating a first password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing funds available; and

a second sub-system comprising;

means for receiving the first password;

means for determining the funds available based on the received password; and

means for performing the transaction based on the available funds.

40. The system according to claim 39, said transmitter sub-system further comprising means for generating a second password dependent upon a further authentication signal, said second password being generated according to an encryption process based on a dynamic input value, said second password comprising an encrypted value representing funds to be debited.

41. A first sub-system for operating in a system for performing a secure transaction, the system comprising a database of biometric signatures, a second sub-system comprising means for receiving a password, and means for performing the secure

transaction based on available funds dependent upon the password, the first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating the password dependent upon said authentication signal, wherein said password is generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing said funds available.

42. A system for performing a secure transaction over a network using a card, the system comprising:

a database of one or more biometric signatures;

a first subsystem comprising:

a biometric sensor for receiving a biometric signal;

means for matching the biometric signal against members of the database of biometric signatures to thereby determine an authentication signal; and

means for generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said first password comprising an encrypted value representing said magnetic stripe card; and

a second sub-system comprising;

means for reading the card;

means for receiving the password;

means for authenticating the received password based on the card number encrypted within password; and

means for performing the transaction based on the authentication.

43. A method of transmitting a secure access signal to a system for providing secure access to one of a plurality of controlled items, said access being dependent on information contained in the secure access signal, the method comprising the steps of:

receiving a biometric signal;

matching the biometric signal to a member of a database of biometric signatures;

selecting one of a plurality of proximity modules, the selected proximity module being associated with at least one of the plurality of controlled items; and

enabling the selected proximity module, if the received biometric signal matches a member of the database of biometric signatures, the enabled selected proximity module being configured for transmitting a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

44. The method according to claim 43, further comprising the step of storing a value associated with the inductive circuit.

45. The method according to claim 44, further comprising the step of decrementing the stored value by an amount depending on the information.

46. The method according to claim 43, further comprising the step of providing conditional access to the controlled item dependent upon said information.

47. A method of performing a secure transaction over a network using a card, the method comprising:

matching a biometric signal against members of a database of biometric signatures to thereby determine an authentication signal; and

generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said password comprising an encrypted number representing said card;

reading the card to determine the card number from said card;

authenticating a received password based on the card number encrypted within password; and

performing the transaction based on the authentication.

48. The method according to claim 47, further comprising the step of determining an amount of funds.

49. The method according to claim 48, further comprising the step of debiting an amount based on the determined amount of funds.

50. The method according to claim 47, further comprising the step of decrementing a value stored on the card based on the determined amount of funds.

51. A computer program product having a computer readable medium having a computer program recorded therein for transmitting a secure access signal to a system for

providing secure access to a controlled item, said access being dependent on information contained in the secure access signal, the program comprising:

code for receiving a biometric signal;

code for matching the biometric signal to a member of a database of biometric signatures;

code for selecting one of a plurality of proximity modules, the selected proximity module being associated with at least one of the plurality of controlled items; and

code for enabling the selected proximity module, if the received biometric signal matches a member of the database of biometric signatures, the enabled selected proximity module being configured for transmitting a secure access signal conveying information stored in the selected proximity module upon the proximity module being placed within range of a radio-frequency field adapted to activate the selected proximity module.

52. A computer program product having a computer readable medium having a computer program recorded therein for performing a secure transaction over a network using a card, the program comprising:

code for matching a biometric signal against members of a database of biometric signatures to thereby determine an authentication signal; and

code for generating a password dependent upon said authentication signal, said password being generated according to an encryption process based on a dynamic input value, said password comprising an encrypted number representing said card;

code for reading the card to determine the card number from said card;

code authenticating a received password based on the card number encrypted within password; and

code for performing the transaction based on the authentication.

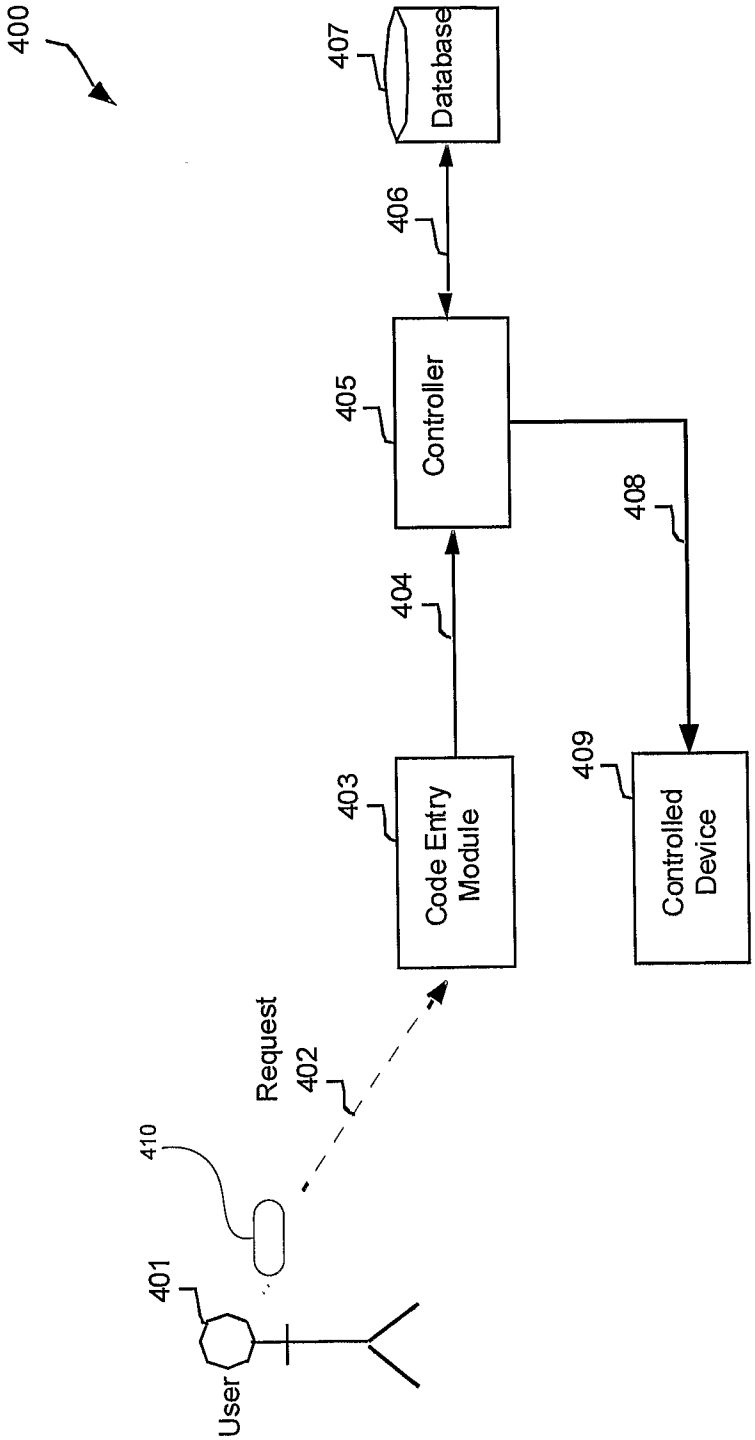
400
407
Database
406
405
Controller
408
404
403
Code Entry Module
409
Controlled Device
Request
402
410
401
User

Fig. 1

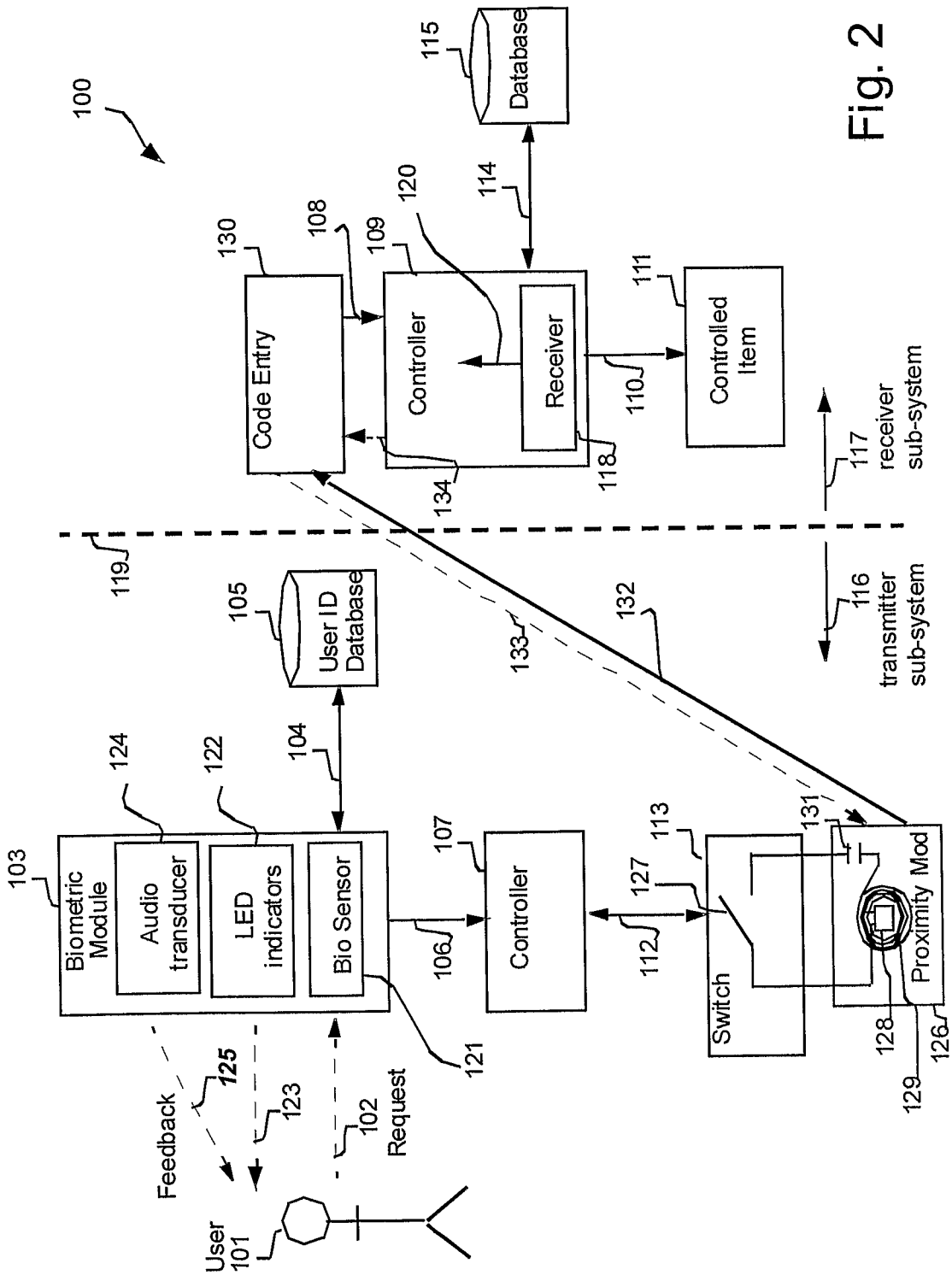
100
115
Database
114
120
130
108
109
Code Entry
Controller
Receiver
111
Controlled Item
110
118
134
117
receiver sub-system
119
116
transmitter sub-system
105
User ID Database
132
133
104
124
122
103
Biometric Module
Audio transducer
LED indicators
Bio Sensor
107
Controller
106
121
127
113
131
112
Switch
Proximity Mod
128
129
126
Feedback
125
123
102
Request
User
101

Fig. 2

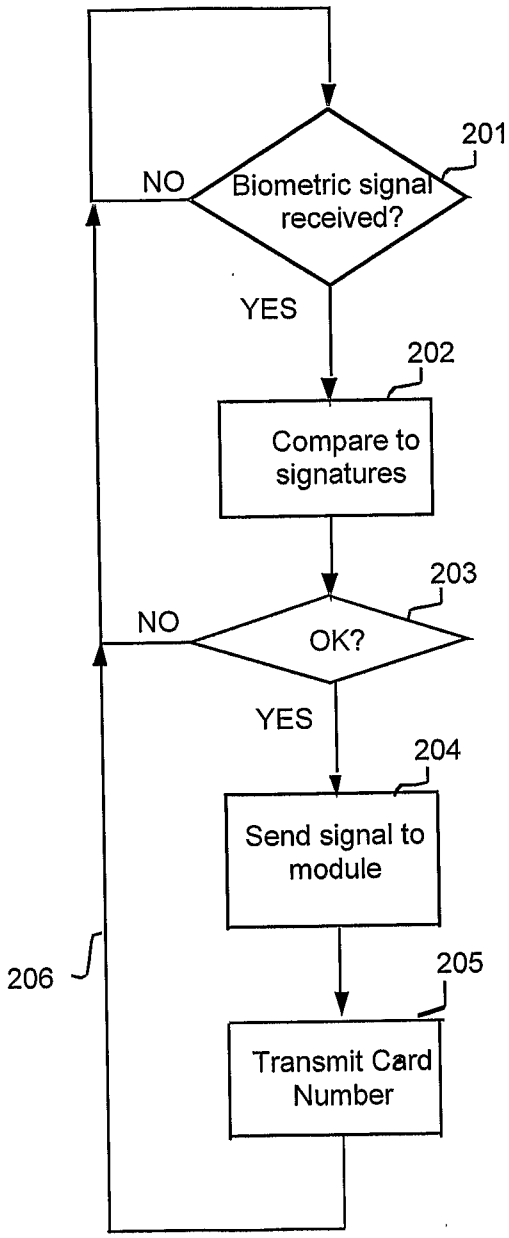
200
201
Biometric signal received?
NO
YES
202
Compare to signatures
203
OK?
NO
YES
204
Send signal to module
205
Transmit Card Number
206

Fig. 3

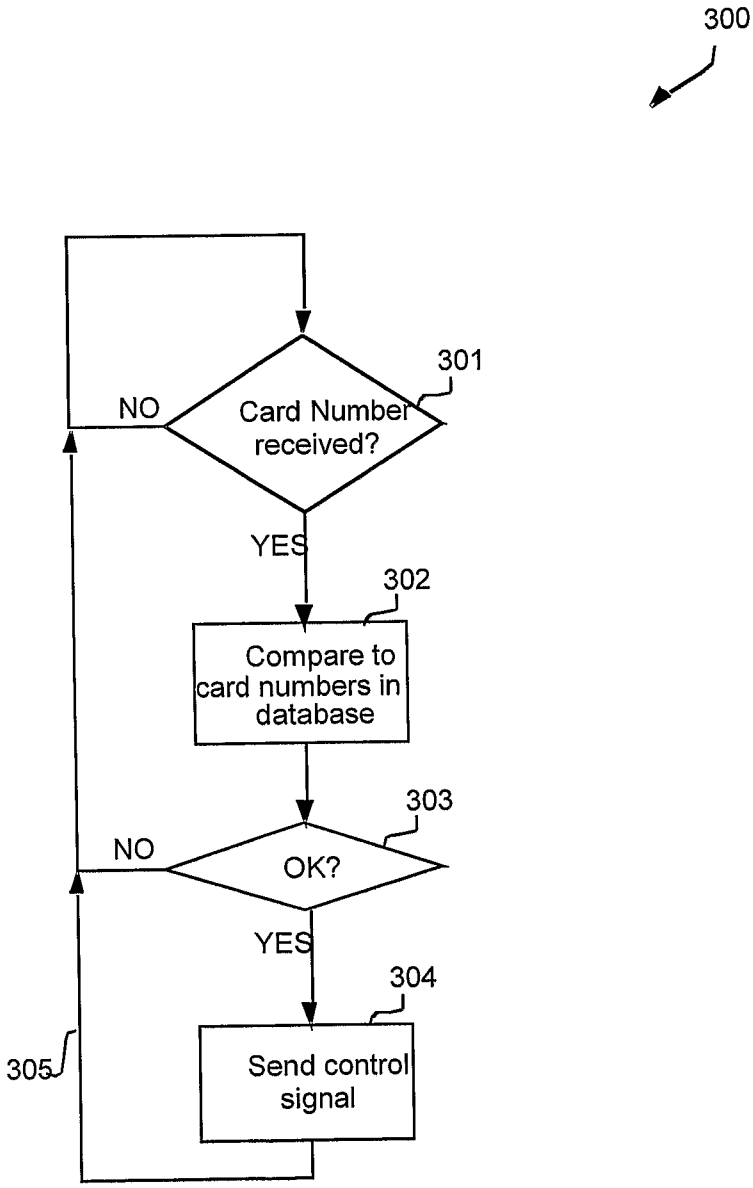
300
301
Card Number received?
NO
YES
302
Compare to card numbers in database
303
OK?
NO
YES
304
Send control signal
305

Fig. 4

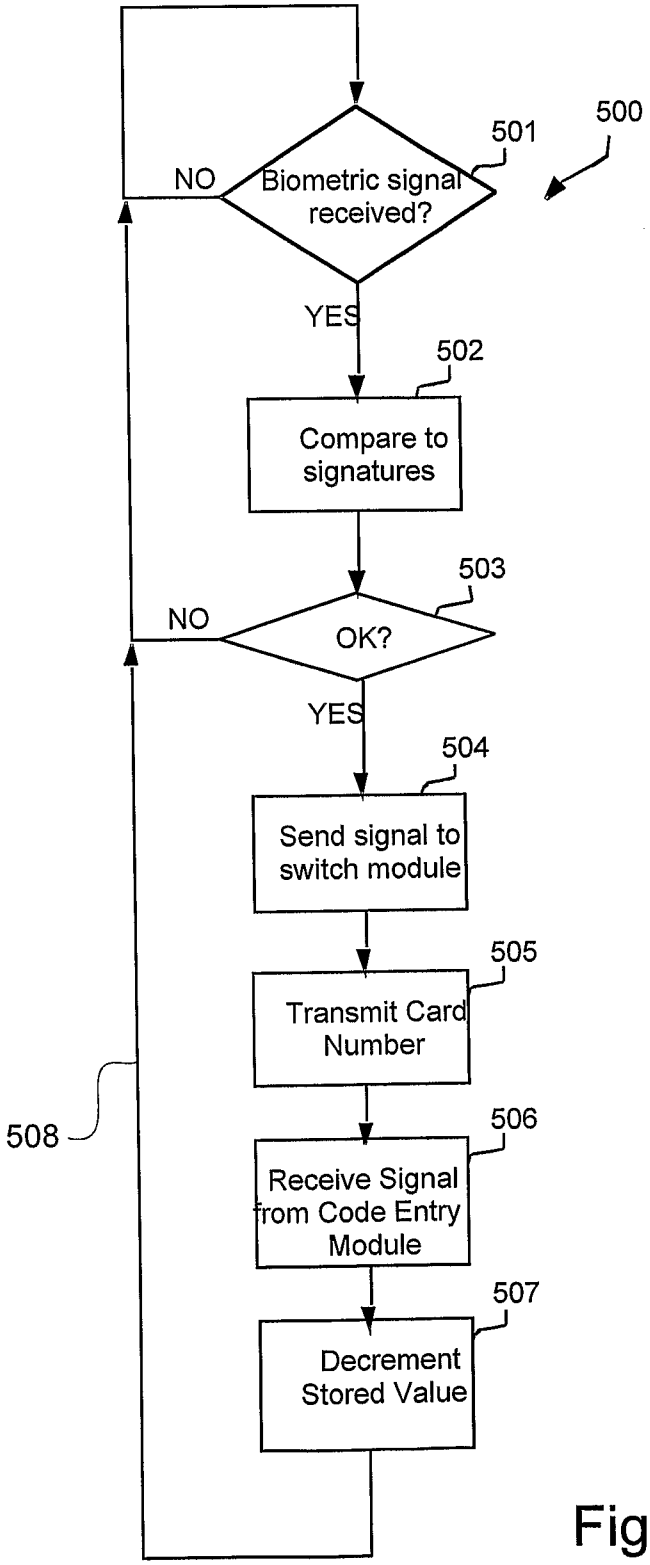
500
501
Biometric signal received?
NO
YES
502
Compare to signatures
503
OK?
NO
YES
504
Send signal to switch module
505
Transmit Card Number
506
Receive Signal from Code Entry Module
507
Decrement Stored Value
508

Fig. 5A

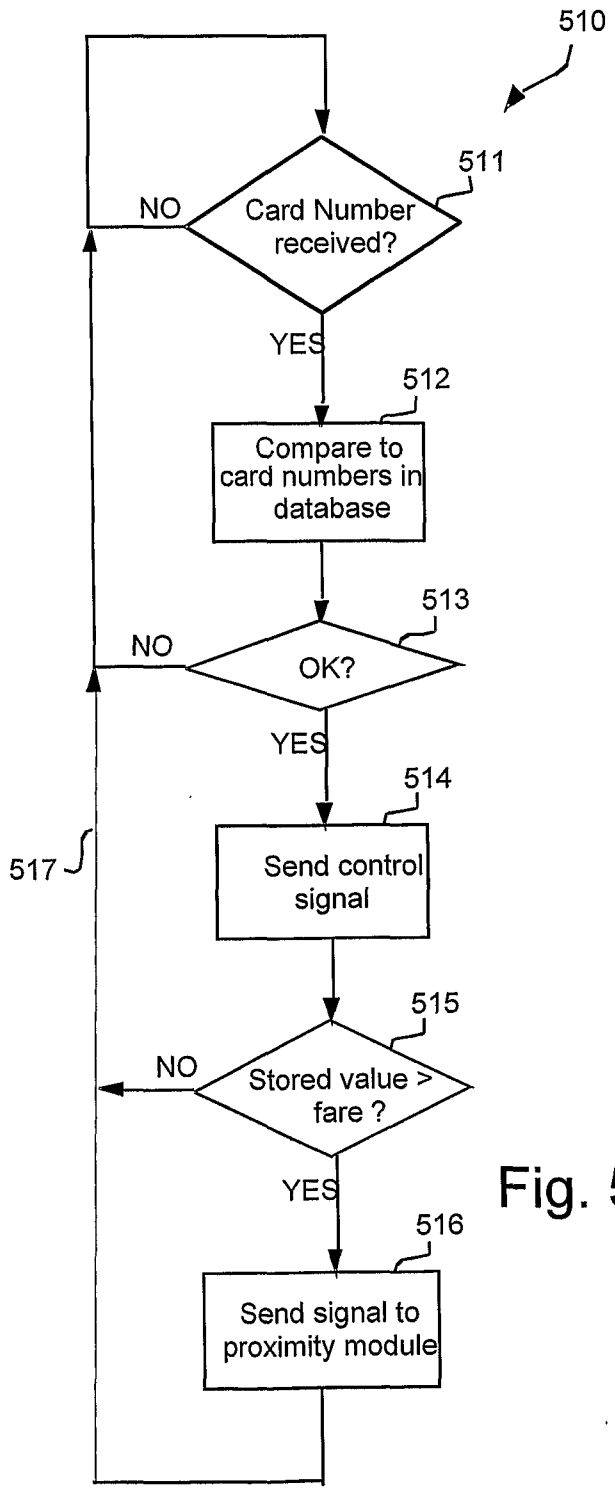
510
511
Card Number received?
NO
YES
512
Compare to card numbers in database
513
OK?
NO
YES
514
Send control signal
517
515
Stored value > fare ?
NO
YES
516
Send signal to proximity module

Fig. 5B

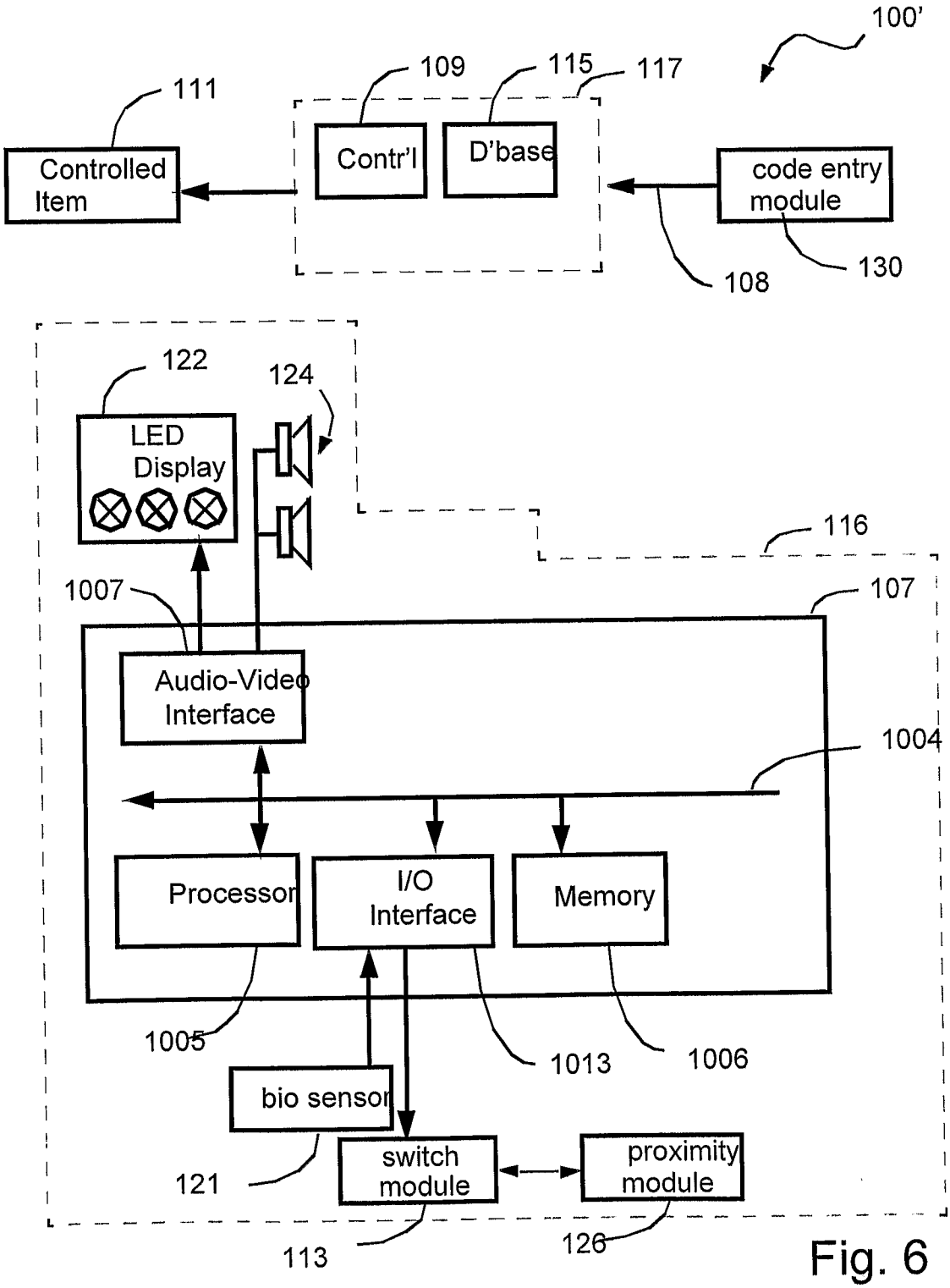
100'
111
109
115
117
Controlled Item
Contr'l
D'base
code entry module
108
130
122
124
LED Display
116
1007
107
Audio-Video Interface
1004
Processor
I/O Interface
Memory
1005
1013
1006
bio sensor
121
switch module
proximity module
113
126

Fig. 6

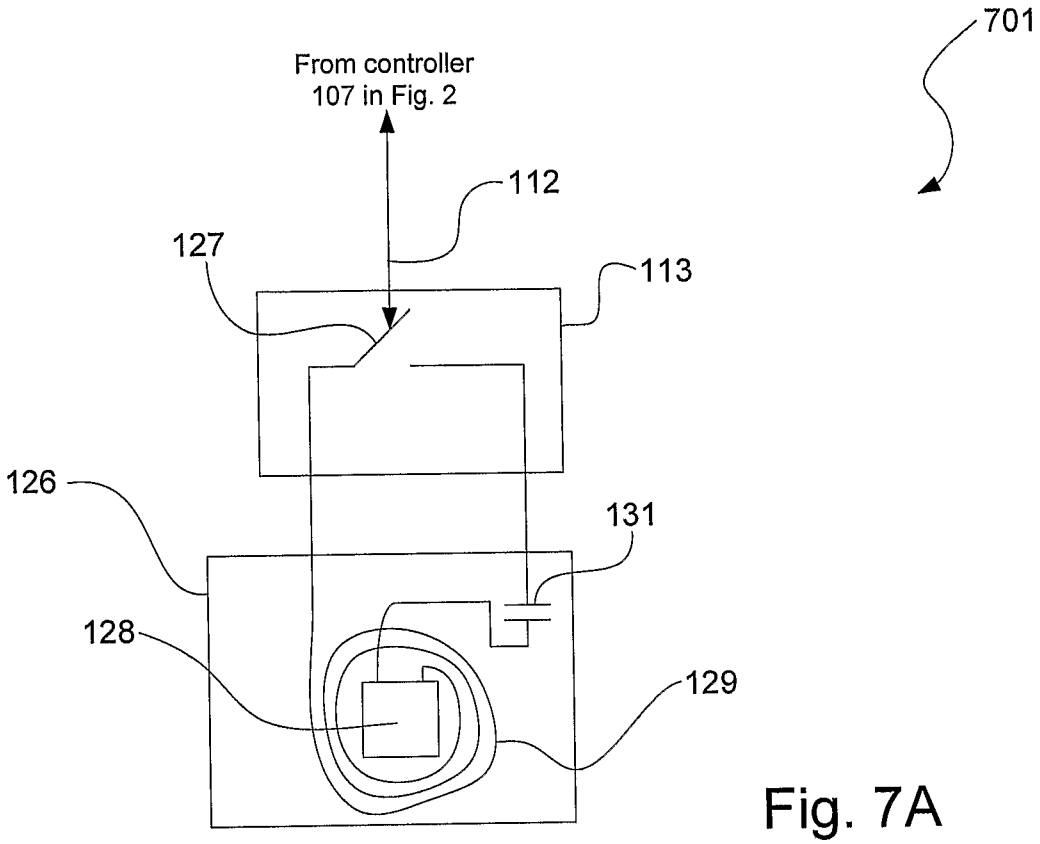
701
From controller
107 in Fig. 2
112
127
113
126
131
128
129

Fig. 7A

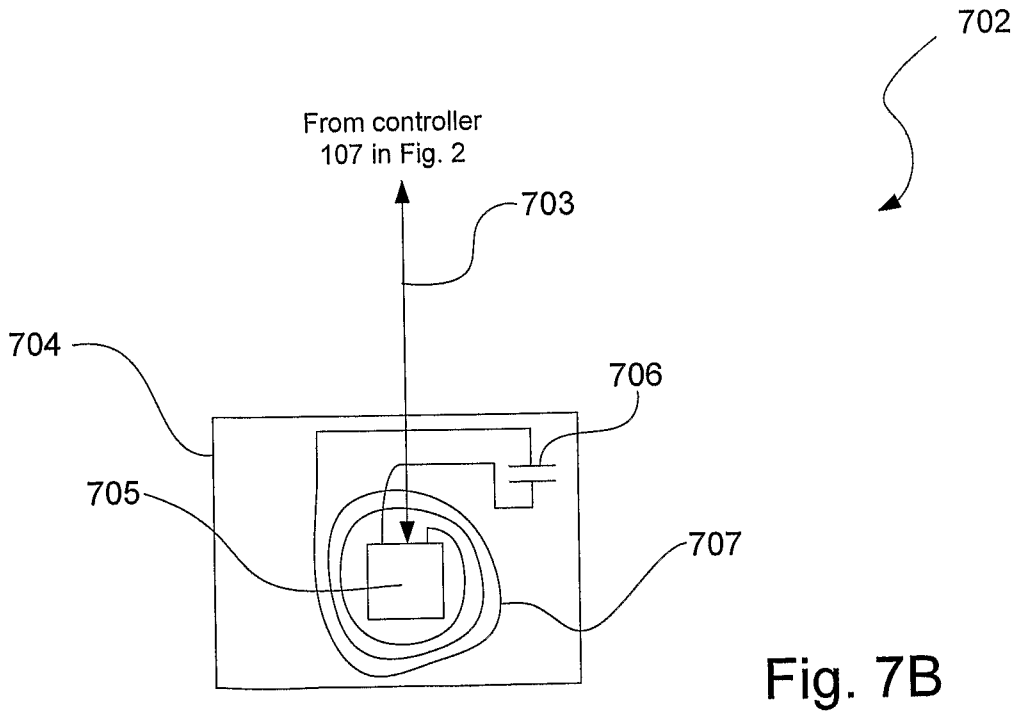
702
From controller
107 in Fig. 2
703
704
706
705
707

Fig. 7B

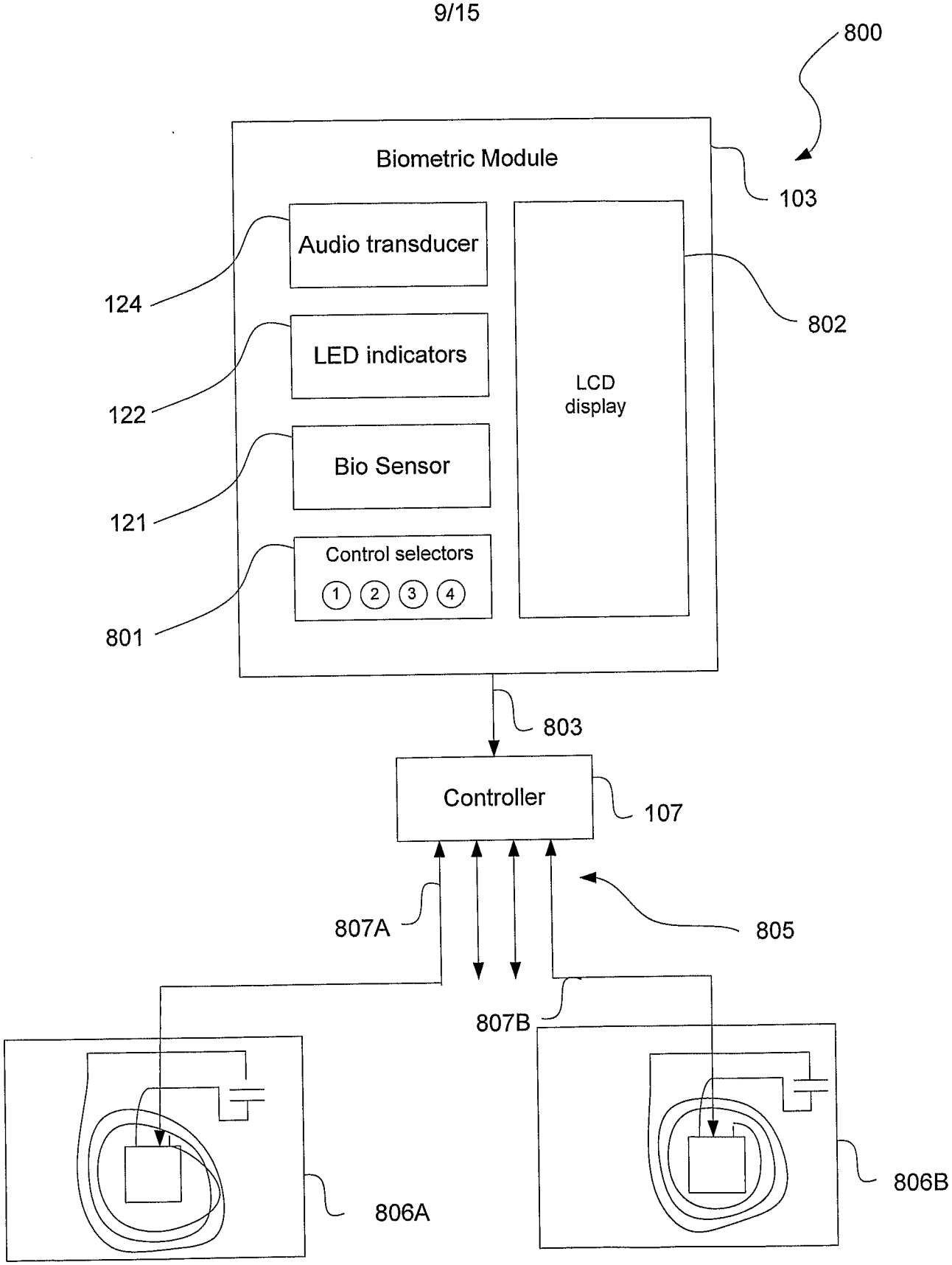
800
Biometric Module
103
Audio transducer
124
LED indicators
122
Bio Sensor
121
Control selectors
1 2 3 4
801
LCD display
802
803
Controller
107
807A
805
807B
806A
806B

Fig. 8

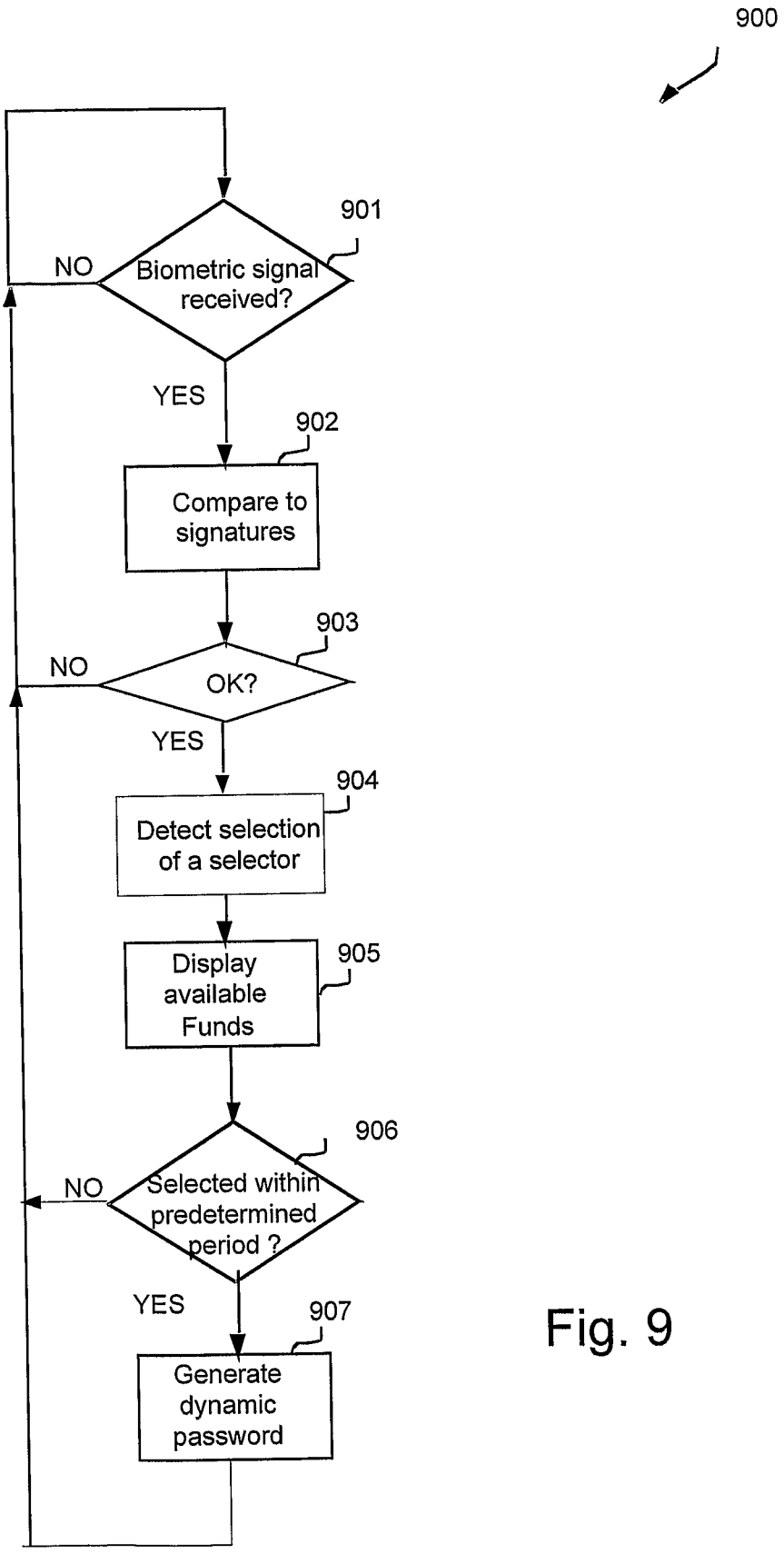
900
901
Biometric signal received?
NO
YES
902
Compare to signatures
903
OK?
NO
YES
904
Detect selection of a selector
905
Display available Funds
906
Selected within predetermined period ?
NO
YES
907
Generate dynamic password

Fig. 9

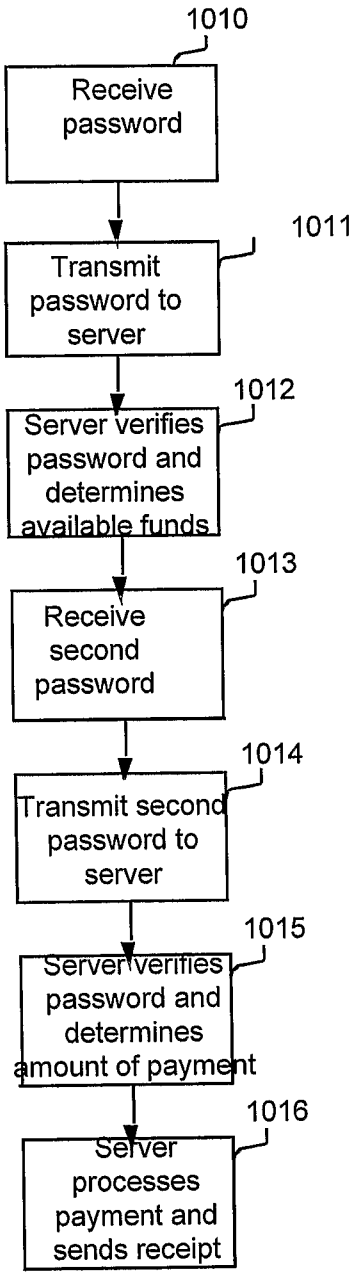
1010
Receive password
1000
1011
Transmit password to server
1012
Server verifies password and determines available funds
1013
Receive second password
1014
Transmit second password to server
1015
Server verifies password and determines amount of payment
1016
Server processes payment and sends receipt

Fig. 10

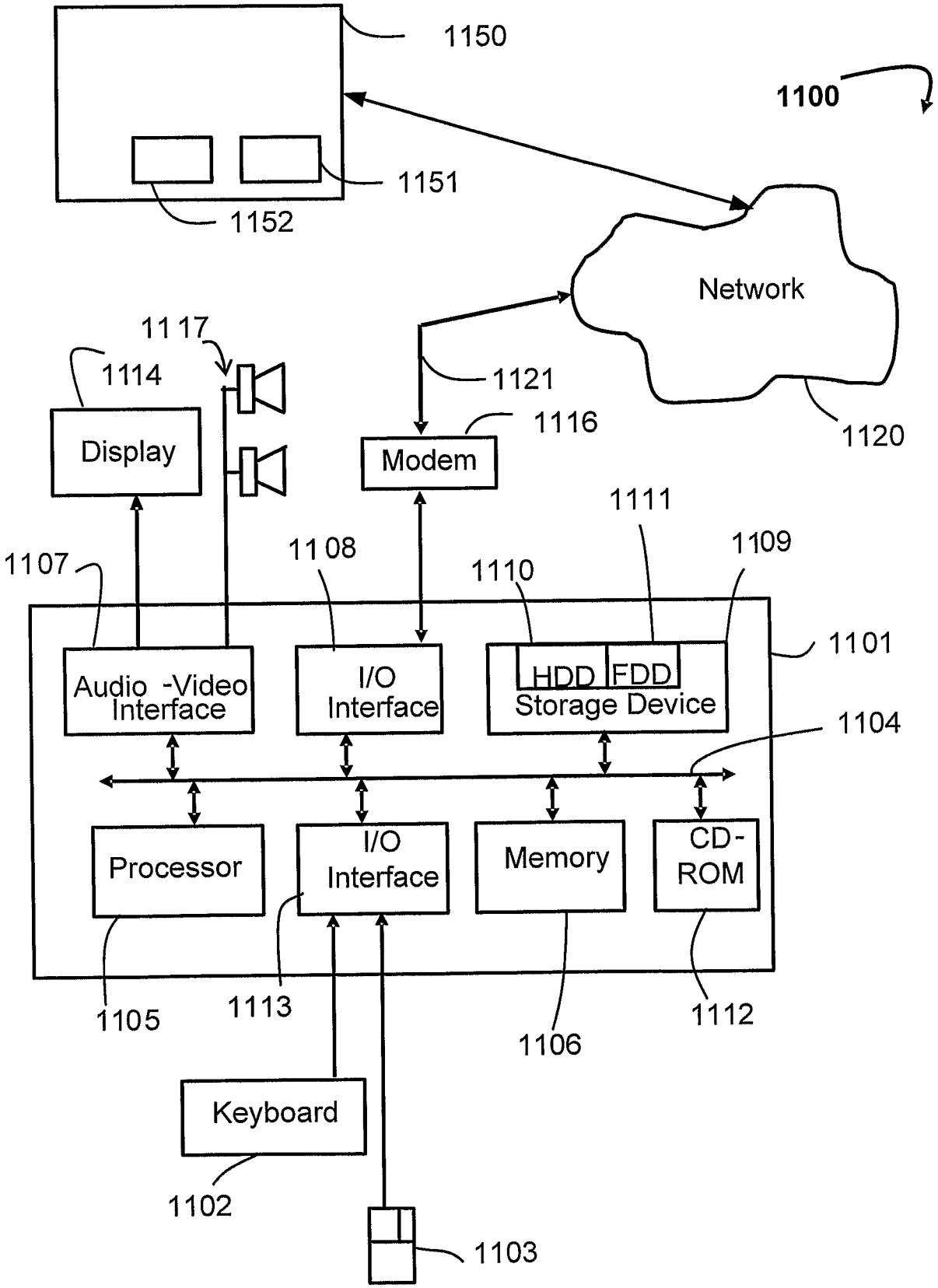
1150
1100
1151
1152
Network
1117
1114
1121
1116
Display
Modem
1120
1111
1109
1107
1108
1110
1101
Audio -Video Interface
I/O Interface
HDD
FDD
Storage Device
1104
Processor
I/O Interface
Memory
CD-ROM
1105
1113
1106
1112
Keyboard
1102
1103

Fig.11

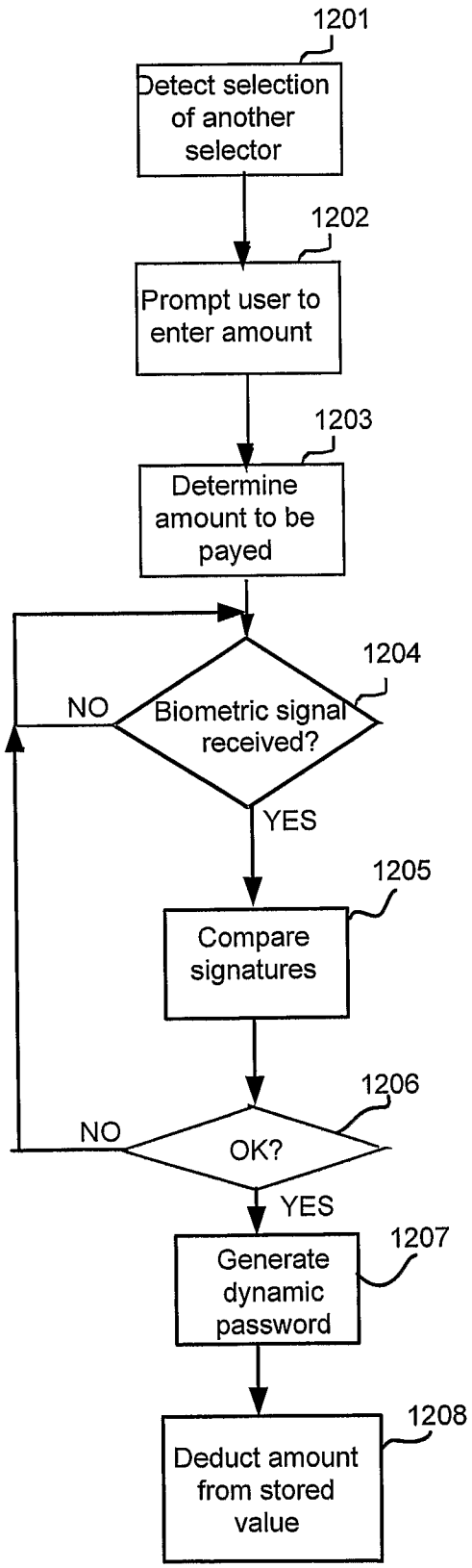
1201
Detect selection of another selector
1200
1202
Prompt user to enter amount
1203
Determine amount to be payed
1204
Biometric signal received?
NO
YES
1205
Compare signatures
1206
OK?
NO
YES
1207
Generate dynamic password
1208
Deduct amount from stored value

Fig. 12

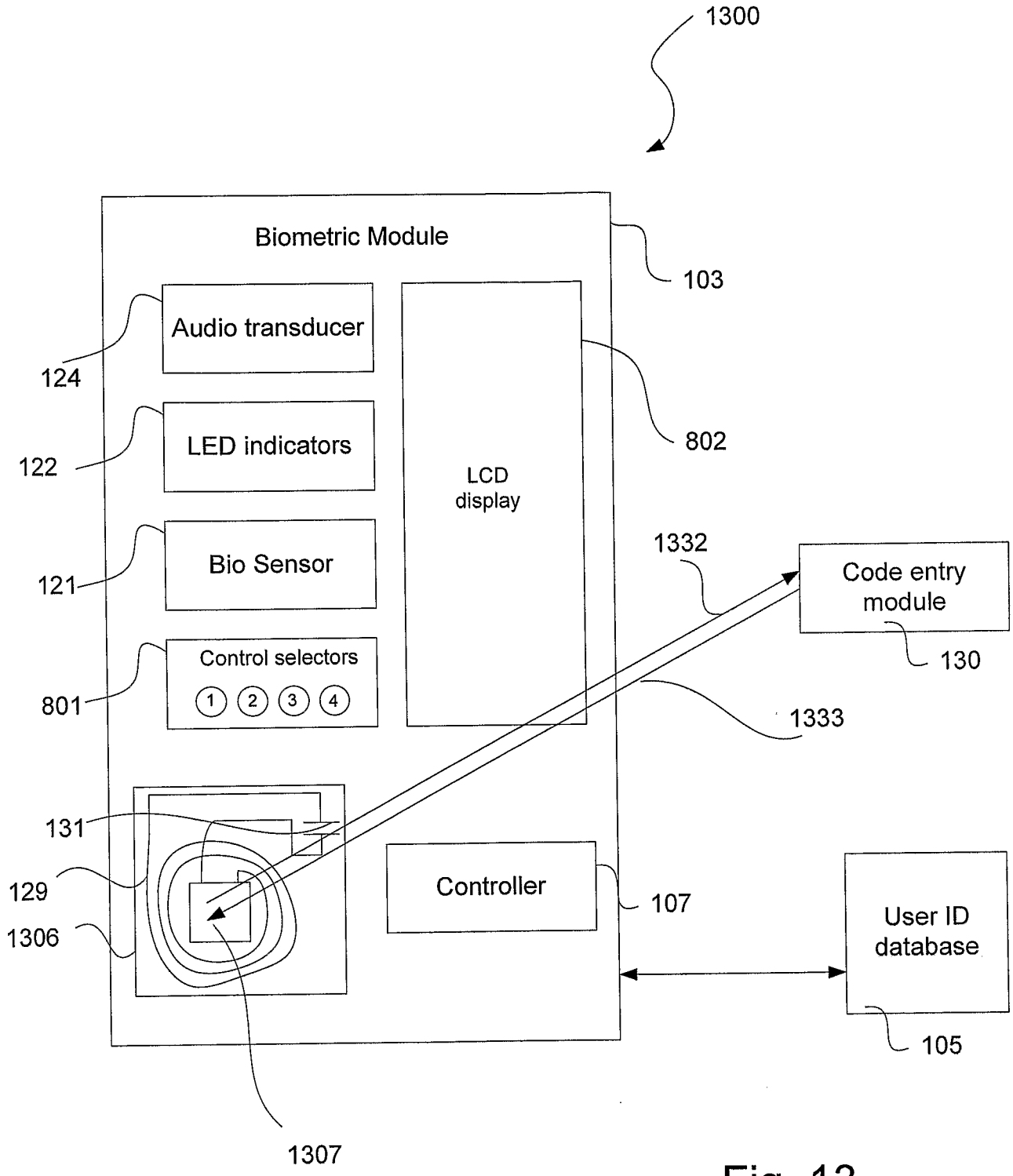
1300
Biometric Module
103
Audio transducer
124
LED indicators
122
Bio Sensor
121
Control selectors
1 2 3 4
801
LCD display
802
1332
Code entry module
130
1333
131
129
1306
Controller
107
User ID database
105
1307

Fig. 13

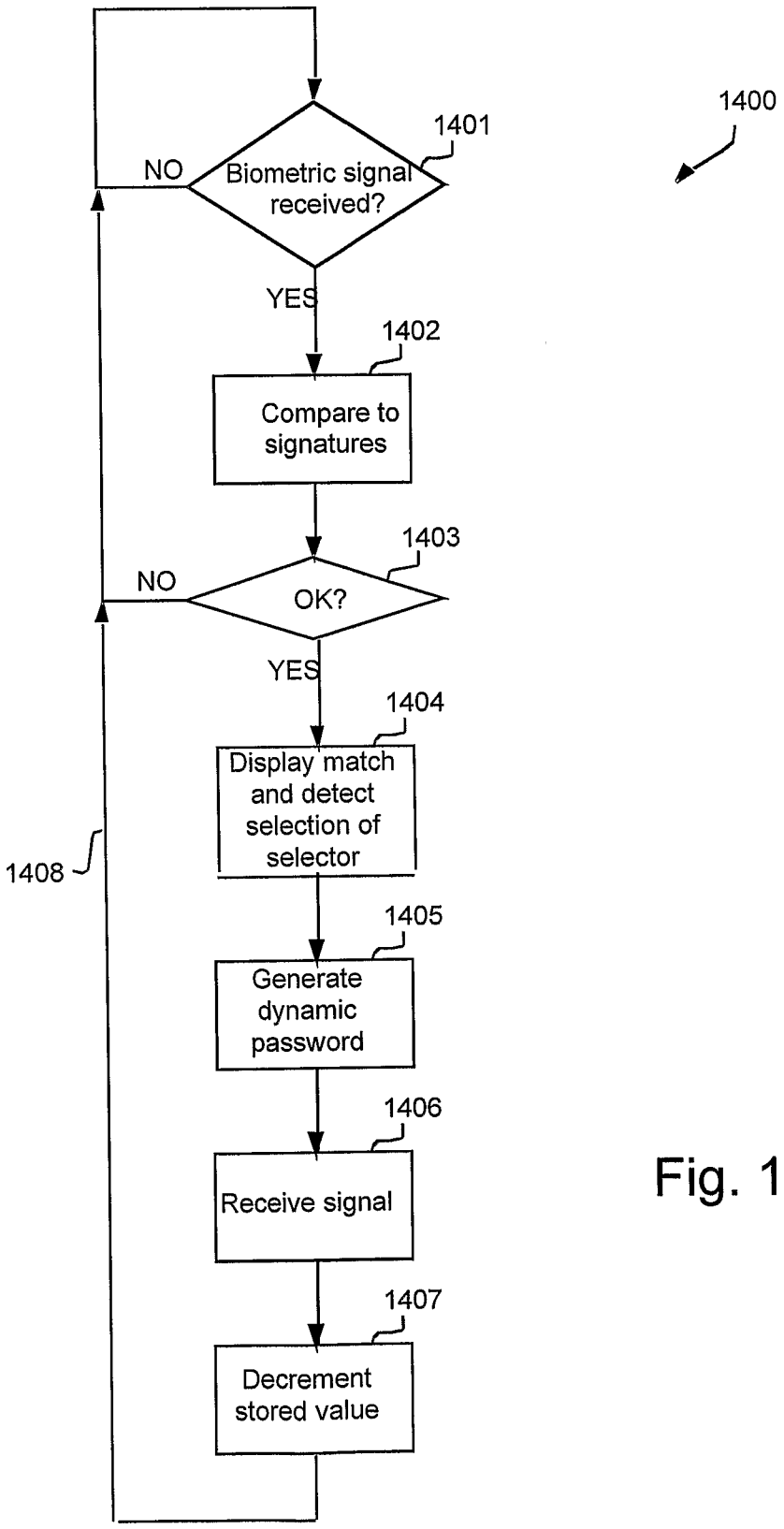
1400
1401
Biometric signal received?
NO
YES
1402
Compare to signatures
1403
OK?
NO
YES
1404
Display match and detect selection of selector
1408
1405
Generate dynamic password
1406
Receive signal
1407
Decrement stored value

Fig. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/001490

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/32 (2006.01) *G06K 9/62* (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO, USPTO and DWPI using IPC and keywords including secur+, identi+, biomet+, +card+, token+, fob?, authent+, verify+, password+, dynamic+, varia+, roll+, transact+, pay+, buy+, shop+, fund+, money, monies, finance+, credit+, balance+, account+, electronic wallet?, stored value, wireless, rf, radio frequency, activate+, access+, entr+ and enable+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2005/0253683 A1 (LOWE) 17 November 2005	
X	See whole document but particularly:	1 to 7, 9, 11 to 13, 15 to 17 and 20
	[0002], [0017], [0020], [0030], [0033] to [0038], [0043]	
Y		8, 10, 14, 18, 19 and 21 to 23
	US 2006/0174353 A1 (RYAL) 3 August 2006	
X	See whole document but particularly:	38
	[0021], [0023]	
Y	[0008], [0033]	10, 14, 18, 19 and 21 to 23

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

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

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

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

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

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

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 November 2008	21-11-2008
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	**LUKE DAVESON** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 2773

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/001490

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	US 2003/0130955 A1 (HAWTHORNE) 10 July 2003	
X	See whole document but particularly:	42, 47 to 50 and 52
	[0019], [0050]	
Y	[0033]	8
	US 2007/0001852 A1 (JALKANEN et al) 4 January 2007	
Y	See whole document but particularly:	14
	[0053], [0061]	
	EP 1637957 A1 (DEUTSCHE THOMSON-BRANDT GMBH) 22 March 2006	
Y	See whole document but particularly:	14
	Abstract and [0029]	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/001490

Box No. II 'Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE SUPPLEMENTAL BOX

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/001490

Supplemental Box
(To be used when the space in any of Boxes I to IV is not sufficient)

Continuation of Box No: III

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

In assessing whether there is more than one invention claimed, I have given consideration to those features which can be considered to potentially distinguish the claimed combination of features from the prior art. Where different claims have different distinguishing features they define different inventions.

This International Searching Authority has found that there are different inventions as follows:

- Claims 1 to 38, 43 to 46 and 51 are directed to the use of a biometric sensor to selectively enable transmission of a secure access code via an inductive circuit/proximity module. It is considered that the enabling of an inductive circuit by the biometric sensor comprises a first distinguishing feature.
- Claims 39 to 42, 47 to 50 and 52 are directed to using a biometric sensor to selectively enable the transmission of a password containing other encrypted information. It is considered that the use of a biometric signal to enable the transmission of a password containing other encrypted information comprises a second distinguishing feature.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

The only feature common to all of the claims is the use of a biometric sensor to selectively enable the transmission of an access code. However this concept is not novel in the light of US 2005/0253683 A1 (LOWE) 17 November 2005 (see [0036] to [0038]).

This means that the common feature can not constitute a special technical feature within the meaning of PCT Rule 13.2, second sentence, since it makes no contribution over the prior art.

Because the common feature does not satisfy the requirement for being a special technical feature it follows that it cannot provide the necessary technical relationship between the identified inventions. Therefore the claims do not satisfy the requirement of unity of invention a posteriori.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2008/001490

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2005253683	AU	2005251339	CA	2567069	EP	1751990
		KR	20070026584	WO	2005120086		
US	2006174353	CA	2553364	CN	1934818	EP	1716661
		KR	20070012345	US	7038985	US	7292512
		US	2005180566	WO	2005079359		
US	2003130955	AU	22020/01	EP	1245009	WO	0145056
US	2007001852	NONE					
EP	1637957	CN	101023402	EP	1792249	US	2008199006
		WO	2006032613				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX