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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2008 (25.09.2008)

PCT

(10) International Publication Number
WO 2008/113110 A1

(51) International Patent Classification:
G06K 9/00 (2006.01) *H04K 1/00* (2006.01)

(21) International Application Number:
PCT/AU2008/000366

(22) International Filing Date: 14 March 2008 (14.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007901361 16 March 2007 (16.03.2007) AU
2007901683 29 March 2007 (29.03.2007) AU

(71) Applicant *(for all designated States except US)*: **MICRO-LATCH 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, 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: METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING VERIFICATION STATION

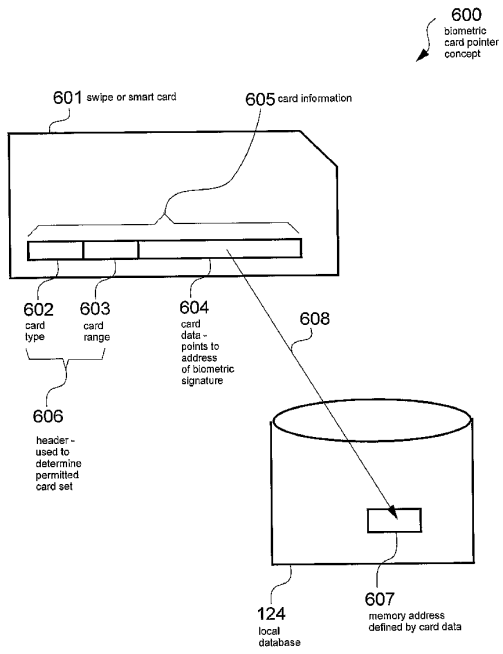


Fig. 4

(57) Abstract: A method of performing a transaction process using a verification station (127) is disclosed. The method compares a first biometric signature, inputted to a biometric reader (102) incorporated into the verification station (127), to one or more further biometric signatures stored in a memory (124) incorporated into the verification station (127). The method performs the transaction process using card information stored in the memory (124), if the inputted biometric signature matches one of the stored biometric signatures, otherwise, the transaction is not performed. The stored card information was read from a card device (112) and stored in the memory (124) during a previous transaction process using a card device reader (112) incorporated into the verification station (127).

WO 2008/113110 A1

METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING A VERIFICATION STATION

Field of the Invention

The present invention relates generally to security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.

Background

This description makes reference to various types of "card device" and their associated "reader devices" (respectively referred to merely as cards and readers). The card devices all contain card information that is accessed by "coupling" the card device to an associated reader device. The card information is used for various purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account, gaining access to a restricted area or controlled device and so on. The card information is typically accessed from the card by a corresponding card reader which then sends the card information to a "back-end" system that completes the appropriate transaction or process.

One type of card device is the "standard credit card" which in this description refers to a traditional plastic card 701 as depicted in **Fig. 1**. The standard credit card is typically "swiped" through a slot in a standard credit card reader in order to access card information 702 on the card 701. The card information 702 can alternately be encoded using an optical code such as a bar code, in which case the reader is suitably adapted. The standard credit card 701 also typically has the signature 703 of the card-owner written onto a paper strip on the card 701. This is used for verification of the identity of the person submitting the card when conducting a transaction using the card 701.

Another type of card device is the smart card (not shown) that typically has an on-board processor and a memory. The smart card typically has electrical contacts that

mate with corresponding contacts on a smart card reader (not shown) when accessing data in the memory of the smart card.

Still another type of card device is a proximity card (not shown) that typically has an on-board microchip. A proximity card reader sends out a low-level radio frequency (RF) signal, which energizes the microchip embedded in the card when the card is placed in close proximity to the reader. The proximity card then transmits data in the form of a unique code to the reader.

Still another type of card device is the wireless "key-fob" which is a small radio transmitter that emits an RF signal when a button on the fob is pressed. The RF signal can be encoded using the Wiegand protocol, or any other suitable protocol, such as rolling code or Bluetooth™ and can include encryption if desired. The key-fob typically has a processor and memory storing data that is sent via the transmitted signal to a corresponding receiver, which is the "reader device" for this type of card device.

The description also refers to "card user" and "card owner". The card user is the person who submits the card for a particular transaction. The card user can thus be the (authorised) card owner or an (unauthorised) person who has found or stolen the card.

Currently, the above described cards are heavily relied on both for financial transactions, as described above, and also for secure access. However, the cards are often used fraudulently. For example, a card may be used without the consent of the card owner to gain access to a bank account. Further, data stored on a card may be copied and used to gain access to a building or the like.

Clearly the signature 703 on the standard credit card 701 in **Fig. 1** can be forged. Thus, if the standard card 701 is stolen or lost, an unauthorised user can use the card provided that they can supply a sufficiently accurate version of the signature 703. The only recourse available to the card owner is to notify the card issuing company to "cancel" the card.

Current card devices such as the standard credit card, the smart card and the key-fob can have their security enhanced by requiring the card user to provide PIN (Personal Identification Number) information through a keypad to verify their identity prior to completing a transaction. However, PIN information can also be "stolen" by surveillance of the card owner's hands as the card owner operates the keypad.

Biometric verification can also be incorporated into current card systems to enhance security. In **Fig. 2** the card user swipes the standard card 701 through an associated card reader (not shown) that accesses the card information 702 on the card 701. The card user also provides a biometric signature 801, for example by pressing their thumb against a biometric (e.g., fingerprint) reader 802. The card information 702 that is read by the card reader (not shown), together with the biometric signature that is read by the biometric (fingerprint) reader 802, are sent, as depicted by a dashed arrow 803, a computer network 804, and a further dashed arrow 805, to a back-end system including a database 806 and associated processor (not shown).

In this arrangement, the card owner needs to have previously registered their biometric signature 801 and the card information 702 for pre-loading onto the back-end database 806. Having done so, the back-end processor (not shown) compares the pre-loaded information on the database 806 with the information received at 805, in order to check that the card holder of the card 701 is the (authorised) card owner and that the card itself is valid, in which case the transaction in question can proceed. Clearly this arrangement requires a central repository (806) of card information 702 and biometric signatures 801. This is cumbersome and potentially compromises the privacy and security of the holder of the card 701. This arrangement also requires complex back-end database management and the communications network 804. Furthermore, the front-end biometric signature reader 802 requires storage and/or processing capabilities for the biometric signatures. This results in a complex and expensive solution.

Privacy concerns have also been raised against the arrangement of **Fig. 2** which involves centralised storage and processing of personal information including biometric information. These concerns have slowed widespread use of biometrics to enhance user verification.

Another disadvantage of the arrangement of Fig. 2 is that even once the card owner's biometric signature 801 and card information 702 has be pre-loaded onto the back-end database 806, the card owner is still required to carry the card and to validate the card for each transaction. This is inconvenient as the card is often lost or damaged.

Summary

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

Disclosed are arrangements which seek to address the above problems by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, a biometric signature reader, the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form), an alphanumeric keypad (optional), and a communication module for communicating with back-end system that may be remotely accessible over a network.

As described herein, when the description refers to "the storing of a biometric signature" in a memory, a person skilled in the art would understand that rather than the actual biometric signature it is a representation of the biometric signature that is actually stored in the memory. This representation may be referred to as a "biometric template" or "template".

The card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase). The biometric signature is stored at a memory address together with a copy of the

card information on the user's card as read by the card reader of the verification station. The memory address may be defined by the ("unique") card information on the user's card. The term "unique" means unique in the context of a permitted set of cards associated with the verification station. This is described in more detail in regard to **Fig. 8**.

All future uses (referred to as uses in the verification phase) of the particular verification station by the user of the aforementioned card requires the user to merely submit a biometric signature (e.g., thumb print or retinal scan etc.), which is compared to the signatures stored in the memory associated with the verification station. Once the submitted biometric signature has been matched to one of the biometric signatures stored in the memory, the card information stored with the stored biometric signature is sent to the back-end system.

An authorised user will be automatically verified by the arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update, allowing entry to a restricted area etc. will simply proceed as normal. The biometric signature of an unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user.

The described arrangements require virtually no modification at all of the back-end systems or the (front-end) card. The additional administrative overheads associated with the described arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The described arrangements also potentially have a reduced impact on privacy of card users. The biometric signatures stored in the local database of the verification station can be made off limits to anyone, or limited to law enforcement agencies, depending on the administrative environment in which the arrangements are implemented. Users of current card systems can learn to use

the described arrangements without much effort, needing only to provide a biometric signature.

According to one aspect of the present invention there is provided a method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

According to another aspect of the present invention there is provided a verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

According to still another aspect of the present invention a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

According to still another aspect of the present invention there is provided a method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

According to still another aspect of the present invention there is provided a verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

According to still another aspect of the present invention there is provided a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said

PIN during a previous transaction process using a card device reader incorporated into the verification station.

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 will now be described with reference to the drawings, in which:

Fig. 1 depicts a standard credit card;

Fig. 2 shows the card of **Fig. 1** being used together with biometric verification;

Fig. 3 is a functional block diagram of a special-purpose computer system upon which described methods for the described arrangements can be practiced;

Fig. 4 illustrates the use of a standard card in the described arrangements;

Fig. 5 is a flow chart of a process for using the verification station of **Fig. 3**;

Fig. 6 shows the verification process of **Fig. 5** in more detail;

Fig. 7 shows the enrolment process of **Fig. 5** in more detail;

Fig. 8 shows the card information process of **Fig. 5** in more detail;

Fig. 9 shows an alternate use for the described arrangements;

Fig.10 is a flow chart of a process for using the verification station of **Fig. 3;** and

Fig. 11 is another flow chart of a process for using the verification station of **Fig. 3.**

Detailed Description including Best Mode

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. 3 is a functional block diagram of a system 100 in which the described arrangements can be practiced. The methods described herein particularly lend

themselves to implementation on the special-purpose computer system 100 such as that shown in **Fig. 3** wherein the processes of **Figs. 5-8, 9** and **10** may be implemented as software, such as an application program executing within the computer system 100. In particular, the steps of the described methods are effected by instructions in the software that are carried out by a verification station 127. The verification station 127 is typically constructed in a tamper-proof manner, both physically and electronically, to prevent unauthorised access to the inner mechanism of the verification station 127. 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 described 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 verification station 127 from the computer readable medium, and is then executed by the verification station 127. 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 effecting the described arrangements.

The computer system 100 consists of a computer module 101, input devices such as a biometric reader 102, a card reader 112, and a keypad 103, output devices including an LCD (Liquid Crystal Display) display device 126 and a loudspeaker 117. The computer module 101 uses a Modulator-Demodulator (Modem) transceiver device 116 for communicating to and from a communications network 120, for example connectable via a telephone line 121 or other functional medium. The modem 116 can be used to obtain access to a back end system including a processor 122 and back-end database 123

over the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The computer module 101 typically includes at least one processor unit 105, and a memory unit 106, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The module 101 also includes a number of input/output (I/O) interfaces including an audio-video interface 107 that couples to the LCD display 126 and loudspeaker 117, an I/O interface 113 for the keypad 103, biometric reader 102 and card reader 112, and an interface 108 for the modem 116. In some implementations, the modem 116 may be incorporated within the computer module 101, for example within the interface 108.

A storage device 109 is provided and typically includes a hard disk drive 110 and a flash memory 111. The components 105 to 111 and 113 of the computer module 101, typically communicate via an interconnected bus 104 and in a manner that results in a conventional mode of operation of the computer system 100 known to those in the relevant art.

Typically, the application program is resident on the hard disk drive 110 and read and controlled in its execution by the processor 105. Intermediate storage of the program and any data fetched from the network 120 may be accomplished using the semiconductor memory 106, possibly in concert with the hard disk drive 110. In some instances, the application program may be supplied to the user encoded on the flash memory device 111, or alternatively may be read by the computer module 101 from the network 120 via the modem device 116.

Still further, the software can also be loaded into the computer system 100 from other computer readable media. 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 computer system 100 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 computer module 101. 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.

As illustrated in **Fig. 4,** a standard card 601 has card information 605 typically comprising three fields, namely 602 which is the card type, 603 which is the card range, and 604 which comprises card data specific to the particular card 601. In the described arrangements, the card data 604 may act as the memory reference which points, as depicted by an arrow 608, to a particular memory address 607 in a local database 124 in the verification station 127 of **Fig. 3.** In another arrangement, a personal identification number (PIN) may also act as the memory reference which points to the particular memory address 607 in the local database 124 in the verification system 127.

The fields 602 and 603, which together form a header 606, can be used by the described system to determine if the card 601 is to be processed according to the described methods or not. This is described in more detail in regard to **Fig. 8.**

In an initial enrolment phase, the card user couples their card 601 (or key-fob or other card device) to the card reader 112. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM). The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader 102. The card data 604 defines the location 607 in the local database 124 where their unique biometric signature is to be stored. In the described arrangements, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 is

then also stored at the location 607 in the local database 124. For example, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

Thereafter, in later verification phases, the card user is merely required to present their unique biometric to the biometric reader 102 in order to perform a transaction. In this instance, the biometric signature provided by the user is compared to each of the signatures stored in the local database 124. Once verification is confirmed, through a match of the provided biometric signature to one of the stored signatures, the card information 605 is transferred from the local database 124 within the verification station 127 to the back-end processor 122 for completion of the transaction.

Importantly, the back-end processor 122 does not see the difference between receiving the card information 605 from the verification station 127, and receiving it from a conventional card reader in the absence of the verification station implementing the described arrangements. This means that back-end processes (depicted by the back-end processor 122 and the back-end database 123) need no modification when incorporating the described arrangements into current card systems. There are additional elements in the verification station 127 (see **Fig. 3**) compared to the normal card reader, however this is a relatively simple and inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Alternatively, rather than only providing their biometric signature in later verification phases, the user may choose to also couple their card 601 to the card reader 112. In this instance, after coupling their card 601 to the card reader 112, the card user is required to again present their unique biometric to the biometric reader 102. In this instance, rather than the biometric signature provided by the user being compared to all of the signatures stored in the local database 124 to determine a match, the biometric signature provided by the card user is only compared to the biometric signature stored at

the memory location 607 defined by the card data 604 read from their card 601 by the card reader 112. Again, once verification is confirmed, the card information 605 is transferred from the local database 124 of the verification station 127 to the back-end processor 122 for completion of the transaction.

Fig. 5 shows a process 200 for using the verification station 127. In the described process 200, rather than only providing their biometric signature in verification phases following the initial enrolment phase, the user couples their card 601 to the card reader 112 to perform a transaction. As described below, in another process 1000, in later verification phases following the initial enrolment phase, the user may merely present their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 201, the processor 105 determines if the card 601 has been read by the card reader 112. If this is not the case, then the process 200 follows a NO arrow back to the step 201. If, on the other hand, the card 601 has been read by the card reader 112, then the process 200 follows a YES arrow to a step 202 (see **Fig. 8** for more details). In the step 202, the processor 105 buffers the card information 605 that is read from the card 601 by the card reader 112 and processes the card information 605. In a following step 203 a request is presented to the card holder to provide a biometric signature to the biometric reader 102. This request can be provided in an audio fashion by means of the audio interface 107 and the speaker 117, this being driven by suitable software running on the processor 105. Alternatively or in addition, a suitable message can be displayed on the LCD display 126 by suitable software running on the processor 105.

In response to the aforementioned request, the holder of the card 601 provides a biometric signature to the biometric reader 102. After the signature has been received by the step 203, the process 200 is directed to a step 204 that reads the contents of the local database 124 at an address defined by the card data 604. If the contents of this memory

address match, to a sufficiently high degree of correspondence, the biometric signature received in the step 203 via the biometric reader 102, then the process follows a YES arrow to a step 205 (see **Fig. 6** for more detail). It is noted that if the step 204 returns a YES value, then the biometric signature at the noted memory address was written into the local database 124 in an earlier enrolment phase. It is also noted that the step 204 reads the biometric signature stored at a single memory address defined by the card data 604 and checks the stored biometric signature against the biometric signature received in the step 203. In the process 200, there is no need to search the database 124 to see if there is a match. Thus, the process 200 provides a particularly simple and fast biometric verification check. Once the step 205 has completed the verification process, the process 200 is directed according to an arrow 209 back to the step 201.

Returning to the step 204, if the biometric signature of the local database 124 at the memory address defined by the card data 604 does not match the signature received by the biometric reader 102, then the process 200 follows NO arrow to a step 206. In the step 206, the processor 105 determines if the biometric signature of the memory location defined by the card data 604 is empty. If this is the case, then the process 200 follows a YES arrow to a step 207 that performs an enrolment process for the card 601 (see **Fig. 7** for more detail). The process 200 then follows the arrow 209 back to the step 201.

Returning to the step 206, if the biometric signature of the aforementioned memory location is not empty, then this means that (i) the card 601 and the associated biometric signature of the card holder have previously been used for the enrolment process 207, and (ii) the biometric signature now received in the step 203 does not match the signature stored in the local database 124. In this event, the process 200 follows a NO arrow to a step 208 that performs an alert process. The process 200 then follows the arrow 209 back to the step 201. The alert process 208 can include sending an alert message from the verification station 127 to the back end processor 122 for later action,

for example by the police. The alert process can also store the (unauthorised) signature for later use by the law enforcement authorities.

As noted in regard to **Fig. 3**, the verification station 127 is constructed in a tamper proof fashion to ensure that the process 200 of **Fig. 5**, particularly the steps 204-207, are not accessible to unauthorised tampering.

Fig. 6 shows the verification process 205 from **Fig. 5** in more detail. The process 205 is entered from the step 204 in **Fig. 5**, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207 applied to the card in question.

After the step 301, a step 302 performs the transaction process, whatever that may be. Thus, for example, if the process 200 of **Fig. 5** relates to withdrawal of cash from an Automatic Teller Machine (ATM), then the step 302 comprises the user specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). After completion of the transaction process by the step 302, the process 205 is directed back to the step 201 in **Fig. 5**.

Fig. 7 shows the enrolment process step 207 from **Fig. 5** in more detail. The process 207 is entered from the step 206 in **Fig. 5**, after which a step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604 received in the step 202 of **Fig. 5**. At step 401, the process 207 also retrieves the card information 605 that was previously buffered in the memory 106 at step 202, and stores the card information in the local database 124 at the memory address defined by the card data 604. The aforementioned step 401 can store the biometric signature and card information 605 in encrypted form to reduce the probability

that the signature can be acquired for unauthorised use, thus helping ensure the privacy of the card owner. As described above, the biometric signature is stored as a biometric template representing the biometric signature provided by the user. The following steps 402 and 403 have the same respective functions as the corresponding steps 301 and 302 in **Fig. 6**. After completion of the step 403, the process 207 is directed back to the step 201 in **Fig. 5**.

Fig. 8 shows the step 202 in **Fig. 5** that is concerned with the processing of the card information 605 from the card 601 when the card 601 is read by the card reader 112 in the step 202 of **Fig. 5**. The process 202 is entered from the step 201 in **Fig. 5**, after which a step 501 reads the card information 605 from the card 601 using the card reader 112 and buffers the card information 605 in the memory 106. In a following step 502, the processor 105 retrieves predefined "permitted card set" parameters to determine the "permitted card set" for the verification station 127 in question. The permitted card set parameters may be retrieved from the local database 124 or from the hard disk drive 110, for example, and be also stored in the memory 106. A separate, or overlapping, permitted card set may be defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the described processes at any given verification station 127. This has the advantage of ensuring that the local database 124 does not overflow, and it also provides control over which users make use of which verification stations. However, the permitted card set for any given verification station 127 is only limited by the size of the local database 124. Card information 605 from any number of cards 601 may be stored in the local database 124 of a particular verification station 127 if the amount of memory is sufficient. In one embodiment, the processor 105 may periodically run a clean-up process where all card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months) may be deleted from the local database 124.

In a following step 503 the processor 105 compares the header 606 against the predefined permitted card set parameters to determine if the card 601 belongs to the permitted card set for the verification station 127 in question. If this is the case, then the process 202 is directed by a YES arrow to the step 203 in **Fig. 5**. If, on the other hand, the card header 606 does not belong to the permitted card set for the particular verification station 127, then the step 202 follows a NO arrow from the step 503 to a step 504. In the step 504, the processor 105 rejects the card that has been entered into the card reader 112. This rejection can take the form of a message displayed on the LCD display 126 and/or a corresponding audio message via the speaker 117. Thereafter, the process 202 is directed back to the step 201 in **Fig. 5**. It is noted that even if the verification station does not reject the card not belonging to the permitted card set for the verification station 127 in question, the back-end processor 122 can do so.

In addition to the predefined permitted card set, other administrative functions can be provided by the described arrangements. Thus, the predefined permitted card set details can be amended and/or the signatures stored in the database 124 can be deleted by a system administrator. The system administrator may also periodically perform the clean-up process described above to delete card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months), so that the local database 124 does not overflow. Audit trail information is also stored in the verification station 127 and can be downloaded for audit purposes. The audit information typically includes information of which cards have been submitted to the verification station and the time stamps of the card submissions. Biometric signatures are typically not part of the downloadable audit information, and require a greater level of authorisation (such as that associated with law enforcement agencies) for access.

Fig. 10 shows a process 1000 for performing a transaction using the described arrangement. The process 1000 may be performed by the owner of the card 601, for

example, in later verification phases once the owner has previously performed the initial enrolment phase, so that their biometric signature and a copy of the card information 605 has been stored in the local database 124. Accordingly, the stored copy of the card information 605 was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127. In the described process 1000, in such a later verification phase, the user may merely present their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 1001, the processor 105 receives a biometric signature as provided by the owner of the card 601 to the biometric reader 102. The biometric signature may be temporarily buffered in the memory 106. After the signature has been received at the step 1001, the process 1000 is directed to a step 1004 that reads the contents of the local database 124 at a first address and compares a biometric signature stored at that first address to the biometric signature received at step 1001. In this instance, the first address may be selected randomly. Alternatively, the first address may be selected in an ordered fashion. For example, the first address may be selected as the first address in a particular block of memory.

Accordingly, at step 1004, the process 1000 compares the received biometric signature, inputted to the biometric reader 102 and buffered in memory 106, to a biometric signature stored at a first address in the local database 124 (or memory) incorporated into the verification station 127. As will be described, if the received biometric signature stored at the first memory address does not match the biometric signature stored at the first address, then the process 1000 compares the received biometric signature to one or more further biometric signatures stored in the local database 124 (or memory) incorporated into the verification station 127.

At the next step 1005, if the biometric signature stored at the first memory address matches, to a sufficiently high degree of correspondence, the inputted biometric signature received in the step 1001, then the process 1000 follows a YES arrow to a step 1006. It is noted that if the step 1005 returns a YES value, then the biometric signature at the first memory address was written into the memory 124 in an earlier enrolment phase together with the card information 605.

At step 1006, the process 1000 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches one of the biometric signatures previously stored in the local database 124 by a previous enrolment process 207 applied for the card 601 in question. After the step 1006, a next step 1008 performs the transaction process, whatever that may be, using the copy of the card information 605 stored in the local database 124. Typically, the transaction process will require the card information 605 to be transferred from the verification station 127 to the back-end processor 122 for completion of the transaction. As an example of a transaction process, if the process 1000 of **Fig. 10** relates to the withdrawal of cash from an Automatic Teller Machine (ATM), then the step 1008 comprises the card owner specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). Accordingly, the stored copy of the card information 605 used in the performed transaction process was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127.

After completion of the step 1008, the process 1000 is directed back to step 1001 or to the step 201 in **Fig. 5**.

If, at step 1005, the biometric signature stored at the first memory address does not match the biometric signature received in the step 1001, then the process 1000 follows a NO arrow to a step 1007. At step 1007, if the processor 105 determines that there are

no further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1001 or to the step 201 in **Fig. 5.** If the processor 105 determines at step 1007 that there are further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1004. At the next execution of step 1004, the processor 105 reads the contents of the local database 124 at a further address and compares a biometric signature stored at that further address to the biometric signature received at step 1001.

Fig. 9 shows another application 900 to which the described arrangements can be applied. In a first step 901 a person purchases or hires a verification station implemented in a portable form. A step 901 is performed at a registered supplier premises. Accordingly in a following step 902, the enrolment process is performed in controlled circumstances at the supplier premises. The "controlled conditions" referred to mean that the enrolment process is performed under conditions where the identity of the holder of the card 601 is verified, using a driving licence, passport or equivalent identification document, this ensuring that the enrolment process enrols the true owner of the card in an authorised manner.

In a following step 903, the verification station together with the card 601 can be used for third party transactions. Thus, in one example, the holder of the card 601 can take the portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises. This station identification number is then transmitted to the on-line casino back-end processes together with the card information 605. This type of application does require some modification of the back-end processes.

In the arrangements described above, a card user is required to enrol at each individual verification station 127. However, in another arrangement, a user may be able to enrol at one verification station 127 and the user's biometric signature and card information 605 may be broadcast over the communications network 120 to one or more other verification stations connected to the communications network 120. The broadcast biometric signature and card information 605 may then be stored in the local databases of each of those verifications stations to which the biometric signatures and card information 605 have been broadcast. Such an arrangement may be referred to as a 'minimum enrolment' arrangement. The minimum enrolment arrangement is particularly advantageous for Electronic Funds Transfer Point of Sale (EFTPOS) transactions, ATM transactions and the like. For example, the verification station 127 described above may be added to an EFTPOS terminal or ATM. The broadcasting of the biometric signature and card information 605 increases the security of the transactions made with the verification stations.

In an initial enrolment phase of the minimum enrolment arrangement, the card user couples their card 601 to the card reader 112 of the verification station 127 in a similar manner to that described above. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM) of the verification station 127. The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader 102. The buffered card data 604 defines the location 607 in the local database 124 where the card user's unique biometric signature is to be stored. Once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 may then also stored at the location 607 in the local database 124. As described above, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

In the minimum enrolment arrangement, following the storing of the user's biometric signature in the local database 124, a copy of the user's biometric signature, together with a copy of the card information 605 read from the user's card, is broadcast over the communications network 120 to one or more of the other verification stations connected to the network. The card user's unique biometric signature together with the card information 605 corresponding to the biometric signature is then stored in the local database (e.g., 124) of each verification station to which the biometric signature and card information 605 has been broadcast. The biometric signature and card information 605 is stored at a particular memory address, as defined by the card data 604, in each of the local databases. The storing of the card information 605 in the each of the local databases of the verification stations allows biometric only transactions as described above to be performed.

In another alternative of the minimum enrolment arrangement, rather than broadcasting the individual biometric signatures and card information to each of the other verification stations connected to the network 120 upon an enrolment taking place, updates to the contents of a local database within a particular verification station 127 or indeed the entire contents of the local database may be broadcast periodically (e.g., overnight).

Accordingly, in the minimum enrolment arrangement described above, the card user is only required to enrol on one verification station 127 connected to the communication network 127 and each of the other verifications stations connected to the communications network 120 will receive a copy of the card user's enrolled biometric signature and possibly the card information 605 corresponding to that biometric signature. Thereafter, in later verification phases, the user may make biometric only transactions, as described above with reference to Fig, 10, at each of the verification stations connected to the communications network 120 after enrolling on one of the verification stations 127.

Alternatively, the user may also choose to couple their card to the card reader (e.g., 112) of one of the verifications stations and present their unique biometric signature in order to perform a transaction, as described above.

In the arrangements described above, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 is then also stored at the location 607 in the local database 124 and may be used to point to the location 607 in the local database 124.

In another arrangement, once the biometric signature and biometric has been stored in the local database 607, the card user may also enter a PIN using the keypad 103. Preferably, the PIN is required to be entered within a predetermined time period. The PIN may be any number and/or letter sequence including names and easy to remember patterns. In this instance, the PIN is then also stored at the location 607 in the local database 124. Again, the PIN may be appended to the biometric signature stored at the location 607. Therefore, the local database 124 contains the biometric signature, the card information 605 (or key-fob information) and the PIN of a card user. The PIN may be used to define a pointer to the memory location 607 in the local database which is the same location 607 pointed to by the card data 604. Thereafter, in later verification phases, the card user is required to present their unique biometric to the biometric reader 102 and then enter their PIN using the keypad 103, in order to perform a transaction. The PIN may be required to be entered within a predetermined period of time.

Once the biometric and PIN has been provided by the user, rather than the biometric signature being compared to all of the signatures stored in the local database 124 to determine a match, the biometric signature provided by the card user is only compared to the biometric signature stored at the memory location 607 defined by the user's PIN entered by the user into the keypad 103.

Again, once verification is confirmed, through a match of the provided biometric signature to the biometric signature stored at the memory location 607 defined by the PIN, the card information 605 is transferred from the local database 124 within the verification station 127 to the back-end processor 122 for completion of the transaction.

In the PIN arrangement, at step 401 of the enrolment process 207, a request is presented to the card holder to provide a PIN to the keypad 103. This request can be provided in an audio fashion by means of the audio interface 107 and the speaker 117, this being driven by suitable software running on the processor 105. Alternatively or in addition, a suitable message can be displayed on the LCD display 126 by suitable software running on the processor 105. The PIN entered into the keypad 103 is stored in the local database 124 at the memory address defined by the card data 604. Again, the biometric signature, PIN and card information 605 may stored in encrypted form to reduce the probability that the signature can be acquired for unauthorised use.

Fig. 11 shows another process 1100 for performing a transaction using the described arrangement. The process 1000 may be performed by the owner of the card 601, for example, in later verification phases once the owner has previously performed the initial enrolment phase, so that their biometric signature, a copy of the card information 605 and a PIN has been stored in the local database 124. Accordingly, the stored copy of the card information 605 was read from the card 601 and together with the PIN entered by the user was stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127. In the described process 1100, in such a later verification phase, the user may present their unique biometric signature to the biometric reader 102 together with their PIN in order to perform a transaction.

In a first step 1101, the processor 105 receives a biometric signature as provided by the owner of the card 601 to the biometric reader 102. The biometric signature may be

temporarily buffered in the memory 106. After the signature has been received at the step 1001, the process 1000 is directed to a step 1003. At step 1003, the processor 105 receives a PIN as provided by the owner of the card 601 to the keypad 103. The keypad 103 may be similar to a telephone where letters are also displayed on the keys together with the numbers. The keypad 103 may be in addition to another keypad (e.g., an existing keypad on an Automatic Teller Machine in which the verification station 127 has been installed.

At a step 1104 the processor 105 reads the contents of the local database 124 at an address defined by the entered PIN and compares a biometric signature stored at that address to the biometric signature received at step 1101.

At the next step 1105, if the biometric signature stored at the memory address defined by the PIN matches, to a sufficiently high degree of correspondence, the inputted biometric signature received in the step 1101, then the process 1000 follows a YES arrow to a step 1106. It is noted that if the step 1105 returns a YES value, then the biometric signature at the memory address and the PIN was written into the memory 124 in an earlier enrolment phase together with the card information 605.

At step 1106, the process 1100 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207 applied for the card 601 in question. After the step 1106, a next step 1108 performs the transaction process, whatever that may be, using the copy of the card information 605 stored in the local database 124. Typically, the transaction process will require the card information 605 to be transferred from the verification station 127 to the back-end processor 122 for completion of the transaction. As an example of a transaction process, if the process 1100 of **Fig. 11** relates to the withdrawal of cash from an Automatic Teller Machine (ATM), then the step 1108 comprises the card owner specifying the required amount of cash and

the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). Accordingly, the stored copy of the card information 605 used in the performed transaction process was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127.

After completion of the step 1108, the process 1100 is directed back to step 1101, to step 1001 in Fig. 10 or to the step 201 in **Fig. 5**.

If, at step 1105, the biometric signature stored at the memory address defined by the PIN does not match the biometric signature received in the step 1001, then the process 1000 follows a NO arrow to a to step 1101, to step 1001 in Fig. 10 or to the step 201 in **Fig. 5**.

As described above, the PIN may be any number and/or letter sequence including names and easy to remember patterns. This allows the card user to select a PIN which may be memorised by recalling letters, which are associated with the numbers similar to a telephone number.

In another minimum enrolment arrangement, following the storing of the user's biometric signature and PIN in the local database 124, a copy of the user's biometric signature and PIN, together with a copy of the card information 605 read from the user's card, is broadcast over the communications network 120 to one or more of the other verification stations connected to the network. The card user's unique biometric signature and PIN, together with the card information 605 corresponding to the biometric signature is then stored in the local database (e.g., 124) of each verification station to which the biometric signature, PIN and card information 605 has been broadcast. The biometric signature, PIN and card information 605 is stored at a particular memory address, as defined by the card data 604 and PIN, in each of the local databases. The storing of the

card information 605 in the each of the local databases of the verification stations allows biometric and PIN only transactions as described above to be performed.

Again, in still another alternative of the minimum enrolment arrangements described above, rather than broadcasting the individual biometric signatures, PIN and card information to each of the other verification stations connected to the network 120 upon an enrolment taking place, updates to the contents of a local database within a particular verification station 127 or indeed the entire contents of the local database may be broadcast periodically (e.g., overnight).

The PIN arrangement and the other arrangements described above can be easily integrated to a security or financial platform system, as an additional component to verify the card user at entry/excess access points. The arrangements may be performed ONLINE or OFFLINE.

In the PIN arrangement, if a unscrupulous user oversees the PIN number of the legitimate card user, the user still requires the biometric of the legitimate card user to perform a transaction. The described arrangements are secure and inexpensive to implement.

The PIN arrangement does not require extensive database searching in order to locate a matching biometric and is therefore the verification is able to be performed in an efficient manner. Further, an incorrectly entered PIN may be used to generate an warning alarm or door chime

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the described arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards, government issued card (e.g., the Australian Medicare card) and others. The arrangements can, in general be used

in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature possibly together with a PIN. For example, in the case of the Australian Medicare card, following enrolment at a verification station 127 located at a particular medical centre, the entire card information 605 of the user's Medicare card is stored in the local database 124 of the verification station 127 located at the medical centre.

As another example, the described arrangements can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying platform. In this instance, the ATM PIN may be used to point to the stored biometric signature. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature, possibly together with their PIN, to withdraw funds.

Furthermore, the described arrangements can be used for secure access to a hotel room or any other room, building, cabinet, or apparatus to which secure access is required.

In the hotel room example, the hotel may have a verification station 127 mounted on each door of the hotel. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining a particular room number and planned departure date. The number on the card is preferably one of an increasing sequence of numbers. The number preferably increases over a period of time and is also encrypted. A verification station 127 positioned at the door of the room corresponding to the room number may be configured so that the verification station 127 will only allow enrolments

and verifications if the number stored on a presented card correctly identifies the room and is in the correct sequence. The verification station 127 may also include a real time clock to match actual time against the planned date of departure. After the guest enrols their biometric signature at the verification station 127 using the aforementioned card in the manner described above, the arrangement will give them secure access to their room for the duration of their stay.

Following enrolment, the above hotel guest may use their card and a biometric signature (e.g., a fingerprint) to enter the room. Alternatively, the guest may merely present their biometric signature, possibly together with a PIN, to enter the room as described above negating the requirement for the guests to carry the room card, plus increasing security and convenience. The verification station 127 may also be configured so that the guest may choose not to enrol their biometric signature if they do not wish to have a record of their biometric signature stored within the local database of the verification station 127.

The verification station 127 located at the door of a particular hotel room or other secure access entry as described above may also allocate memory for storage of any number of biometric signatures (e.g., fingerprints) to be associated with the new card. This allows the hotel guest and all associated guests (e.g., the hotel guest's family) to enrol their individual biometrics at the verification station 127. The enrolment may simply be achieved, for example, by inserting the card and placing a finger on the biometric reader 102, for each guest. Following this enrolment stage, the card or the biometric signature can be used to gain access to the room, again, negating the requirement for each of the guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the biometric signature (e.g., fingerprints) memory address is that the time and date of departure can also be added to the same

memory location. Therefore, the hotel application also allows other related data to be added to the memory location, enhancing the capability of the described arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the described arrangements is in regard to passport control and customs. The arrangements can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to **Figs. 5** and **10.**

Finally, in each of the arrangements described above, the verification stations 127 may be configured to provide the card user with the option of performing transactions with the card 601 only. For example, the card user may not wish to provide their biometric signature. In this instance, the card user may use their card only to perform a transaction with the verification stations in a conventional manner.

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.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

In the context of this specification, the word "comprising" means "including principally but not necessarily solely" or "having" or "including", and not "consisting only of". Variations of the word "comprising", such as "comprise" and "comprises" have correspondingly varied meanings.

The claims defining the invention are as follows:

1. A method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

2. The method according to claim 1, wherein the card information is stored in said memory with the matching one of said previously stored biometric signatures.

3. A method according to claim 1, wherein the card device is one of:

a card device in which the card information is encoded in a magnetic strip;

a card device in which the card information is encoded in a bar code;

a smart card device in which the card information is stored in a solid state memory on the smart card; and

a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

4. A method according to claim 1, further comprising the step of outputting information indicating that the user of the card device is not authorised.

5. A method according to claim 4 wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

6. A method according to claim 1, wherein the stored card information and said one stored biometric signature was broadcast over a communications network to which said verification station is connected, to one or more further verification stations, following said previous transaction.

7. A verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

8. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

9. A method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

10. The method according to claim 9, wherein the card information is stored in said memory with said previously stored biometric signature.

11. A method according to claim 9, wherein the card device is one of:

a card device in which the card information is encoded in a magnetic strip;

a card device in which the card information is encoded in a bar code;

a smart card device in which the card information is stored in a solid state memory on the smart card; and

a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

12. A method according to claim 9, further comprising the step of outputting information indicating that the user of the card device is not authorised.

13. A method according to claim 12 wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

14. A method according to claim 9, wherein the stored card information and said stored biometric signature was broadcast over a communications network to which said verification station is connected, to one or more further verification stations, following said previous transaction.

15. A verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

16. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

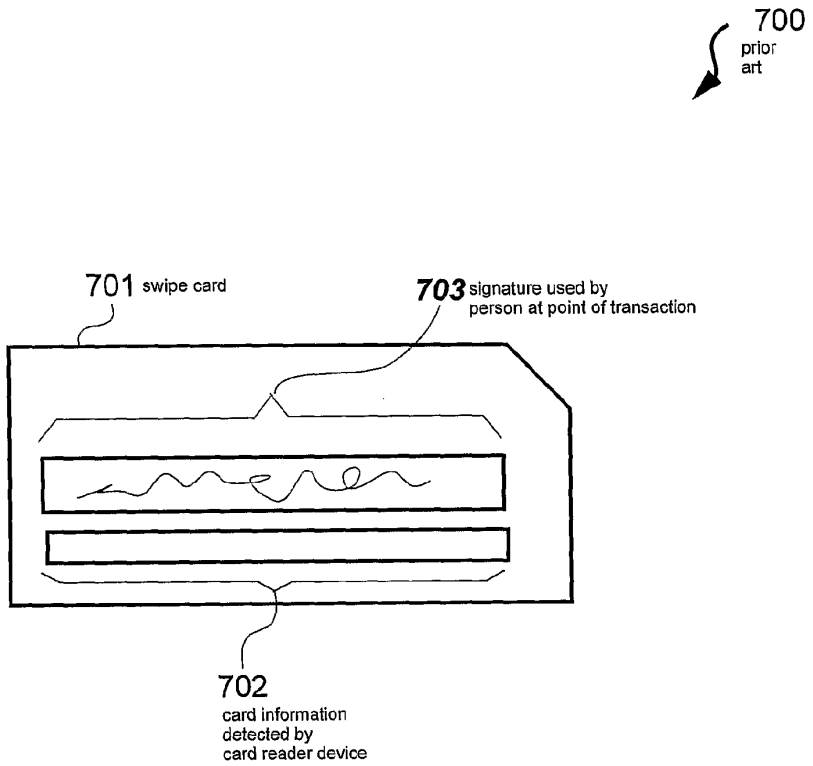


Fig. 1
prior art

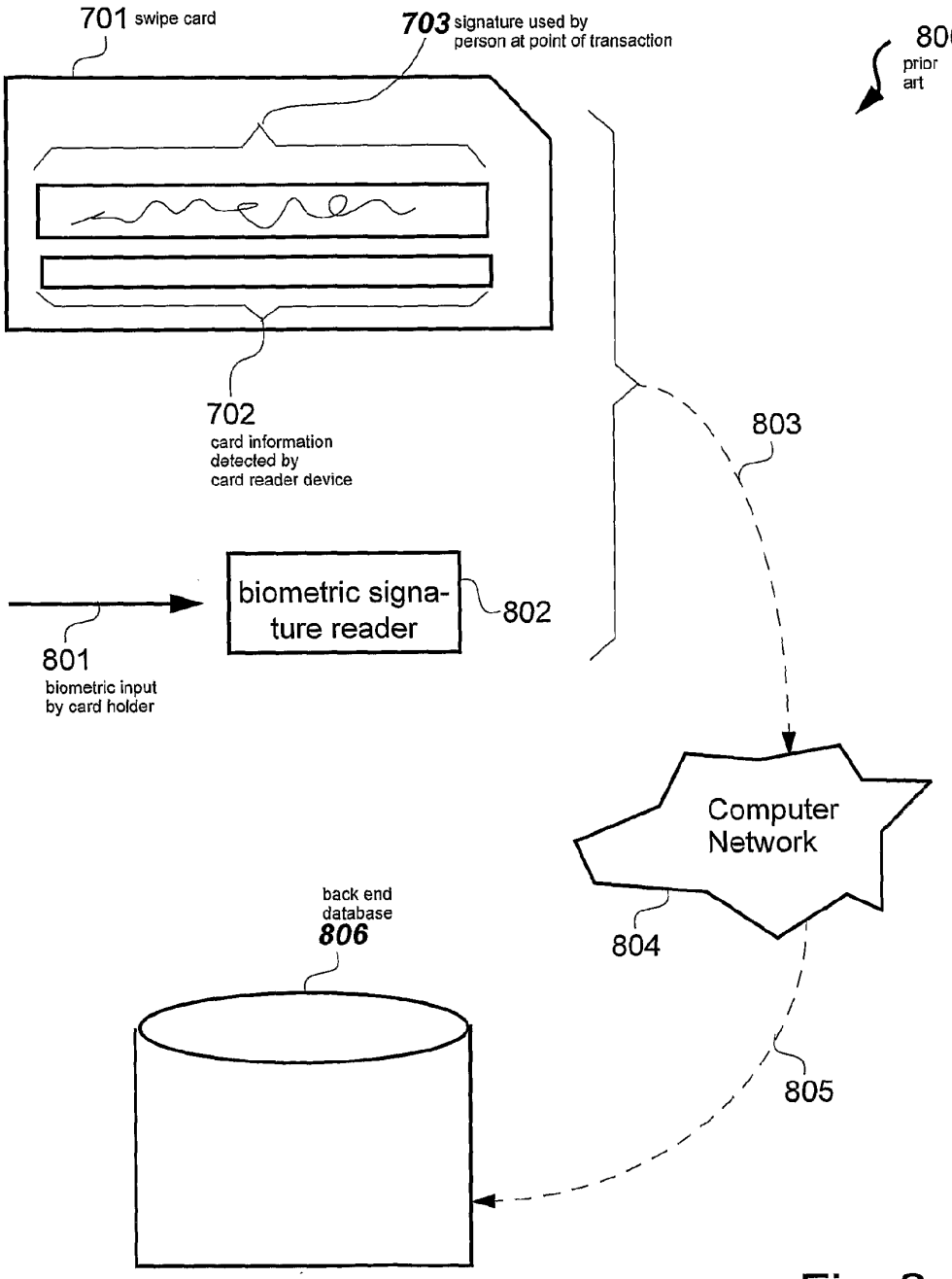


Fig. 2
prior art

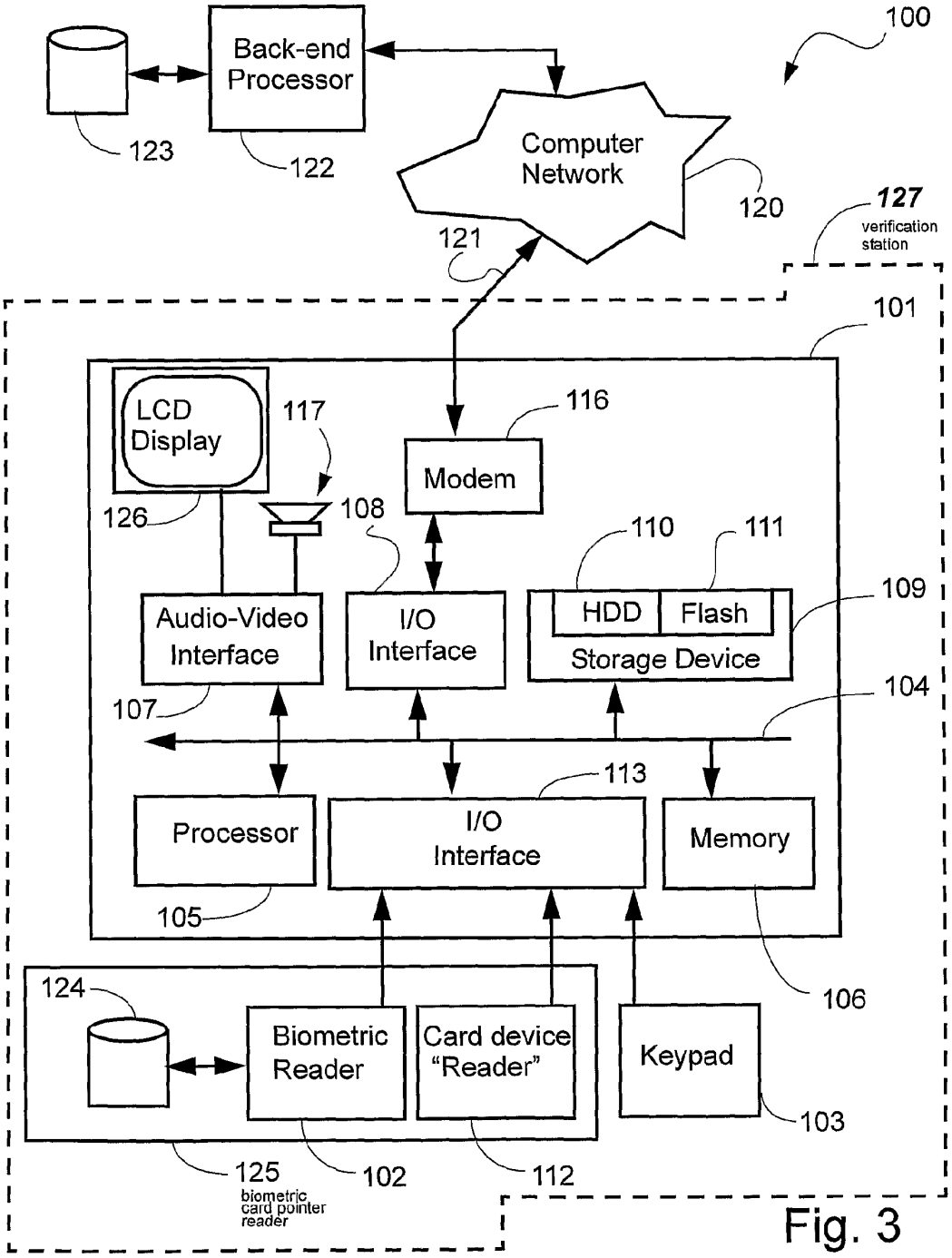

100
Back-end Processor
123
122
Computer Network
120
127
verification station
121
101
LCD Display
117
116
Modem
126
108
110
111
109
Audio-Video Interface
I/O Interface
HDD
Flash
Storage Device
107
104
113
Processor
I/O Interface
Memory
105
106
124
Biometric Reader
Card device "Reader"
Keypad
103
125
biometric card pointer reader
102
112

Fig. 3

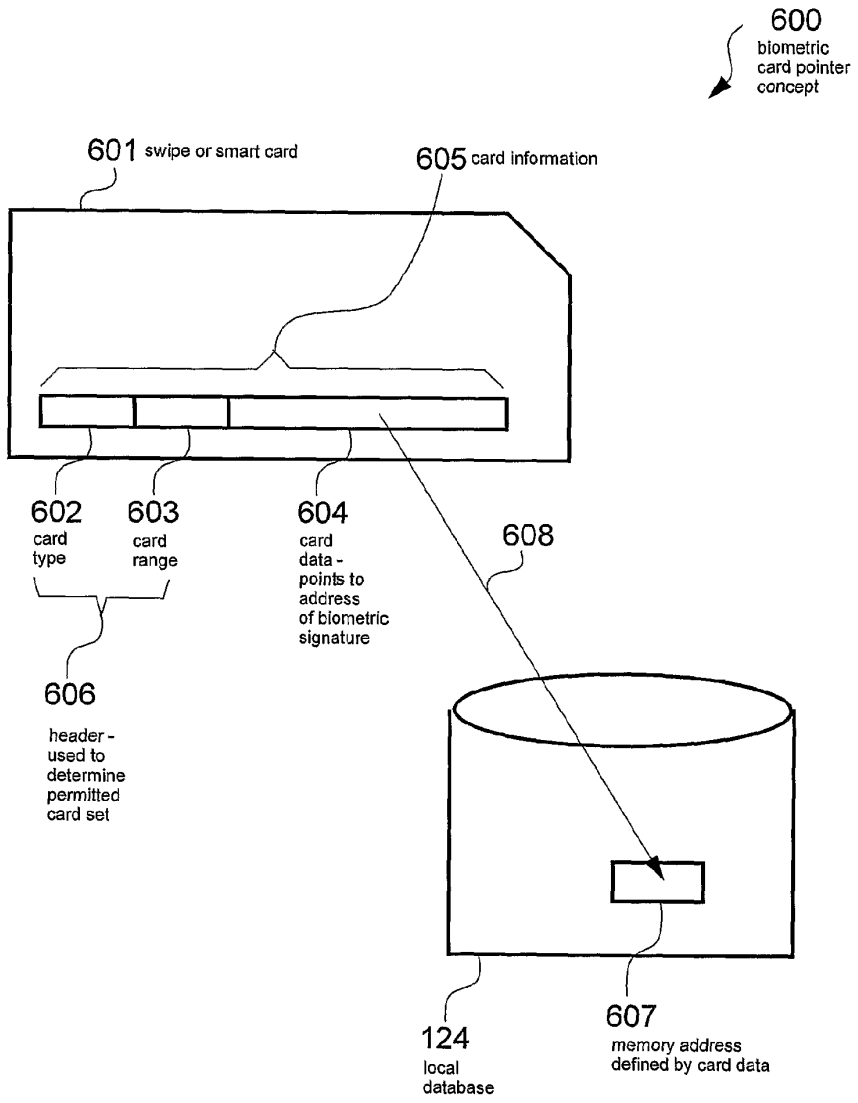

600
biometric
card pointer
concept
601 swipe or smart card
605 card information
602
card
type
603
card
range
604
card
data -
points to
address
of biometric
signature
608
606
header -
used to
determine
permitted
card set
124
local
database
607
memory address
defined by card data

Fig. 4

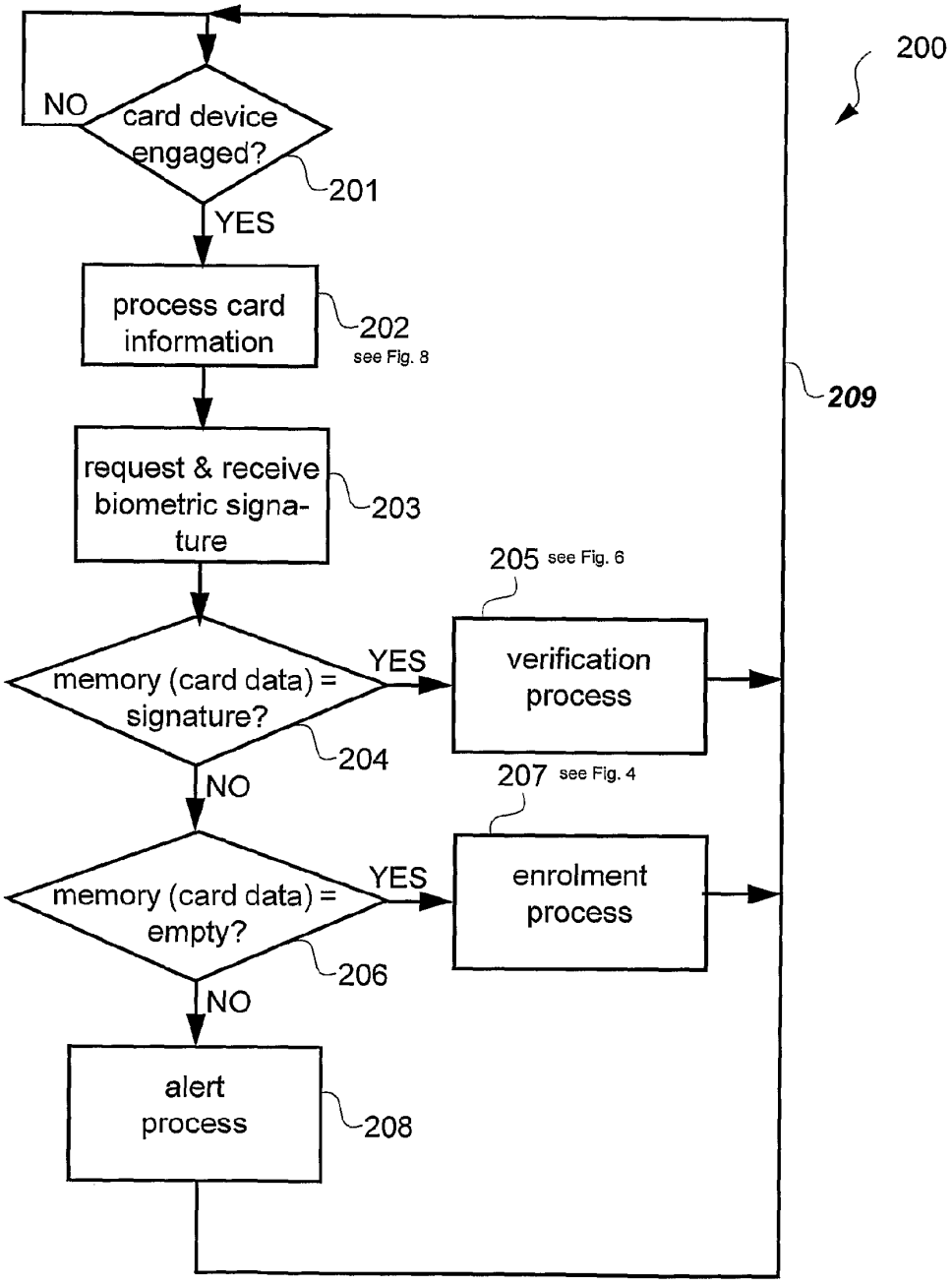

200
NO
card device engaged?
201
YES
process card information
202
see Fig. 8
209
request & receive biometric signature
203
205 see Fig. 6
memory (card data) = signature?
YES
verification process
204
NO
207 see Fig. 4
memory (card data) = empty?
YES
enrolment process
206
NO
alert process
208

Fig. 5

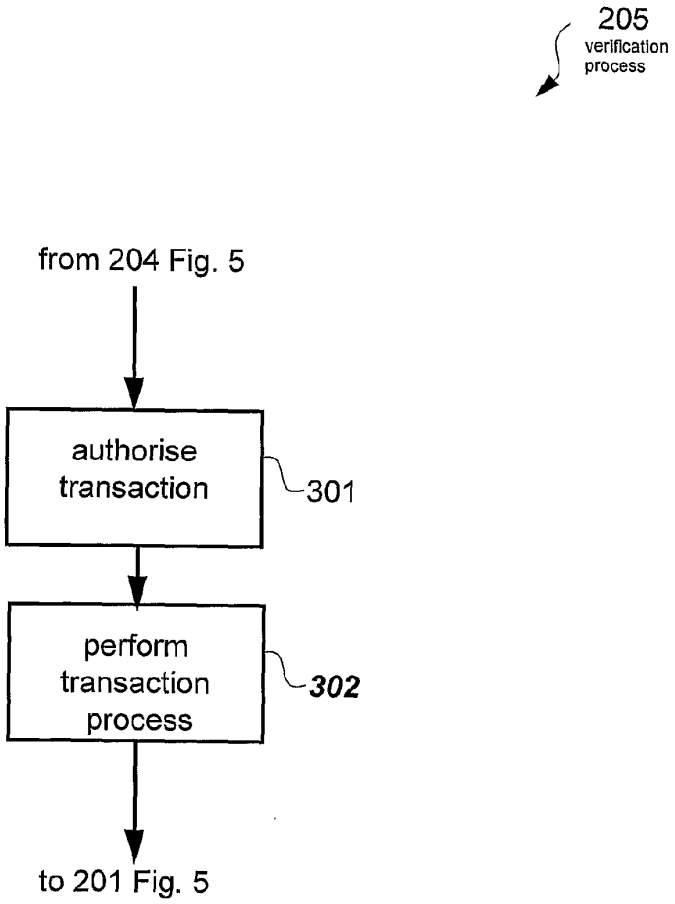
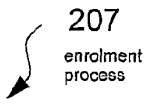

205
verification process
from 204 Fig. 5
authorise transaction
301
perform transaction process
302
to 201 Fig. 5

Fig. 6


207
enrolment process

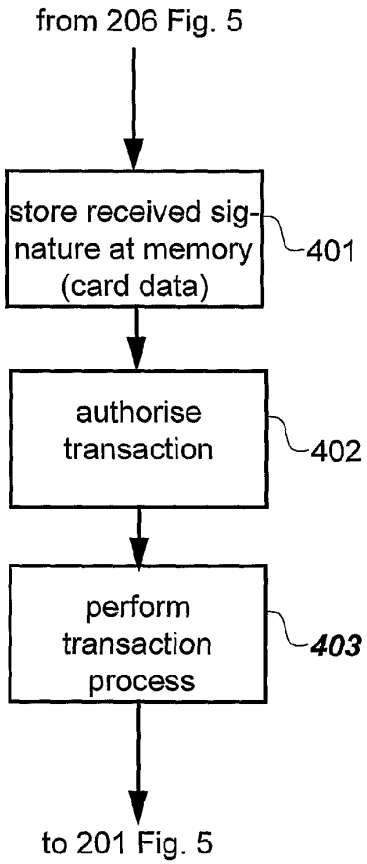

from 206 Fig. 5
store received signature at memory (card data)
401
authorise transaction
402
perform transaction process
403
to 201 Fig. 5

Fig. 7

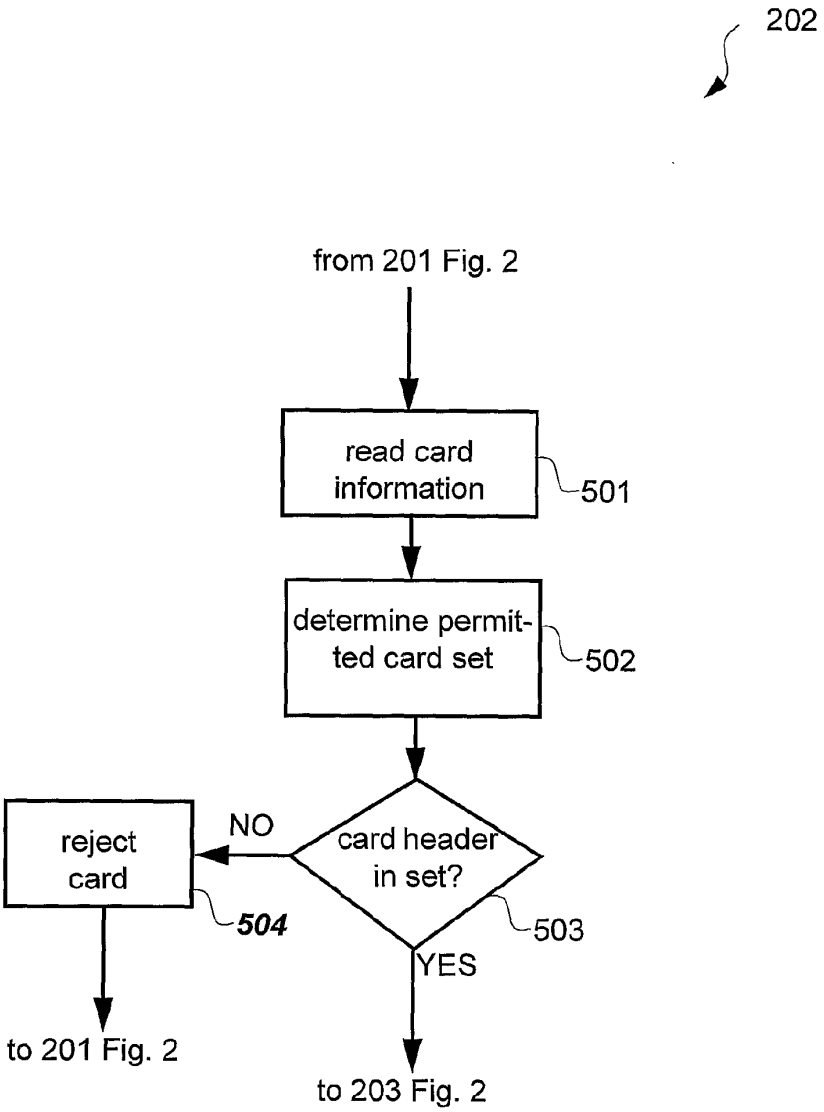

202
from 201 Fig. 2
read card information
501
determine permitted card set
502
card header in set?
503
NO
reject card
504
YES
to 201 Fig. 2
to 203 Fig. 2

Fig. 8

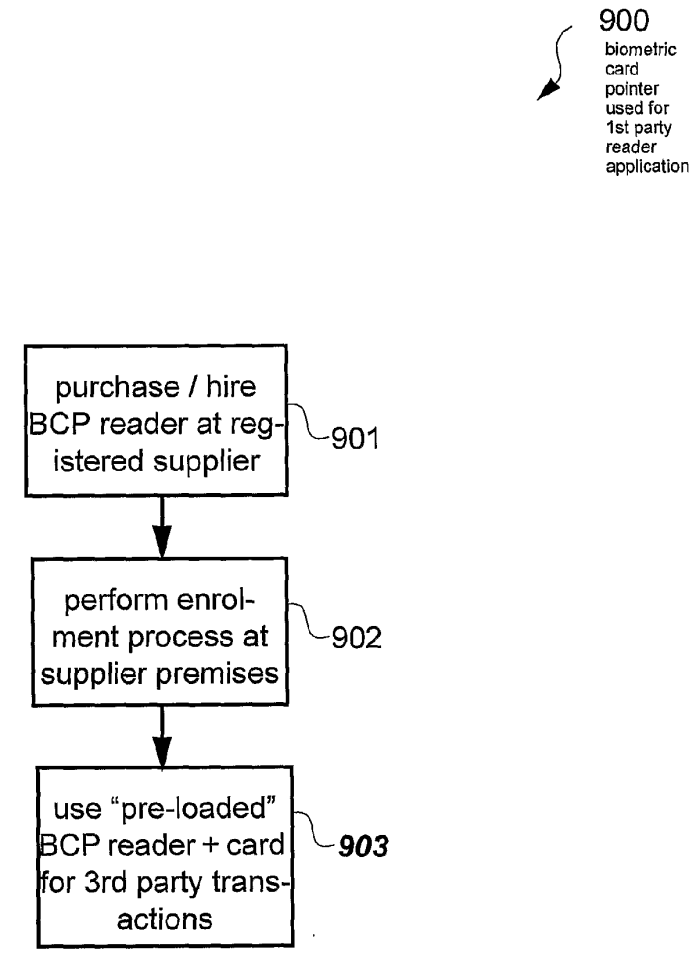

900
biometric card pointer used for 1st party reader application
purchase / hire BCP reader at registered supplier
901
perform enrolment process at supplier premises
902
use "pre-loaded" BCP reader + card for 3rd party transactions
903

Fig. 9

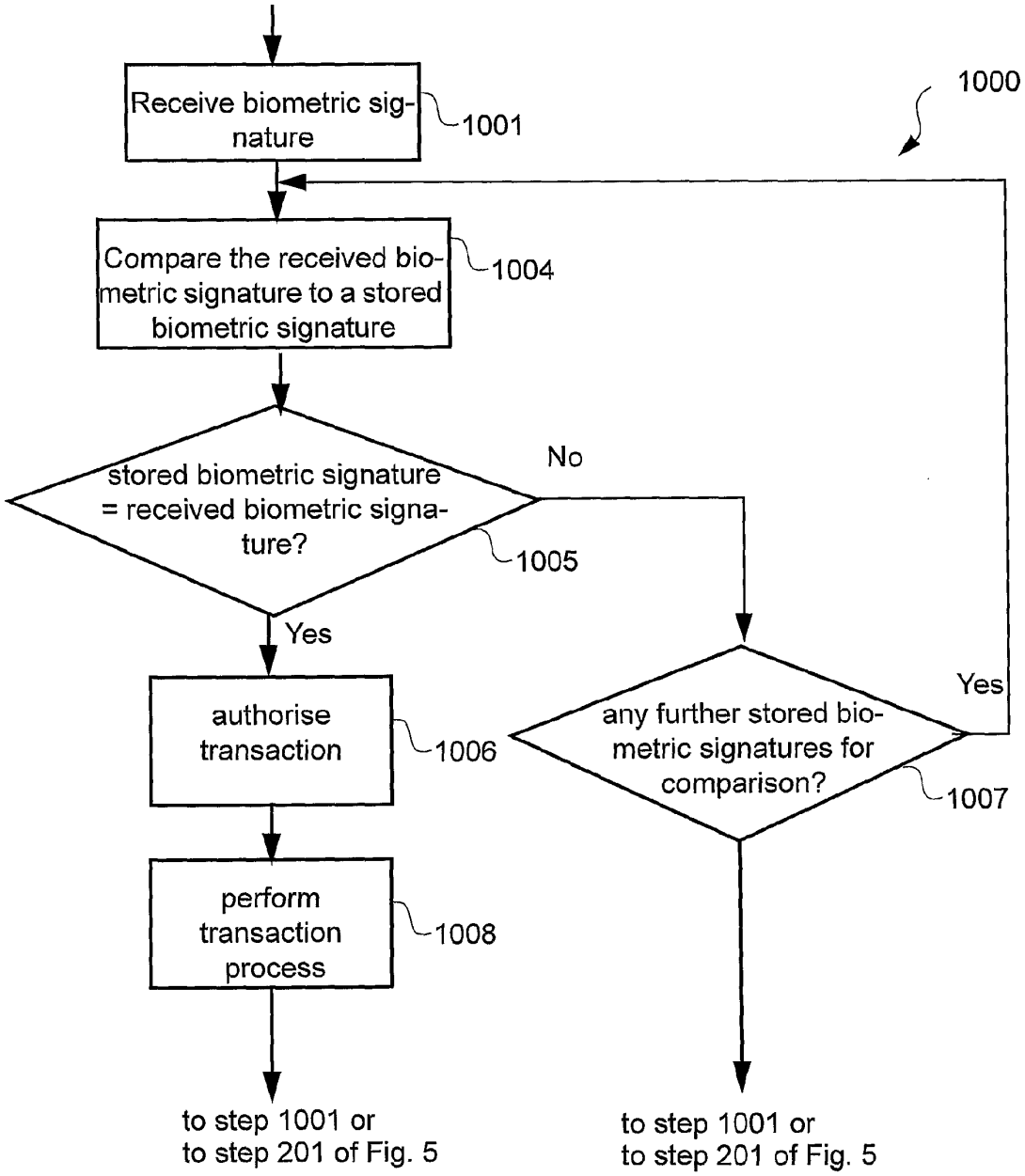

1000
Receive biometric signature
1001
Compare the received biometric signature to a stored biometric signature
1004
stored biometric signature = received biometric signature?
1005
No
Yes
authorise transaction
1006
perform transaction process
1008
to step 1001 or to step 201 of Fig. 5
any further stored biometric signatures for comparison?
1007
Yes
to step 1001 or to step 201 of Fig. 5

Fig. 10

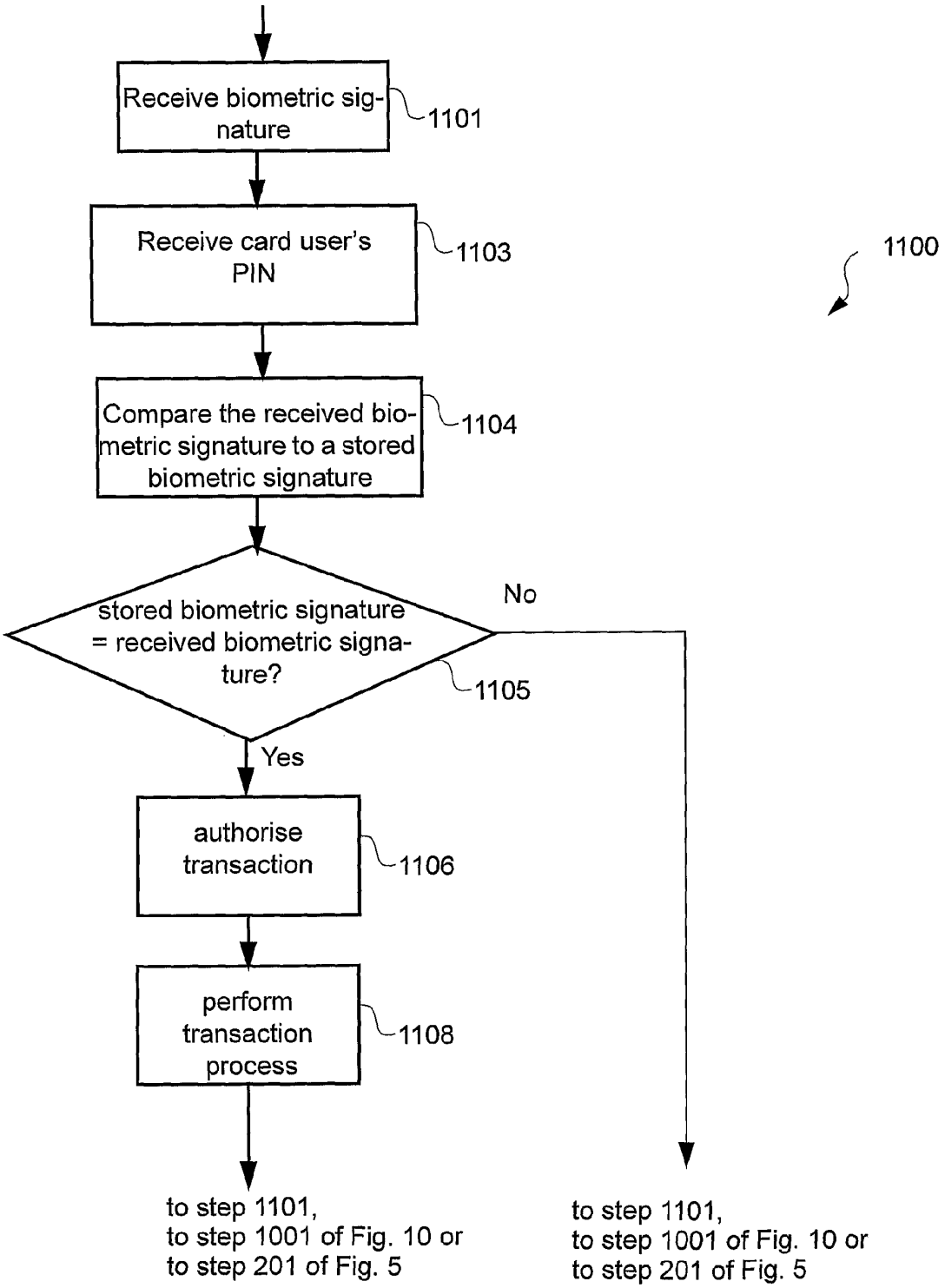

Receive biometric signature
1101
Receive card user's PIN
1103
1100
Compare the received biometric signature to a stored biometric signature
1104
stored biometric signature = received biometric signature?
1105
No
Yes
authorise transaction
1106
perform transaction process
1108
to step 1101, to step 1001 of Fig. 10 or to step 201 of Fig. 5
to step 1101, to step 1001 of Fig. 10 or to step 201 of Fig. 5

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/000366

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06K 9/00 (2006.01) ***H04K 1/00*** (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)
USPTO, WPAT: biometric, fingerprint, verify+, compare+, author+, transaction, payment, approval, access, secur+, smartcard, barcode, chip, magnetic strip, wireless, PIN, in-situ, local, in-built, stand-alone, isolate+, memory.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/019605 A (SECURICOM (NSW) PTY LTD) 22 February 2007 Entire document	1-16
X	CA 2412403 A (TAYLOR) 20 May 2003 Entire document particularly abstract	1-16
X	http://www.scmmicro.com/pdf/Smart_Card_Biometric_paper.pdf May 2002 Whole document (pages 1-21) particularly page 9	1-16
X	WO 2006/058039 A (SOLIDUA NETWORKS, INC.) 1 June 2006 Entire document	1-16

[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
21 April 2008	09 MAY 2008
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **JYOTI SHAMDASANI** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2836

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/000366

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/0039027 A (SHAPIRO) 17 February 2005 Entire document	1-16
A	US 2006/0104224 A (SINGH et al.) 18 May 2006 Entire document	1-16
A	US 6920561 A (GOULD et al.) 19 July 2005 Entire document	1-16
A	WO 2001/08055 A (SECURECOM LTD) 1 February 2001 Entire document	1-16
A	US 2005/036663 A (CASPI et al.) 17 February 2005 Entire document	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2008/000366

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					
WO	2007019605		NONE				
CA	2412403	CA	2363372	EP	1315118	US	7239727
		US	2003120933				
WO	2006058039	BR	PI0509496	CA	2562964	CN	1965325
		EP	1743276	KR	2007003845	US	6728397
		US	7231068	US	7349557	US	2003128866
		US	2004234117	US	2005097037	WO	2005098741
US	2005039027		NONE				
US	2006104224	JP	2006127502				
US	6920561		NONE				
WO	0108055	AU	55978/01	AU	59542/00	CN	1441932
		EP	1305749	HK	1058979	NZ	522686
		WO	0190962				
US	2005036663		NONE				

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

END OF ANNEX

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU2008/000366

International filing date: 14 March 2008 (14.03.2008)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2007901361
Filing date: 16 March 2007 (16.03.2007)

Date of receipt at the International Bureau: 07 April 2008 (07.04.2008)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/AU2008/000366

Australian Government

Patent Office
Canberra

I, DAVID CARNOVALE, EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2007901361 for a patent by MICROLATCH PTY LTD as filed on 16 March 2007.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Third day of April 2008

David Carnovale

DAVID CARNOVALE
EXAMINATION SUPPORT AND SALES

S&F Ref: 801105

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED:

Method and apparatus for performing a transaction using a verification station

Name and Address of Applicant:

Microlatch Pty Ltd,
an Australian company, ACN 059 640 747, of Unit 13, 145-147 Forest Road, Hurstville, New South Wales, 2220, Australia

Name of Inventor:

Christopher John Burke

This invention is best described in the following statement:

METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING A VERIFICATION STATION

Field of the Invention

The present invention relates generally to security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.

Background

This description makes reference to various types of "card device" and their associated "reader devices" (respectively referred to merely as cards and readers). The card devices all contain card information that is accessed by "coupling" the card device to an associated reader device. The card information is used for various purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account, gaining access to a restricted area or controlled device and so on. The card information is typically accessed from the card by a corresponding card reader which then sends the card information to a "back-end" system that completes the appropriate transaction or process. One type of card device is the "standard credit card" which in this description refers to a traditional plastic card 701 as depicted in **Fig. 1**. The standard credit card is typically "swiped" through a slot in a standard credit card reader in order to access card information 702 on the card 701. The card information 702 can alternately be encoded using an optical code such as a bar code, in which case the reader is suitably adapted. The standard credit card 701 also typically has the signature 703 of the card-owner written onto a paper strip on the card 701. This is used for verification of the identity of the person submitting the card when conducting a transaction using the card 701.

Another type of card device is the smart card (not shown) that typically has an on-board processor and a memory. The smart card typically has electrical contacts that

mate with corresponding contacts on a smart card reader (not shown) when accessing data in the memory of the smart card.

Still another type of card device is a proximity card (not shown) that typically has an on-board microchip. A proximity card reader sends out a low-level radio frequency (RF) signal, which energizes the microchip embedded in the card when the card is placed in close proximity to the reader. The proximity card then transmits data in the form of a unique code to the reader.

Still another type of card device is the wireless "key-fob" which is a small radio transmitter that emits an RF signal when a button on the fob is pressed. The RF signal can be encoded using the Wiegand protocol, or any other suitable protocol, such as rolling code or Bluetooth™ and can include encryption if desired. The key-fob typically has a processor and memory storing data that is sent via the transmitted signal to a corresponding receiver, which is the "reader device" for this type of card device.

The description also refers to "card user" and "card owner". The card user is the person who submits the card for a particular transaction. The card user can thus be the (authorised) card owner or an (unauthorised) person who has found or stolen the card.

Currently, the above described cards are heavily relied on both for financial transactions, as described above, and also for secure access. However, the cards are often used fraudulently. For example, a card may be used without the consent of the card owner to gain access to a bank account. Further, data stored on a card may be copied and used to gain access to a building or the like.

Clearly the signature 703 on the standard credit card 701 in **Fig. 1** can be forged. Thus, if the standard card 701 is stolen or lost, an unauthorised user can use the card provided that they can supply a sufficiently accurate version of the signature 703. The only recourse available to the card owner is to notify the card issuing company to "cancel" the card.

Current card devices such as the standard credit card, the smart card and the key-fob can have their security enhanced by requiring the card user to provide PIN (Personal Identification Number) information through a keypad to verify their identity prior to completing a transaction. However, PIN information can also be "stolen" by surveillance of the card owner's hands as the card owner operates the keypad.

Biometric verification can also be incorporated into current card systems to enhance security. In **Fig. 2** the card user swipes the standard card 701 through an associated card reader (not shown) that accesses the card information 702 on the card 701. The card user also provides a biometric signature 801, for example by pressing their thumb against a biometric (e.g., fingerprint) reader 802. The card information 702 that is read by the card reader (not shown), together with the biometric signature that is read by the biometric (fingerprint) reader 802, are sent, as depicted by a dashed arrow 803, a computer network 804, and a further dashed arrow 805, to a back-end system including a database 806 and associated processor (not shown).

In this arrangement, the card owner needs to have previously registered their biometric signature 801 and the card information 702 for pre-loading onto the back-end database 806. Having done so, the back-end processor (not shown) compares the pre-loaded information on the database 806 with the information received at 805, in order to check that the card holder of the card 701 is the (authorised) card owner and that the card itself is valid, in which case the transaction in question can proceed. Clearly this arrangement requires a central repository (806) of card information 702 and biometric signatures 801. This is cumbersome and potentially compromises the privacy and security of the holder of the card 701. This arrangement also requires complex back-end database management and the communications network 804. Furthermore, the front-end biometric signature reader 802 requires storage and/or processing capabilities for the biometric signatures. This results in a complex and expensive solution.

Privacy concerns have also been raised against the arrangement of **Fig. 2** which involves centralised storage and processing of personal information including biometric information. These concerns have slowed widespread use of biometrics to enhance user verification.

Another disadvantage of the arrangement of Fig. 2 is that even once the card owner's biometric signature 801 and card information 702 has be pre-loaded onto the back-end database 806, the card owner is still required to carry the card and to validate the card for each transaction. This is inconvenient as the card is often lost or damaged.

Summary

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

Disclosed are arrangements which seek to address the above problems by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, a biometric signature reader, the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form), an alphanumeric keypad (optional), and a communication module for communicating with back-end system that may be remotely accessible over a network.

As described herein, when the description refers to "the storing of a biometric signature" in a memory, a person skilled in the art would understand that rather than the actual biometric signature it is a representation of the biometric signature that is actually stored in the memory. This representation may be referred to as a "biometric template" or "template".

The card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase). The biometric signature is stored at a memory address together with a copy of the

card information on the user's card as read by the card reader of the verification station. The memory address may be defined by the ("unique") card information on the user's card. The term "unique" means unique in the context of a permitted set of cards associated with the verification station. This is described in more detail in regard to **Fig. 8.**

All future uses (referred to as uses in the verification phase) of the particular verification station by the user of the aforementioned card requires the user to merely submit a biometric signature (e.g., thumb print or retinal scan etc.), which is compared to the signatures stored in the memory associated with the verification station. Once the submitted biometric signature has been matched to one of the biometric signatures stored in the memory, the card information stored with the stored biometric signature is sent to the back-end system.

An authorised user will be automatically verified by the arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update, allowing entry to a restricted area etc. will simply proceed as normal. The biometric signature of an unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user.

The described arrangements require virtually no modification at all of the back-end systems or the (front-end) card. The additional administrative overheads associated with the described arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The described arrangements also potentially have a reduced impact on privacy of card users. The biometric signatures stored in the local database of the verification station can be made off limits to anyone, or limited to law enforcement agencies, depending on the administrative environment in which the arrangements are implemented. Users of current card systems can learn to use

the described arrangements without much effort, needing only to provide a biometric signature.

According to one aspect of the present invention there is provided a method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

According to another aspect of the present invention there is provided a verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

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

thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

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 will now be described with reference to the drawings, in which:

Fig. 1 depicts a standard credit card;

Fig. 2 shows the card of **Fig. 1** being used together with biometric verification;

Fig. 3 is a functional block diagram of a special-purpose computer system upon which described methods for the described arrangements can be practiced;

Fig. 4 illustrates the use of a standard card in the described arrangements;

Fig. 5 is a flow chart of a process for using the verification station of **Fig. 3**;

Fig. 6 shows the verification process of **Fig. 5** in more detail;

Fig. 7 shows the enrolment process of **Fig. 5** in more detail;

Fig. 8 shows the card information process of **Fig. 5** in more detail;

Fig. 9 shows an alternate use for the described arrangements; and

Fig.10 is a flow chart of a process for using the verification station of **Fig. 3**.

Detailed Description including Best Mode

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. 3 is a functional block diagram of a system 100 in which the described arrangements can be practiced. The methods described herein particularly lend themselves to implementation on the special-purpose computer system 100 such as that shown in **Fig. 3** wherein the processes of **Figs. 5-8, 9** and 10 may be implemented as software, such as an application program executing within the computer system 100. In particular, the steps of the described methods are effected by instructions in the software that are carried out by a verification station 127. The verification station 127 is typically constructed in a tamper-proof manner, both physically and electronically, to prevent unauthorised access to the inner mechanism of the verification station 127. 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 described 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 verification station 127 from the computer readable medium, and is then executed by the verification station 127. 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 effecting the described arrangements.

The computer system 100 consists of a computer module 101, input devices such as a biometric reader 102, a card reader 112, and a keypad 103, output devices including

an LCD (Liquid Crystal Display) display device 126 and a loudspeaker 117. The computer module 101 uses a Modulator-Demodulator (Modem) transceiver device 116 for communicating to and from a communications network 120, for example connectable via a telephone line 121 or other functional medium. The modem 116 can be used to obtain access to a back end system including a processor 122 and back-end database 123 over the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The computer module 101 typically includes at least one processor unit 105, and a memory unit 106, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The module 101 also includes a number of input/output (I/O) interfaces including an audio-video interface 107 that couples to the LCD display 126 and loudspeaker 117, an I/O interface 113 for the keypad 103, biometric reader 102 and card reader 112, and an interface 108 for the modem 116. In some implementations, the modem 1116 may be incorporated within the computer module 101, for example within the interface 108.

A storage device 109 is provided and typically includes a hard disk drive 110 and a flash memory 111. The components 105 to 111 and 113 of the computer module 101, typically communicate via an interconnected bus 104 and in a manner that results in a conventional mode of operation of the computer system 100 known to those in the relevant art.

Typically, the application program is resident on the hard disk drive 110 and read and controlled in its execution by the processor 105. Intermediate storage of the program and any data fetched from the network 120 may be accomplished using the semiconductor memory 106, possibly in concert with the hard disk drive 110. In some instances, the application program may be supplied to the user encoded on the flash

memory device 111, or alternatively may be read by the computer module 101 from the network 120 via the modem device 116.

Still further, the software can also be loaded into the computer system 100 from other computer readable media. 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 computer system 100 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 computer module 101. 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.

As illustrated in **Fig. 4,** a standard card 601 has card information 605 typically comprising three fields, namely 602 which is the card type, 603 which is the card range, and 604 which comprises card data specific to the particular card 601. In the described arrangements, the card data 604 may act as the memory reference which points, as depicted by an arrow 608, to a particular memory address 607 in the local database 124 in the verification station 127 of **Fig. 3.** The fields 602 and 603, which together form a header 606, can be used by the described system to determine if the card 601 is to be processed according to the described methods or not. This is described in more detail in regard to **Fig. 8.**

In an initial enrolment phase, the card user couples their card 601 (or key-fob or other card device) to the card reader 112. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM). The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other

unique signature, into the biometric reader 102. The card data 604 defines the location 607 in the local database 124 where their unique biometric signature is to be stored. In the described arrangements, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 is then also stored at the location 607 in the local database 124. For example, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

Thereafter, in later verification phases, the card user is merely required to present their unique biometric to the biometric reader 102 in order to perform a transaction. In this instance, the biometric signature provided by the user is compared to each of the signatures stored in the local database 124. Once verification is confirmed, through a match of the provided biometric signature to one of the stored signatures, the card information 605 is transferred from the local database 124 within the verification station 127 to the back-end processor 122 for completion of the transaction.

Importantly, the back-end processor 122 does not see the difference between receiving the card information 605 from the verification station 127, and receiving it from a conventional card reader in the absence of the verification station implementing the described arrangements. This means that back-end processes (depicted by the back-end processor 122 and the back-end database 123) need no modification when incorporating the described arrangements into current card systems. There are additional elements in the verification station 127 (see **Fig. 3**) compared to the normal card reader, however this is a relatively simple and inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Alternatively, rather than only providing their biometric signature in later verification phases, the user may choose to also couple their card 601 to the card reader 112. In this instance, after coupling their card 601 to the card reader 112, the card user is

required to again present their unique biometric to the biometric reader 102. In this instance, rather than the biometric signature provided by the user being compared to all of the signatures stored in the local database 124 to determine a match, the biometric signature provided by the card user is only compared to the biometric signature stored at the memory location 607 defined by the card data 604 read from their card 601 by the card reader 112. Again, once verification is confirmed, the card information 605 is transferred from the local database 124 of the verification station 127 to the back-end processor 122 for completion of the transaction.

Fig. 5 shows a process 200 for using the verification station 127. In the described process 200, rather than only providing their biometric signature in verification phases following the initial enrolment phase, the user couples their card 601 to the card reader 112 to perform a transaction. As described below, in another process 1000, in later verification phases following the initial enrolment phase, the user may merely present their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 201, the processor 105 determines if the card 601 has been read by the card reader 112. If this is not the case, then the process 200 follows a NO arrow back to the step 201. If, on the other hand, the card 601 has been read by the card reader 112, then the process 200 follows a YES arrow to a step 202 (see **Fig. 8** for more details). In the step 202, the processor 105 buffers the card information 605 that is read from the card 601 by the card reader 112 and processes the card information 605. In a following step 203 a request is presented to the card holder to provide a biometric signature to the biometric reader 102. This request can be provided in an audio fashion by means of the audio interface 107 and the speaker 117, this being driven by suitable software running on the processor 105. Alternatively or in addition, a suitable message can be displayed on the LCD display 126 by suitable software running on the processor 105.

In response to the aforementioned request, the holder of the card 601 provides a biometric signature to the biometric reader 102. After the signature has been received by the step 203, the process 200 is directed to a step 204 that reads the contents of the local database 124 at an address defined by the card data 604. If the contents of this memory address match, to a sufficiently high degree of correspondence, the biometric signature received in the step 203 via the biometric reader 102, then the process follows a YES arrow to a step 205 (see **Fig. 6** for more detail). It is noted that if the step 204 returns a YES value, then the biometric signature at the noted memory address was written into the local database 124 in an earlier enrolment phase. It is also noted that the step 204 reads the biometric signature stored at a single memory address defined by the card data 604 and checks the stored biometric signature against the biometric signature received in the step 203. In the process 200, there is no need to search the database 124 to see if there is a match. Thus, the process 200 provides a particularly simple and fast biometric verification check. Once the step 205 has completed the verification process, the process 200 is directed according to an arrow 209 back to the step 201.

Returning to the step 204, if the biometric signature of the local database 124 at the memory address defined by the card data 604 does not match the signature received by the biometric reader 102, then the process 200 follows NO arrow to a step 206. In the step 206, the processor 105 determines if the biometric signature of the memory location defined by the card data 604 is empty. If this is the case, then the process 200 follows a YES arrow to a step 207 that performs an enrolment process for the card 601 (see **Fig. 7** for more detail). The process 200 then follows the arrow 209 back to the step 201.

Returning to the step 206, if the biometric signature of the aforementioned memory location is not empty, then this means that (i) the card 601 and the associated biometric signature of the card holder have previously been used for the enrolment process 207, and (ii) the biometric signature now received in the step 203 does not match

the signature stored in the local database 124. In this event, the process 200 follows a NO arrow to a step 208 that performs an alert process. The process 200 then follows the arrow 209 back to the step 201. The alert process 208 can include sending an alert message from the verification station 127 to the back end processor 122 for later action, for example by the police. The alert process can also store the (unauthorised) signature for later use by the law enforcement authorities.

As noted in regard to **Fig. 3**, the verification station 127 is constructed in a tamper proof fashion to ensure that the process 200 of **Fig. 5**, particularly the steps 204-207, are not accessible to unauthorised tampering.

Fig. 6 shows the verification process 205 from **Fig. 5** in more detail. The process 205 is entered from the step 204 in **Fig. 5**, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207 applied to the card in question.

After the step 301, a step 302 performs the transaction process, whatever that may be. Thus, for example, if the process 200 of **Fig. 5** relates withdrawal of cash from an Automatic Teller Machine (ATM), then the step 302 comprises the user specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). After completion of the transaction process by the step 302, the process 205 is directed back to the step 201 in **Fig. 5**.

Fig. 7 shows the enrolment process step 207 from **Fig. 5** in more detail. The process 207 is entered from the step 206 in **Fig. 5**, after which a step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604 received in the step 202 of **Fig. 5**. At step 401, the process

207 also retrieves the card information 605 that was previously buffered in the memory 106 at step 202, and stores the card information in the local database 124 at the memory address defined by the card data 604. The aforementioned step 401 can store the biometric signature and card information 605 in encrypted form to reduce the probability that the signature can be acquired for unauthorised use, thus helping ensure the privacy of the card owner. As described above, the biometric signature is stored as a biometric template representing the biometric signature provided by the user. The following steps 402 and 403 have the same respective functions as the corresponding steps 301 and 302 in **Fig. 6**. After completion of the step 403, the process 207 is directed back to the step 201 in **Fig. 5**.

Fig. 8 shows the step 202 in **Fig. 5** that is concerned with the processing of the card information 605 from the card 601 when the card 601 is read by the card reader 112 in the step 202 of **Fig. 5**. The process 202 is entered from the step 201 in **Fig. 5**, after which a step 501 reads the card information 605 from the card 601 using the card reader 112 and buffers the card information 605 in the memory 106. In a following step 502, the processor 105 retrieves predefined "permitted card set" parameters to determine the "permitted card set" for the verification station 127 in question. The permitted card set parameters may be retrieved from the local database 124 or from the hard disk drive 110, for example, and be also stored in the memory 106. A separate, or overlapping, permitted card set may be defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the described processes at any given verification station 127. This has the advantage of ensuring that the local database 124 does not overflow, and it also provides control over which users make use of which verification stations. However, the permitted card set for any given verification station 127 is only limited by the size of the local database 124. Card information 605 from any number of cards 601 may be stored in the local database 124 of a particular verification station 127 if

the amount of memory is sufficient. In one embodiment, the processor 105 may periodically run a clean-up process where all card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months) may be deleted from the local database 124.

In a following step 503 the processor 105 compares the header 606 against the predefined permitted card set parameters to determine if the card 601 belongs to the permitted card set for the verification station 127 in question. If this is the case, then the process 202 is directed by a YES arrow to the step 203 in **Fig. 5**. If, on the other hand, the card header 606 does not belong to the permitted card set for the particular verification station 127, then the step 202 follows a NO arrow from the step 503 to a step 504. In the step 504, the processor 105 rejects the card that has been entered into the card reader 112. This rejection can take the form of a message displayed on the LCD display 126 and/or a corresponding audio message via the speaker 117. Thereafter, the process 202 is directed back to the step 201 in **Fig. 5**. It is noted that even if the verification station does not reject the card not belonging to the permitted card set for the verification station 127 in question, the back-end processor 122 can do so.

In addition to the predefined permitted card set, other administrative functions can be provided by the described arrangements. Thus, the predefined permitted card set details can be amended and/or the signatures stored in the database 124 can be deleted by a system administrator. The system administrator may also periodically perform the clean-up process described above to delete card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months), so that the local database 124 does not overflow. Audit trail information is also stored in the verification station 127 and can be downloaded for audit purposes. The audit information typically includes information of which cards have been submitted to the verification station and the time stamps of the card submissions. Biometric signatures

are typically not part of the downloadable audit information, and require a greater level of authorisation (such as that associated with law enforcement agencies) for access.

Fig. 10 shows a process 1000 for performing a transaction using the described arrangement. The process 1000 may be performed by the owner of the card 601, for example, in later verification phases once the owner has previously performed the initial enrolment phase, so that their biometric signature and a copy of the card information 605 has been stored in the local database 124. Accordingly, the stored copy of the card information 605 was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127. In the described process 1000, in such a later verification phase, the user may merely present their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 1001, the processor 105 receives a biometric signature as provided by the owner of the card 601 to the biometric reader 102. The biometric signature may be temporarily buffered in the memory 106. After the signature has been received at the step 1001, the process 1000 is directed to a step 1004 that reads the contents of the local database 124 at a first address and compares a biometric signature stored at that first address to the biometric signature received at step 1001. In this instance, the first address may be selected randomly. Alternatively, the first address may be selected in an ordered fashion. For example, the first address may be selected as the first address in a particular block of memory.

Accordingly, at step 1004, the process 1000 compares the received biometric signature, inputted to the biometric reader 102 and buffered in memory 106, to a biometric signature stored at a first address in the local database 124 (or memory) incorporated into the verification station 127. As will be described, if the received biometric signature stored at the first memory address does not match the biometric

signature stored at the first address, then the process 1000 compares the received biometric signature to one or more further biometric signatures stored in the local database 124 (or memory) incorporated into the verification station 127.

At the next step 1005, if the biometric signature stored at the first memory address matches, to a sufficiently high degree of correspondence, the inputted biometric signature received in the step 1001, then the process 1000 follows a YES arrow to a step 1006. It is noted that if the step 1005 returns a YES value, then the biometric signature at the first memory address was written into the memory 124 in an earlier enrolment phase together with the card information 605.

At step 1006, the process 1000 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches one of the biometric signatures previously stored in the local database 124 by a previous enrolment process 207 applied for the card 601 in question. After the step 1006, a next step 1008 performs the transaction process, whatever that may be, using the copy of the card information 605 stored in the local database 124. Typically, the transaction process will require the card information 605 to be transferred from the verification station 127 to the back-end processor 122 for completion of the transaction. As an example of a transaction process, if the process 1000 of **Fig. 10** relates to the withdrawal of cash from an Automatic Teller Machine (ATM), then the step 1008 comprises the card owner specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). Accordingly, the stored copy of the card information 605 used in the performed transaction process was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127.

After completion of the step 1008, the process 1000 is directed back to step 1001 or to the step 201 in **Fig. 5**.

If, at step 1005, the biometric signature stored at the first memory address does not match the biometric signature received in the step 1001, then the process 1000 follows a NO arrow to a step 1007. At step 1007, if the processor 105 determines that there are no further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1001 or to the step 201 in **Fig. 5.** If the processor 105 determines at step 1007 that there are further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1004. At the next execution of step 1004, the processor 105 reads the contents of the local database 124 at a further address and compares a biometric signature stored at that further address to the biometric signature received at step 1001.

Fig. 9 shows another application 900 to which the described arrangements can be applied. In a first step 901 a person purchases or hires a verification station implemented in a portable form. A step 901 is performed at a registered supplier premises. Accordingly in a following step 902, the enrolment process is performed in controlled circumstances at the supplier premises. The "controlled conditions" referred to mean that the enrolment process is performed under conditions where the identity of the holder of the card 601 is verified, using a driving licence, passport or equivalent identification document, this ensuring that the enrolment process enrols the true owner of the card in an authorised manner.

In a following step 903, the verification station together with the card 601 can be used for third party transactions. Thus, in one example, the holder of the card 601 can take the portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises.

This station identification number is then transmitted to the on-line casino back-end processes together with the card information 605. This type of application does require some modification of the back-end processes.

In the arrangements described above, a card user is required to enrol at each individual verification station 127. However, in another arrangement, a user may be able to enrol at one verification station 127 and the user's biometric signature and card information 605 may be broadcast over the communications network 120 to one or more other verification stations connected to the communications network 120. The broadcast biometric signature and card information 605 may then be stored in the local databases of each of those verifications stations to which the biometric signatures and card information 605 have been broadcast. Such an arrangement may be referred to as a 'minimum enrolment' arrangement. The minimum enrolment arrangement is particularly advantageous for Electronic Funds Transfer Point of Sale (EFTPOS) transactions, ATM transactions and the like. For example, the verification station 127 described above may be added to an EFTPOS terminal or ATM. The broadcasting of the biometric signature and card information 605 increases the security of the transactions made with the verification stations.

In an initial enrolment phase of the minimum enrolment arrangement, the card user couples their card 601 to the card reader 112 of the verification station 127 in a similar manner to that described above. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM) of the verification station 127. The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader 102. The buffered card data 604 defines the location 607 in the local database 124 where the card user's unique biometric signature is to be stored. Once the biometric signature has been stored in the local database 124 at the location 607, the card information 605

buffered in memory 106 may then also stored at the location 607 in the local database 124. As described above, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

In the minimum enrolment arrangement, following the storing of the user's biometric signature in the local database 124, a copy of the user's biometric signature, together with a copy of the card information 605 read from the user's card, is broadcast over the communications network 120 to one or more of the other verification stations connected to the network. The card user's unique biometric signature together with the card information 605 corresponding to the biometric signature is then stored in the local database (e.g., 124) of each verification station to which the biometric signature and card information 605 has been broadcast. The biometric signature and card information 605 is stored at a particular memory address, as defined by the card data 604, in each of the local databases. The storing of the card information 605 in the each of the local databases of the verification stations allows biometric only transactions as described above to be performed.

In another alternative of the minimum enrolment arrangement, rather than broadcasting the individual biometric signatures and card information to each of the other verification stations connected to the network 120 upon an enrolment taking place, updates to the contents of a local database within a particular verification station 127 or indeed the entire contents of the local database may be broadcast periodically (e.g., overnight).

Accordingly, in the minimum enrolment arrangement described above, the card user is only required to enrol on one verification station 127 connected to the communication network 127 and each of the other verifications stations connected to the communications network 120 will receive a copy of the card user's enrolled biometric signature and possibly the card information 605 corresponding to that biometric signature.

Thereafter, in later verification phases, the user may make biometric only transactions, as described above with reference to Fig, 10, at each of the verification stations connected to the communications network 120 after enrolling on one of the verification stations 127. Alternatively, the user may also choose to couple their card to the card reader (e.g., 112) of one of the verifications stations and present their unique biometric signature in order to perform a transaction, as described above.

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the described arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards, government issued card (e.g., the Australian Medicare card) and others. The arrangements can, in general be used in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature. For example, in the case of the Australian Medicare card, following enrolment at a verification station 127 located at a particular medical centre, the entire card information 605 of the user's Medicare card is stored in the local database 124 of the verification station 127 located at the medical centre.

As another example, the described arrangements can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying

platform. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature to withdraw funds.

Furthermore, the described arrangements can be used for secure access to a hotel room or any other room, building, cabinet, or apparatus to which secure access is required.

In the hotel room example, the hotel may have a verification station 127 mounted on each door of the hotel. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining a particular room number and planned departure date. The number on the card is preferably one of an increasing sequence of numbers. The number preferably increases over a period of time and is also encrypted. A verification station 127 positioned at the door of the room corresponding to the room number may be configured so that the verification station 127 will only allow enrolments and verifications if the number stored on a presented card correctly identifies the room and is in the correct sequence. The verification station 127 may also include a real time clock to match actual time against the planned date of departure. After the guest enrols their biometric signature at the verification station 127 using the aforementioned card in the manner described above, the arrangement will give them secure access to their room for the duration of their stay.

Following enrolment, the above hotel guest may use their card and a biometric signature (e.g., a fingerprint) to enter the room. Alternatively, the guest may merely present their biometric signature to enter the room as described above negating the requirement for the guests to carry the room card, plus increasing security and convenience. The verification station 127 may also be configured so that the guest may choose not to enrol their biometric signature if they do not wish to have a record of their biometric signature stored within the local database of the verification station 127.

The verification station 127 located at the door of a particular hotel room or other secure access entry as described above may also allocate memory for storage of any number of biometric signatures (e.g., fingerprints) to be associated with the new card. This allows the hotel guest and all associated guests (e.g., the hotel guest's family) to enrol their individual biometrics at the verification station 127. The enrolment may simply be achieved, for example, by inserting the card and placing a finger on the biometric reader 102, for each guest. Following this enrolment stage, the card or the biometric signature can be used to gain access to the room, again, negating the requirement for each of the guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the biometric signature (e.g., fingerprints) memory address is that the time and date of departure can also be added to the same memory location. Therefore, the hotel application also allows other related data to be added to the memory location, enhancing the capability of the described arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the described arrangements is in regard to passport control and customs. The arrangements can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to **Figs. 5** and **10.**

In each of the arrangements described above, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 is then also stored at the location 607 in the local database 124. However, in alternative

arrangements, local databases 124 associated with each of the verification stations 127 may only contain biometric signatures. In this instance, it is only the biometric signatures and card data 604 which is broadcast following an enrolment. However, such arrangements require the card 601 to be used for all transactions.

Finally, in each of the arrangements described above, the verification stations 127 may be configured to provide the card user with the option of performing transactions with the card 601 only. For example, the card user may not wish to provide their biometric signature. In this instance, the card user may use their card only to perform a transaction with the verification stations in a conventional manner.

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.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

In the context of this specification, the word "comprising" means "including principally but not necessarily solely" or "having" or "including", and not "consisting only of". Variations of the word "comprising", such as "comprise" and "comprises" have correspondingly varied meanings.

The claims defining the invention are as follows:

1. A method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

2. The method according to claim 1, wherein the card information is stored in said memory with the matching one of said previously stored biometric signatures.

3. A method according to claim 1, wherein the card device is one of:

a card device in which the card information is encoded in a magnetic strip;

a card device in which the card information is encoded in a bar code;

a smart card device in which the card information is stored in a solid state memory on the smart card; and

a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

4. A method according to claim 1, further comprising the step of outputting information indicating that the user of the card device is not authorised.

5. A method according to claim 4 wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

6. A method according to claim 1, wherein the stored card information and said one stored biometric signature was broadcast over a communications network to which said verification station is connected, to one or more further verification stations, following said previous transaction.

7. A verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

8. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to one or more further biometric signatures stored in a memory incorporated into the verification station; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches one of said stored biometric signatures, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory during a previous transaction process using a card device reader incorporated into the verification station.

DATED this 15th Day of March 2007

MICROLATCH PTY LTD

Patent Attorneys for the Applicant

SPRUSON&FERGUSON

2007901361 16 Mar 2007

700
prior
art

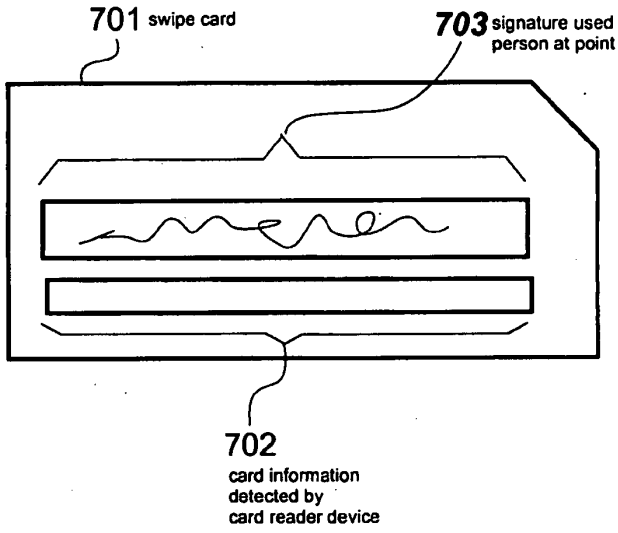


Fig. 1
prior art

2007901361 16 Mar 2007

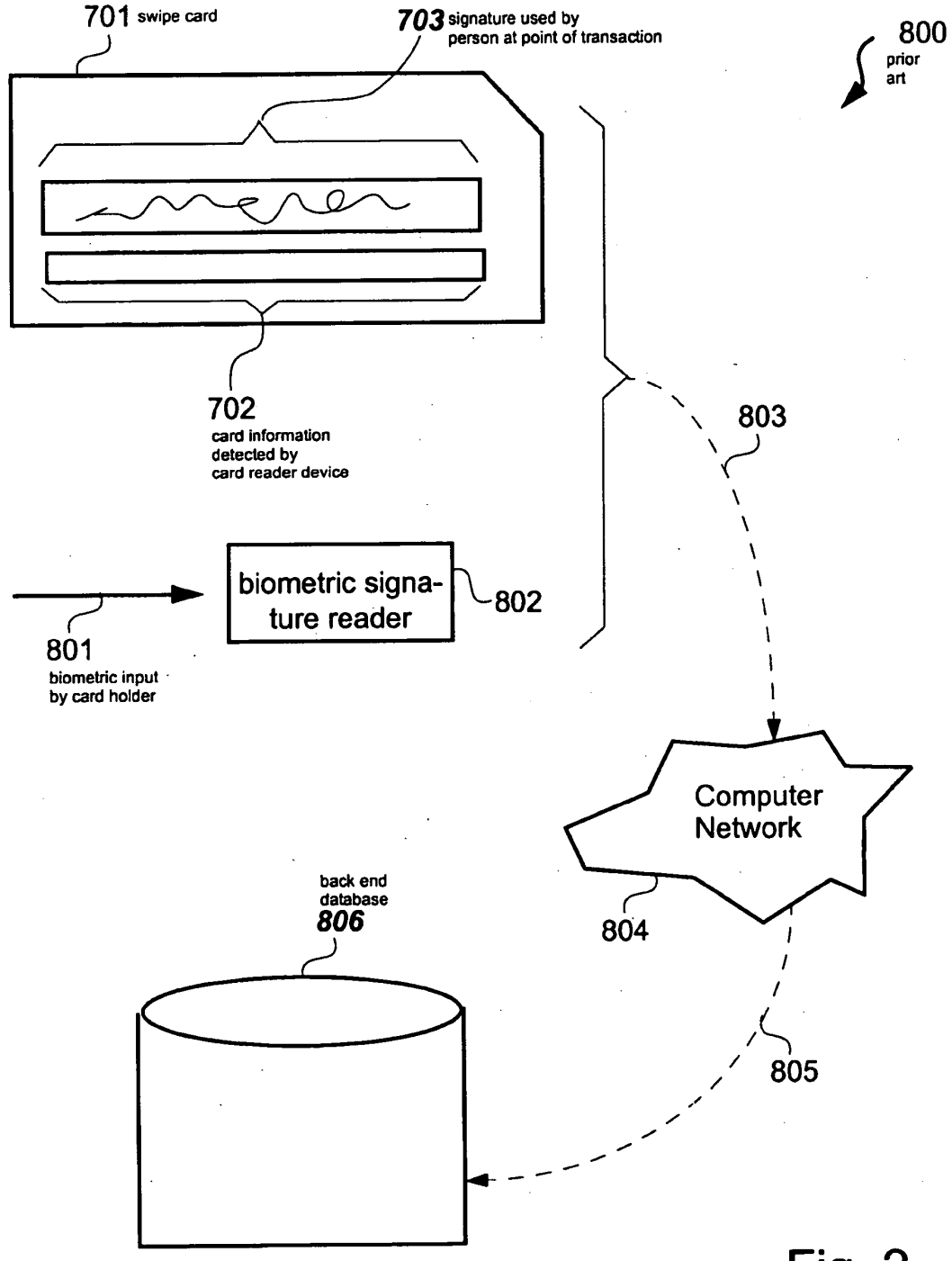


Fig. 2
prior art

150307

801105.FM

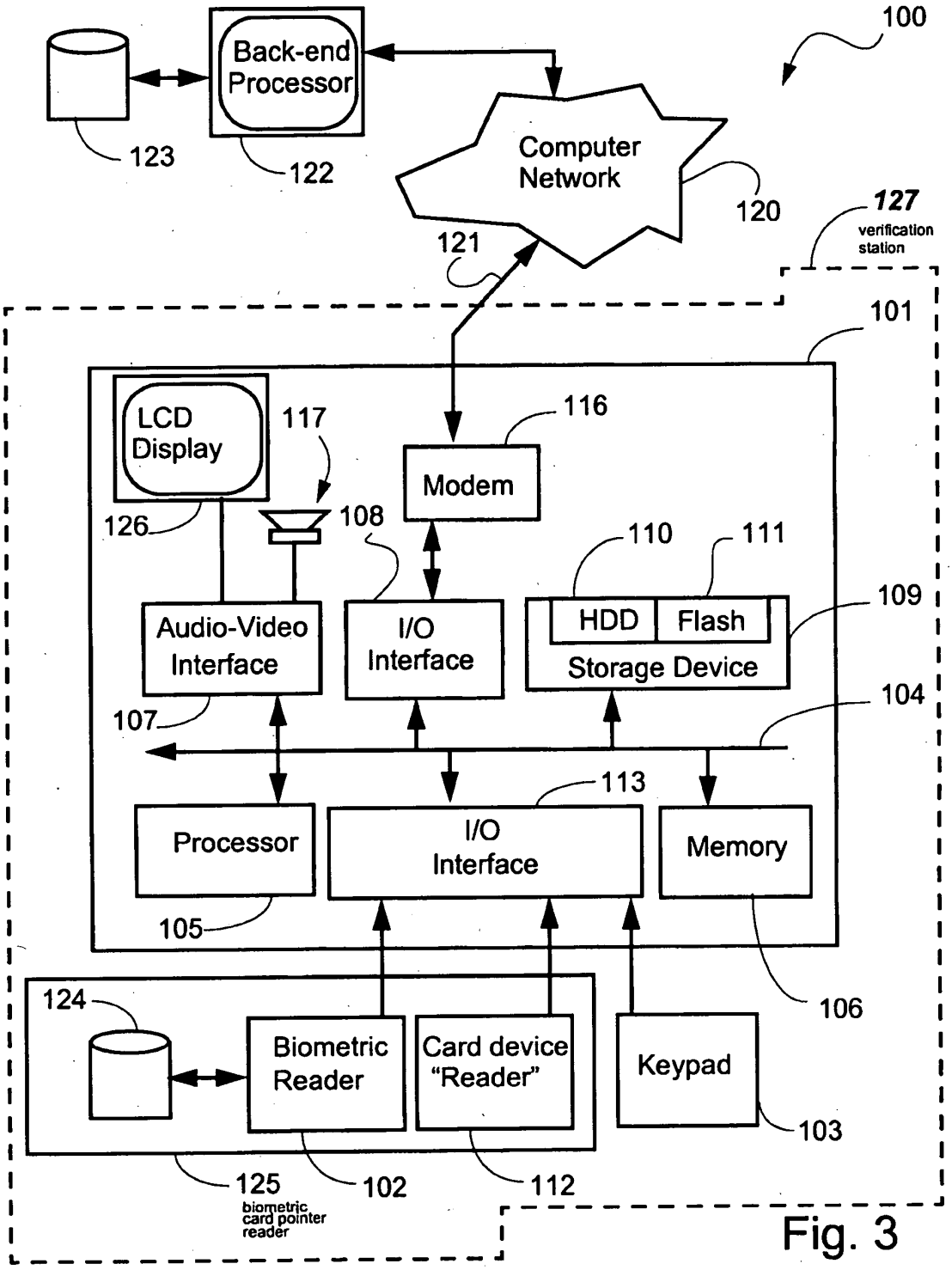


Fig. 3

150307

801105.FM

2007901361 16 Mar 2007

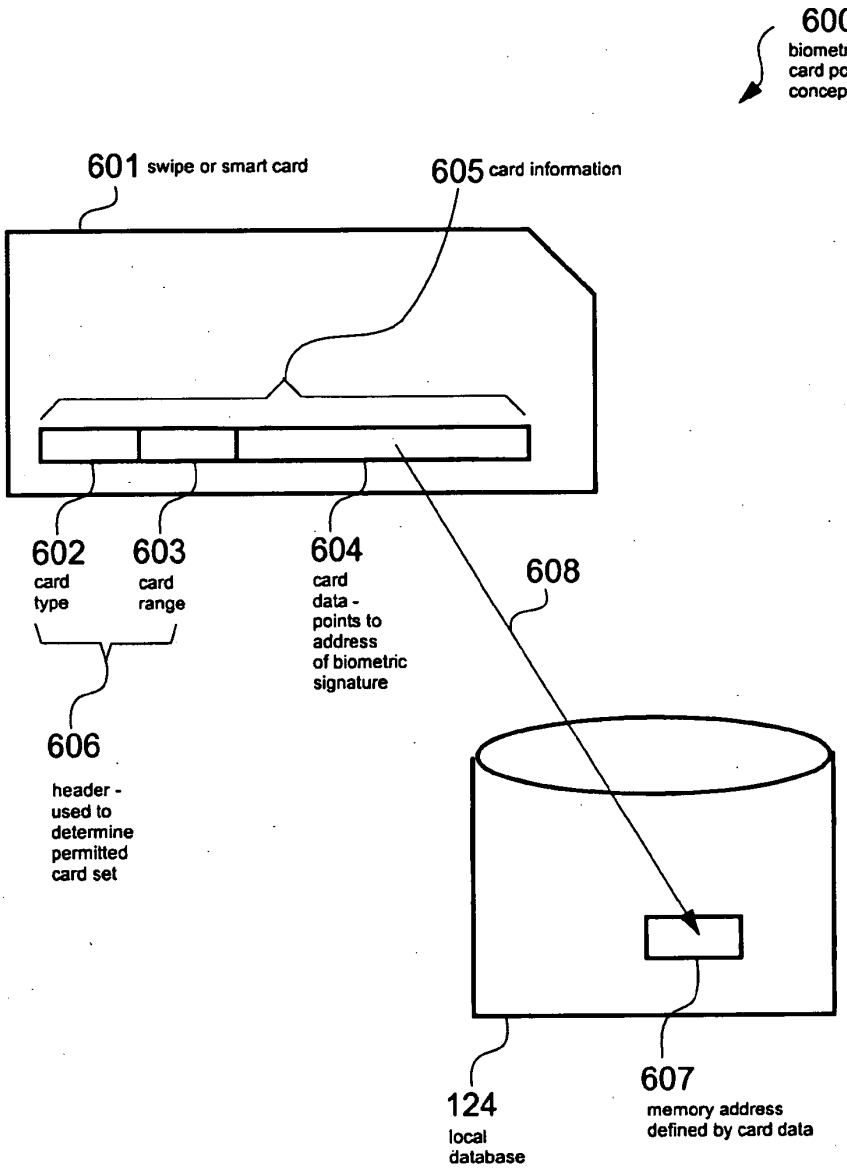


Fig. 4

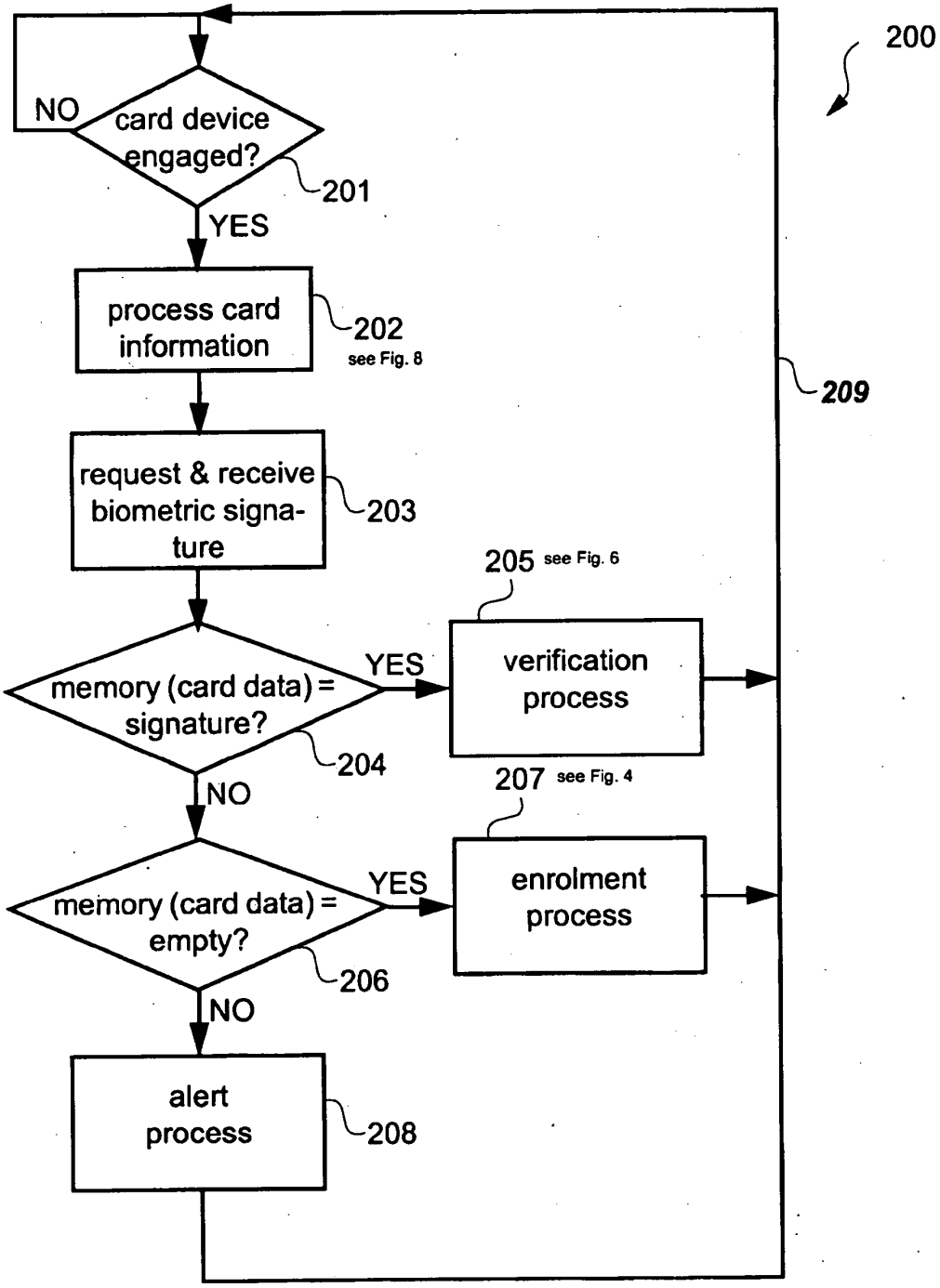


Fig. 5

2007901361 16 Mar 2007

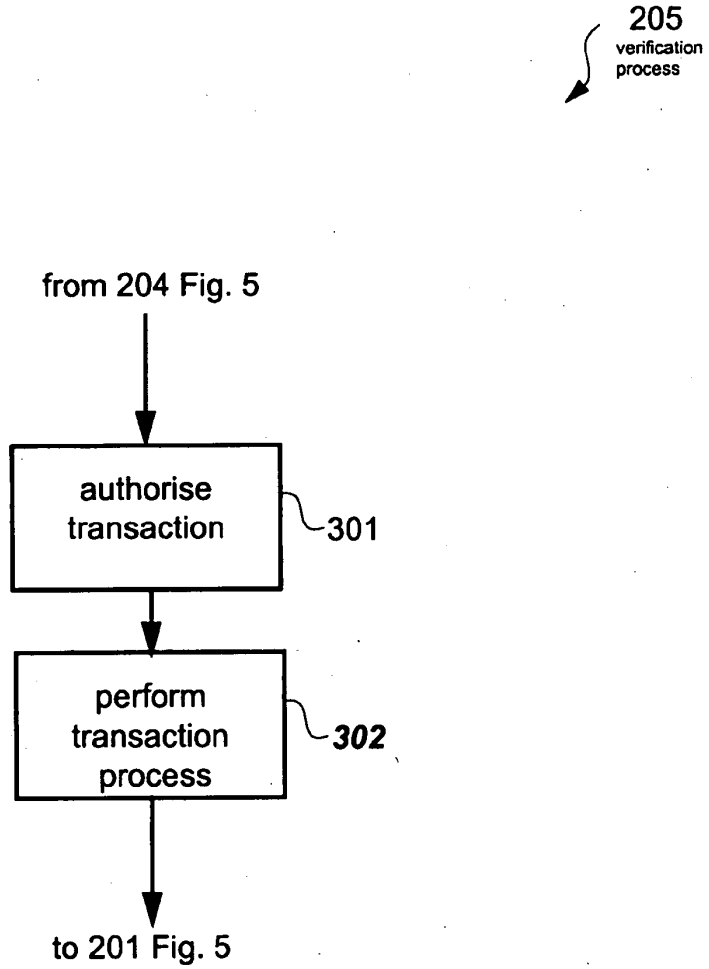


Fig. 6

2007901361 16 Mar 2007

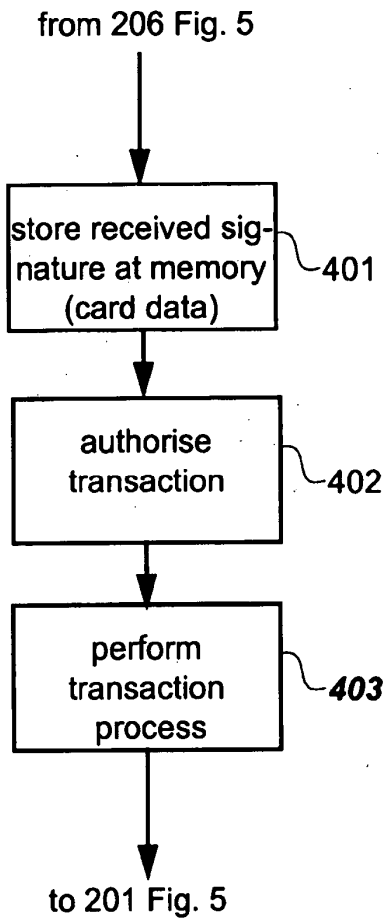


Fig. 7

2007901361 16 Mar 2007

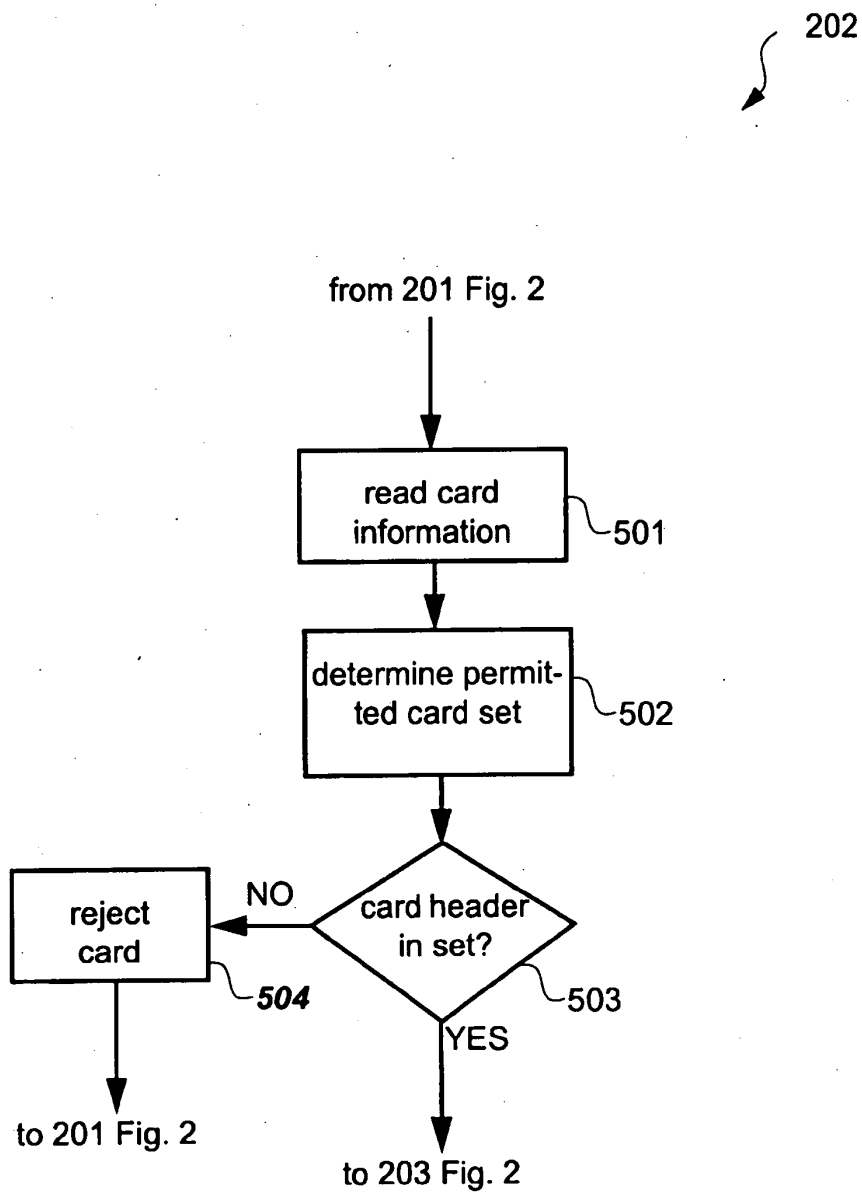


Fig. 8

2007901361 16 Mar 2007

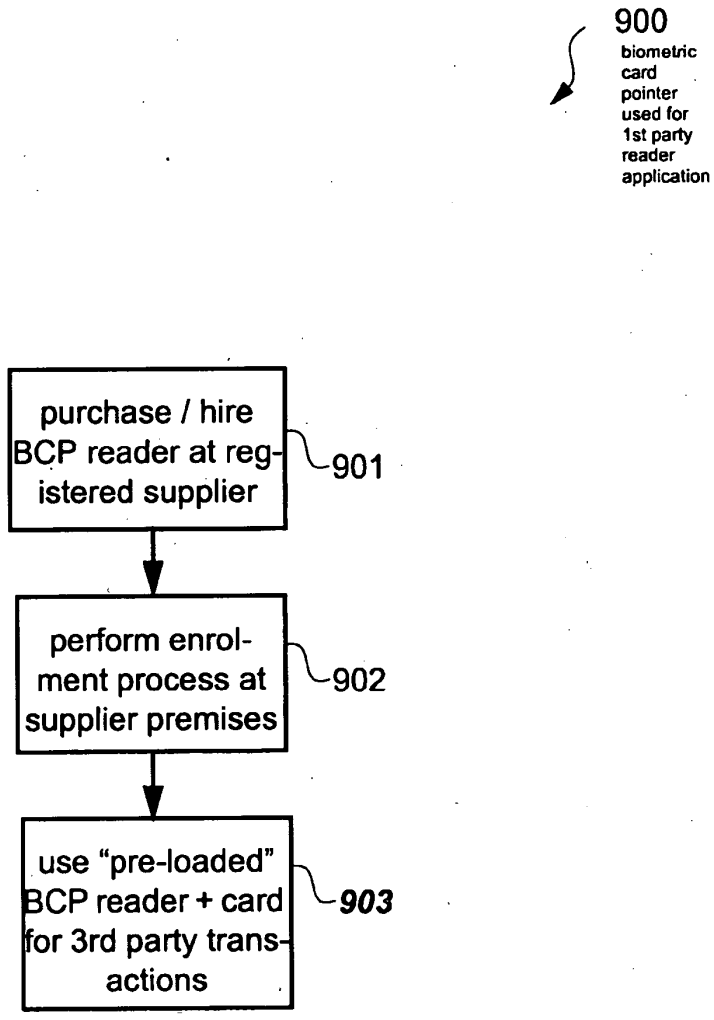


Fig. 9

2007901361 16 Mar 2007

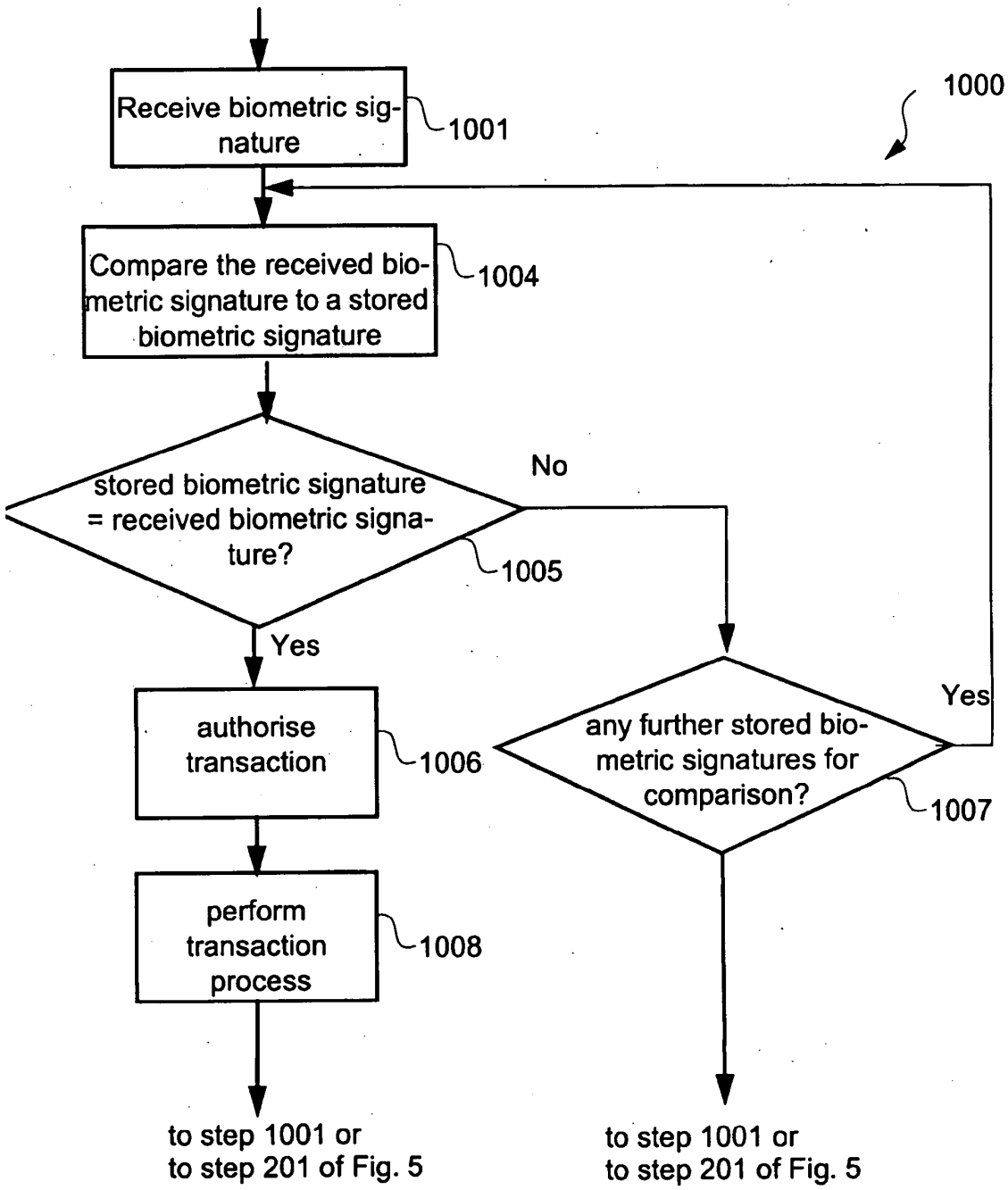


Fig. 10

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU2008/000366

International filing date: 14 March 2008 (14.03.2008)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2007901683
Filing date: 29 March 2007 (29.03.2007)

Date of receipt at the International Bureau: 07 April 2008 (07.04.2008)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/AU2008/000366

Australian Government

Patent Office
Canberra

I, DAVID CARNOVALE, EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2007901683 for a patent by MICROLATCH PTY LTD as filed on 29 March 2007.

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

WITNESS my hand this
Third day of April 2008

DAVID CARNOVALE
EXAMINATION SUPPORT AND SALES

S&F Ref: 805006

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED:

Method and apparatus for performing a transaction using a verification station

---

Name and Address of Applicant:

Microlatch Pty Ltd,
an Australian company, ACN 059 640 747, of Unit 13, 145-147 Forest Road, Hurstville, New South Wales, 2220, Australia

Name of Inventor:

Christopher John Burke

This invention is best described in the following statement:

METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING A VERIFICATION STATION

Field of the Invention

The present invention relates generally to security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.

Background

This description makes reference to various types of "card device" and their associated "reader devices" (respectively referred to merely as cards and readers). The card devices all contain card information that is accessed by "coupling" the card device to an associated reader device. The card information is used for various purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account, gaining access to a restricted area or controlled device and so on. The card information is typically accessed from the card by a corresponding card reader which then sends the card information to a "back-end" system that completes the appropriate transaction or process.

One type of card device is the "standard credit card" which in this description refers to a traditional plastic card 701 as depicted in **Fig. 1**. The standard credit card is typically "swiped" through a slot in a standard credit card reader in order to access card information 702 on the card 701. The card information 702 can alternately be encoded using an optical code such as a bar code, in which case the reader is suitably adapted. The standard credit card 701 also typically has the signature 703 of the card-owner written onto a paper strip on the card 701. This is used for verification of the identity of the person submitting the card when conducting a transaction using the card 701.

Another type of card device is the smart card (not shown) that typically has an on-board processor and a memory. The smart card typically has electrical contacts that

mate with corresponding contacts on a smart card reader (not shown) when accessing data in the memory of the smart card.

Still another type of card device is a proximity card (not shown) that typically has an on-board microchip. A proximity card reader sends out a low-level radio frequency (RF) signal, which energizes the microchip embedded in the card when the card is placed in close proximity to the reader. The proximity card then transmits data in the form of a unique code to the reader.

Still another type of card device is the wireless "key-fob" which is a small radio transmitter that emits an RF signal when a button on the fob is pressed. The RF signal can be encoded using the Wiegand protocol, or any other suitable protocol, such as rolling code or Bluetooth™ and can include encryption if desired. The key-fob typically has a processor and memory storing data that is sent via the transmitted signal to a corresponding receiver, which is the "reader device" for this type of card device.

The description also refers to "card user" and "card owner". The card user is the person who submits the card for a particular transaction. The card user can thus be the (authorised) card owner or an (unauthorised) person who has found or stolen the card.

Currently, the above described cards are heavily relied on both for financial transactions, as described above, and also for secure access. However, the cards are often used fraudulently. For example, a card may be used without the consent of the card owner to gain access to a bank account. Further, data stored on a card may be copied and used to gain access to a building or the like.

Clearly the signature 703 on the standard credit card 701 in **Fig. 1** can be forged. Thus, if the standard card 701 is stolen or lost, an unauthorised user can use the card provided that they can supply a sufficiently accurate version of the signature 703. The only recourse available to the card owner is to notify the card issuing company to "cancel" the card.

Current card devices such as the standard credit card, the smart card and the key-fob can have their security enhanced by requiring the card user to provide PIN (Personal Identification Number) information through a keypad to verify their identity prior to completing a transaction. However, PIN information can also be "stolen" by surveillance of the card owner's hands as the card owner operates the keypad.

Biometric verification can also be incorporated into current card systems to enhance security. In **Fig. 2** the card user swipes the standard card 701 through an associated card reader (not shown) that accesses the card information 702 on the card 701. The card user also provides a biometric signature 801, for example by pressing their thumb against a biometric (e.g., fingerprint) reader 802. The card information 702 that is read by the card reader (not shown), together with the biometric signature that is read by the biometric (fingerprint) reader 802, are sent, as depicted by a dashed arrow 803, a computer network 804, and a further dashed arrow 805, to a back-end system including a database 806 and associated processor (not shown).

In this arrangement, the card owner needs to have previously registered their biometric signature 801 and the card information 702 for pre-loading onto the back-end database 806. Having done so, the back-end processor (not shown) compares the pre-loaded information on the database 806 with the information received at 805, in order to check that the card holder of the card 701 is the (authorised) card owner and that the card itself is valid, in which case the transaction in question can proceed. Clearly this arrangement requires a central repository (806) of card information 702 and biometric signatures 801. This is cumbersome and potentially compromises the privacy and security of the holder of the card 701. This arrangement also requires complex back-end database management and the communications network 804. Furthermore, the front-end biometric signature reader 802 requires storage and/or processing capabilities for the biometric signatures. This results in a complex and expensive solution.

Privacy concerns have also been raised against the arrangement of **Fig. 2** which involves centralised storage and processing of personal information including biometric information. These concerns have slowed widespread use of biometrics to enhance user verification.

Another disadvantage of the arrangement of Fig. 2 is that even once the card owner's biometric signature 801 and card information 702 has be pre-loaded onto the back-end database 806, the card owner is still required to carry the card and to validate the card for each transaction. This is inconvenient as the card is often lost or damaged.

Summary

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

Disclosed are arrangements which seek to address the above problems by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, a biometric signature reader, the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form), an alphanumeric keypad (optional), and a communication module for communicating with back-end system that may be remotely accessible over a network.

As described herein, when the description refers to "the storing of a biometric signature" in a memory, a person skilled in the art would understand that rather than the actual biometric signature it is a representation of the biometric signature that is actually stored in the memory. This representation may be referred to as a "biometric template" or "template".

The card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase). The biometric signature is stored at a memory address together with a copy of the

card information on the user's card as read by the card reader of the verification station. The memory address may be defined by the ("unique") card information on the user's card. The term "unique" means unique in the context of a permitted set of cards associated with the verification station. This is described in more detail in regard to **Fig. 8**.

All future uses (referred to as uses in the verification phase) of the particular verification station by the user of the aforementioned card requires the user to merely submit a biometric signature (e.g., thumb print or retinal scan etc.), which is compared to the signatures stored in the memory associated with the verification station. Once the submitted biometric signature has been matched to one of the biometric signatures stored in the memory, the card information stored with the stored biometric signature is sent to the back-end system.

An authorised user will be automatically verified by the arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update, allowing entry to a restricted area etc. will simply proceed as normal. The biometric signature of an unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user.

The described arrangements require virtually no modification at all of the back-end systems or the (front-end) card. The additional administrative overheads associated with the described arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The described arrangements also potentially have a reduced impact on privacy of card users. The biometric signatures stored in the local database of the verification station can be made off limits to anyone, or limited to law enforcement agencies, depending on the administrative environment in which the arrangements are implemented. Users of current card systems can learn to use

the described arrangements without much effort, needing only to provide a biometric signature.

According to one aspect of the present invention there is provided a method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

According to another aspect of the present invention there is provided a verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said

PIN during a previous transaction process using a card device reader incorporated into the verification station.

According to still another aspect of the present invention there is provided a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

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 will now be described with reference to the drawings, in which:

Fig. 1 depicts a standard credit card;

Fig. 2 shows the card of **Fig. 1** being used together with biometric verification;

Fig. 3 is a functional block diagram of a special-purpose computer system upon which described methods for the described arrangements can be practiced;

Fig. 4 illustrates the use of a standard card in the described arrangements;

Fig. 5 is a flow chart of a process for using the verification station of **Fig. 3**;

Fig. 6 shows the verification process of **Fig. 5** in more detail;

Fig. 7 shows the enrolment process of **Fig. 5** in more detail;

Fig. 8 shows the card information process of **Fig. 5** in more detail;

Fig. 9 shows an alternate use for the described arrangements;

Fig.10 is a flow chart of a process for using the verification station of **Fig. 3**; **and**

Fig. 11 is another flow chart of a process for using the verification station of **Fig. 3**.

Detailed Description including Best Mode

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. 3 is a functional block diagram of a system 100 in which the described arrangements can be practiced. The methods described herein particularly lend themselves to implementation on the special-purpose computer system 100 such as that shown in **Fig. 3** wherein the processes of **Figs. 5-8, 9** and **10** may be implemented as software, such as an application program executing within the computer system 100. In particular, the steps of the described methods are effected by instructions in the software that are carried out by a verification station 127. The verification station 127 is typically constructed in a tamper-proof manner, both physically and electronically, to prevent unauthorised access to the inner mechanism of the verification station 127. 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 described 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 verification station 127 from the computer readable medium, and is then executed by the verification station 127. 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 effecting the described arrangements.

The computer system 100 consists of a computer module 101, input devices such as a biometric reader 102, a card reader 112, and a keypad 103, output devices including an LCD (Liquid Crystal Display) display device 126 and a loudspeaker 117. The computer module 101 uses a Modulator-Demodulator (Modem) transceiver device 116 for communicating to and from a communications network 120, for example connectable via a telephone line 121 or other functional medium. The modem 116 can be used to obtain access to a back end system including a processor 122 and back-end database 123 over the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The computer module 101 typically includes at least one processor unit 105, and a memory unit 106, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The module 101 also includes a number of input/output (I/O) interfaces including an audio-video interface 107 that couples to the LCD display 126 and loudspeaker 117, an I/O interface 113 for the keypad 103, biometric reader 102 and card reader 112, and an interface 108 for the modem 116. In some implementations, the modem 1116 may be incorporated within the computer module 101, for example within the interface 108.

A storage device 109 is provided and typically includes a hard disk drive 110 and a flash memory 111. The components 105 to 111 and 113 of the computer module 101, typically communicate via an interconnected bus 104 and in a manner that results in a conventional mode of operation of the computer system 100 known to those in the relevant art.

Typically, the application program is resident on the hard disk drive 110 and read and controlled in its execution by the processor 105. Intermediate storage of the program and any data fetched from the network 120 may be accomplished using the semiconductor memory 106, possibly in concert with the hard disk drive 110. In some instances, the application program may be supplied to the user encoded on the flash memory device 111, or alternatively may be read by the computer module 101 from the network 120 via the modem device 116.

Still further, the software can also be loaded into the computer system 100 from other computer readable media. 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 computer system 100 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 computer module 101. 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.

As illustrated in **Fig. 4,** a standard card 601 has card information 605 typically comprising three fields, namely 602 which is the card type, 603 which is the card range, and 604 which comprises card data specific to the particular card 601. In the described

arrangements, the card data 604 may act as the memory reference which points, as depicted by an arrow 608, to a particular memory address 607 in the local database 124 in the verification station 127 of **Fig. 3.** In another arrangement, a personal identification number (PIN) may also act as the memory reference which points to the particular memory address 607 in the local database 124 in the verification system 127.

The fields 602 and 603, which together form a header 606, can be used by the described system to determine if the card 601 is to be processed according to the described methods or not. This is described in more detail in regard to **Fig. 8.**

In an initial enrolment phase, the card user couples their card 601 (or key-fob or other card device) to the card reader 112. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM). The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader 102. The card data 604 defines the location 607 in the local database 124 where their unique biometric signature is to be stored. In the described arrangements, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 is then also stored at the location 607 in the local database 124. For example, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

Thereafter, in later verification phases, the card user is merely required to present their unique biometric to the biometric reader 102 in order to perform a transaction. In this instance, the biometric signature provided by the user is compared to each of the signatures stored in the local database 124. Once verification is confirmed, through a match of the provided biometric signature to one of the stored signatures, the card information 605 is transferred from the local database 124 within the verification station 127 to the back-end processor 122 for completion of the transaction.

Importantly, the back-end processor 122 does not see the difference between receiving the card information 605 from the verification station 127, and receiving it from a conventional card reader in the absence of the verification station implementing the described arrangements. This means that back-end processes (depicted by the back-end processor 122 and the back-end database 123) need no modification when incorporating the described arrangements into current card systems. There are additional elements in the verification station 127 (see **Fig. 3**) compared to the normal card reader, however this is a relatively simple and inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Alternatively, rather than only providing their biometric signature in later verification phases, the user may choose to also couple their card 601 to the card reader 112. In this instance, after coupling their card 601 to the card reader 112, the card user is required to again present their unique biometric to the biometric reader 102. In this instance, rather than the biometric signature provided by the user being compared to all of the signatures stored in the local database 124 to determine a match, the biometric signature provided by the card user is only compared to the biometric signature stored at the memory location 607 defined by the card data 604 read from their card 601 by the card reader 112. Again, once verification is confirmed, the card information 605 is transferred from the local database 124 of the verification station 127 to the back-end processor 122 for completion of the transaction.

Fig. 5 shows a process 200 for using the verification station 127. In the described process 200, rather than only providing their biometric signature in verification phases following the initial enrolment phase, the user couples their card 601 to the card reader 112 to perform a transaction. As described below, in another process 1000, in later verification phases following the initial enrolment phase, the user may merely present

their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 201, the processor 105 determines if the card 601 has been read by the card reader 112. If this is not the case, then the process 200 follows a NO arrow back to the step 201. If, on the other hand, the card 601 has been read by the card reader 112, then the process 200 follows a YES arrow to a step 202 (see **Fig. 8** for more details). In the step 202, the processor 105 buffers the card information 605 that is read from the card 601 by the card reader 112 and processes the card information 605. In a following step 203 a request is presented to the card holder to provide a biometric signature to the biometric reader 102. This request can be provided in an audio fashion by means of the audio interface 107 and the speaker 117, this being driven by suitable software running on the processor 105. Alternatively or in addition, a suitable message can be displayed on the LCD display 126 by suitable software running on the processor 105.

In response to the aforementioned request, the holder of the card 601 provides a biometric signature to the biometric reader 102. After the signature has been received by the step 203, the process 200 is directed to a step 204 that reads the contents of the local database 124 at an address defined by the card data 604. If the contents of this memory address match, to a sufficiently high degree of correspondence, the biometric signature received in the step 203 via the biometric reader 102, then the process follows a YES arrow to a step 205 (see **Fig. 6** for more detail). It is noted that if the step 204 returns a YES value, then the biometric signature at the noted memory address was written into the local database 124 in an earlier enrolment phase. It is also noted that the step 204 reads the biometric signature stored at a single memory address defined by the card data 604 and checks the stored biometric signature against the biometric signature received in the step 203. In the process 200, there is no need to search the database 124 to see if there is a match. Thus, the process 200 provides a particularly simple and fast biometric

verification check. Once the step 205 has completed the verification process, the process 200 is directed according to an arrow 209 back to the step 201.

Returning to the step 204, if the biometric signature of the local database 124 at the memory address defined by the card data 604 does not match the signature received by the biometric reader 102, then the process 200 follows NO arrow to a step 206. In the step 206, the processor 105 determines if the biometric signature of the memory location defined by the card data 604 is empty. If this is the case, then the process 200 follows a YES arrow to a step 207 that performs an enrolment process for the card 601 (see **Fig. 7** for more detail). The process 200 then follows the arrow 209 back to the step 201.

Returning to the step 206, if the biometric signature of the aforementioned memory location is not empty, then this means that (i) the card 601 and the associated biometric signature of the card holder have previously been used for the enrolment process 207, and (ii) the biometric signature now received in the step 203 does not match the signature stored in the local database 124. In this event, the process 200 follows a NO arrow to a step 208 that performs an alert process. The process 200 then follows the arrow 209 back to the step 201. The alert process 208 can include sending an alert message from the verification station 127 to the back end processor 122 for later action, for example by the police. The alert process can also store the (unauthorised) signature for later use by the law enforcement authorities.

As noted in regard to **Fig. 3**, the verification station 127 is constructed in a tamper proof fashion to ensure that the process 200 of **Fig. 5**, particularly the steps 204-207, are not accessible to unauthorised tampering.

Fig. 6 shows the verification process 205 from **Fig. 5** in more detail. The process 205 is entered from the step 204 in **Fig. 5**, after which a step 301 authorises the transaction. This authorisation step 301 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches the biometric signature previously stored

in the local database 124 by a previous enrolment process 207 applied to the card in question.

After the step 301, a step 302 performs the transaction process, whatever that may be. Thus, for example, if the process 200 of **Fig. 5** relates withdrawal of cash from an Automatic Teller Machine (ATM), then the step 302 comprises the user specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). After completion of the transaction process by the step 302, the process 205 is directed back to the step 201 in **Fig. 5**.

Fig. 7 shows the enrolment process step 207 from **Fig. 5** in more detail. The process 207 is entered from the step 206 in **Fig. 5**, after which a step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604 received in the step 202 of **Fig. 5**. At step 401, the process 207 also retrieves the card information 605 that was previously buffered in the memory 106 at step 202, and stores the card information in the local database 124 at the memory address defined by the card data 604. The aforementioned step 401 can store the biometric signature and card information 605 in encrypted form to reduce the probability that the signature can be acquired for unauthorised use, thus helping ensure the privacy of the card owner. As described above, the biometric signature is stored as a biometric template representing the biometric signature provided by the user. The following steps 402 and 403 have the same respective functions as the corresponding steps 301 and 302 in **Fig. 6**. After completion of the step 403, the process 207 is directed back to the step 201 in **Fig. 5**.

Fig. 8 shows the step 202 in **Fig. 5** that is concerned with the processing of the card information 605 from the card 601 when the card 601 is read by the card reader 112 in the step 202 of **Fig. 5**. The process 202 is entered from the step 201 in **Fig. 5**, after

which a step 501 reads the card information 605 from the card 601 using the card reader 112 and buffers the card information 605 in the memory 106. In a following step 502, the processor 105 retrieves predefined "permitted card set" parameters to determine the "permitted card set" for the verification station 127 in question. The permitted card set parameters may be retrieved from the local database 124 or from the hard disk drive 110, for example, and be also stored in the memory 106. A separate, or overlapping, permitted card set may be defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the described processes at any given verification station 127. This has the advantage of ensuring that the local database 124 does not overflow, and it also provides control over which users make use of which verification stations. However, the permitted card set for any given verification station 127 is only limited by the size of the local database 124. Card information 605 from any number of cards 601 may be stored in the local database 124 of a particular verification station 127 if the amount of memory is sufficient. In one embodiment, the processor 105 may periodically run a clean-up process where all card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months) may be deleted from the local database 124.

In a following step 503 the processor 105 compares the header 606 against the predefined permitted card set parameters to determine if the card 601 belongs to the permitted card set for the verification station 127 in question. If this is the case, then the process 202 is directed by a YES arrow to the step 203 in **Fig. 5**. If, on the other hand, the card header 606 does not belong to the permitted card set for the particular verification station 127, then the step 202 follows a NO arrow from the step 503 to a step 504. In the step 504, the processor 105 rejects the card that has been entered into the card reader 112. This rejection can take the form of a message displayed on the LCD display 126 and/or a corresponding audio message via the speaker 117. Thereafter, the process

202 is directed back to the step 201 in **Fig. 5**. It is noted that even if the verification station does not reject the card not belonging to the permitted card set for the verification station 127 in question, the back-end processor 122 can do so.

In addition to the predefined permitted card set, other administrative functions can be provided by the described arrangements. Thus, the predefined permitted card set details can be amended and/or the signatures stored in the database 124 can be deleted by a system administrator. The system administrator may also periodically perform the clean-up process described above to delete card information 605 and biometric signatures related to cards that have not been used for a predetermined period of time (e.g., twelve months), so that the local database 124 does not overflow. Audit trail information is also stored in the verification station 127 and can be downloaded for audit purposes. The audit information typically includes information of which cards have been submitted to the verification station and the time stamps of the card submissions. Biometric signatures are typically not part of the downloadable audit information, and require a greater level of authorisation (such as that associated with law enforcement agencies) for access.

Fig. 10 shows a process 1000 for performing a transaction using the described arrangement. The process 1000 may be performed by the owner of the card 601, for example, in later verification phases once the owner has previously performed the initial enrolment phase, so that their biometric signature and a copy of the card information 605 has been stored in the local database 124. Accordingly, the stored copy of the card information 605 was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127. In the described process 1000, in such a later verification phase, the user may merely present their unique biometric signature to the biometric reader 102 in order to perform a transaction.

In a first step 1001, the processor 105 receives a biometric signature as provided by the owner of the card 601 to the biometric reader 102. The biometric signature may be temporarily buffered in the memory 106. After the signature has been received at the step 1001, the process 1000 is directed to a step 1004 that reads the contents of the local database 124 at a first address and compares a biometric signature stored at that first address to the biometric signature received at step 1001. In this instance, the first address may be selected randomly. Alternatively, the first address may be selected in an ordered fashion. For example, the first address may be selected as the first address in a particular block of memory.

Accordingly, at step 1004, the process 1000 compares the received biometric signature, inputted to the biometric reader 102 and buffered in memory 106, to a biometric signature stored at a first address in the local database 124 (or memory) incorporated into the verification station 127. As will be described, if the received biometric signature stored at the first memory address does not match the biometric signature stored at the first address, then the process 1000 compares the received biometric signature to one or more further biometric signatures stored in the local database 124 (or memory) incorporated into the verification station 127.

At the next step 1005, if the biometric signature stored at the first memory address matches, to a sufficiently high degree of correspondence, the inputted biometric signature received in the step 1001, then the process 1000 follows a YES arrow to a step 1006. It is noted that if the step 1005 returns a YES value, then the biometric signature at the first memory address was written into the memory 124 in an earlier enrolment phase together with the card information 605.

At step 1006, the process 1000 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches one of the biometric signatures previously stored in the local database 124 by a previous enrolment process 207 applied

for the card 601 in question. After the step 1006, a next step 1008 performs the transaction process, whatever that may be, using the copy of the card information 605 stored in the local database 124. Typically, the transaction process will require the card information 605 to be transferred from the verification station 127 to the back-end processor 122 for completion of the transaction. As an example of a transaction process, if the process 1000 of **Fig. 10** relates to the withdrawal of cash from an Automatic Teller Machine (ATM), then the step 1008 comprises the card owner specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). Accordingly, the stored copy of the card information 605 used in the performed transaction process was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127.

After completion of the step 1008, the process 1000 is directed back to step 1001 or to the step 201 in **Fig. 5**.

If, at step 1005, the biometric signature stored at the first memory address does not match the biometric signature received in the step 1001, then the process 1000 follows a NO arrow to a step 1007. At step 1007, if the processor 105 determines that there are no further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1001 or to the step 201 in **Fig. 5.** If the processor 105 determines at step 1007 that there are further biometric signatures stored in the local database 124 to compare with the received biometric signature, then the process 1000 returns to step 1004. At the next execution of step 1004, the processor 105 reads the contents of the local database 124 at a further address and compares a biometric signature stored at that further address to the biometric signature received at step 1001.

Fig. 9 shows another application 900 to which the described arrangements can be applied. In a first step 901 a person purchases or hires a verification station implemented in a portable form. A step 901 is performed at a registered supplier premises. Accordingly in a following step 902, the enrolment process is performed in controlled circumstances at the supplier premises. The "controlled conditions" referred to mean that the enrolment process is performed under conditions where the identity of the holder of the card 601 is verified, using a driving licence, passport or equivalent identification document, this ensuring that the enrolment process enrols the true owner of the card in an authorised manner.

In a following step 903, the verification station together with the card 601 can be used for third party transactions. Thus, in one example, the holder of the card 601 can take the portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises. This station identification number is then transmitted to the on-line casino back-end processes together with the card information 605. This type of application does require some modification of the back-end processes.

In the arrangements described above, a card user is required to enrol at each individual verification station 127. However, in another arrangement, a user may be able to enrol at one verification station 127 and the user's biometric signature and card information 605 may be broadcast over the communications network 120 to one or more other verification stations connected to the communications network 120. The broadcast biometric signature and card information 605 may then be stored in the local databases of each of those verifications stations to which the biometric signatures and card information 605 have been broadcast. Such an arrangement may be referred to as a 'minimum

enrolment' arrangement. The minimum enrolment arrangement is particularly advantageous for Electronic Funds Transfer Point of Sale (EFTPOS) transactions, ATM transactions and the like. For example, the verification station 127 described above may be added to an EFTPOS terminal or ATM. The broadcasting of the biometric signature and card information 605 increases the security of the transactions made with the verification stations.

In an initial enrolment phase of the minimum enrolment arrangement, the card user couples their card 601 to the card reader 112 of the verification station 127 in a similar manner to that described above. The card information 605 is read by the card reader 112 and is initially buffered in the memory 106 (e.g., within RAM) of the verification station 127. The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader 102. The buffered card data 604 defines the location 607 in the local database 124 where the card user's unique biometric signature is to be stored. Once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 may then also stored at the location 607 in the local database 124. As described above, the card information 605 may be appended to the biometric signature stored at the location 607 within the local database 124.

In the minimum enrolment arrangement, following the storing of the user's biometric signature in the local database 124, a copy of the user's biometric signature, together with a copy of the card information 605 read from the user's card, is broadcast over the communications network 120 to one or more of the other verification stations connected to the network. The card user's unique biometric signature together with the card information 605 corresponding to the biometric signature is then stored in the local database (e.g., 124) of each verification station to which the biometric signature and card information 605 has been broadcast. The biometric signature and card information 605 is

stored at a particular memory address, as defined by the card data 604, in each of the local databases. The storing of the card information 605 in the each of the local databases of the verification stations allows biometric only transactions as described above to be performed.

In another alternative of the minimum enrolment arrangement, rather than broadcasting the individual biometric signatures and card information to each of the other verification stations connected to the network 120 upon an enrolment taking place, updates to the contents of a local database within a particular verification station 127 or indeed the entire contents of the local database may be broadcast periodically (e.g., overnight).

Accordingly, in the minimum enrolment arrangement described above, the card user is only required to enrol on one verification station 127 connected to the communication network 127 and each of the other verifications stations connected to the communications network 120 will receive a copy of the card user's enrolled biometric signature and possibly the card information 605 corresponding to that biometric signature. Thereafter, in later verification phases, the user may make biometric only transactions, as described above with reference to Fig, 10, at each of the verification stations connected to the communications network 120 after enrolling on one of the verification stations 127. Alternatively, the user may also choose to couple their card to the card reader (e.g., 112) of one of the verifications stations and present their unique biometric signature in order to perform a transaction, as described above.

In the arrangements described above, once the biometric signature has been stored in the local database 124 at the location 607, the card information 605 buffered in memory 106 is then also stored at the location 607 in the local database 124 and may be used to point to the location 607 in the local database 124.

In another arrangement, once the biometric signature and biometric has been stored in the local database 607, the card user may also enter a PIN using the keypad 103. Preferably, the PIN is required to be entered within a predetermined time period. The PIN may be any number and/or letter sequence including names and easy to remember patterns. In this instance, the PIN is then also stored at the location 607 in the local database 124. Again, the PIN may be appended to the biometric signature stored at the location 607. Therefore, the local database 124 contains the biometric signature, the card information 605 (or key-fob information) and the PIN of a card user. The PIN may be used to define a pointer to the memory location 607 in the local database which is the same location 607 pointed to by the card data 604. Thereafter, in later verification phases, the card user is required to present their unique biometric to the biometric reader 102 and then enter their PIN using the keypad 103, in order to perform a transaction. The PIN may be required to be entered within a predetermined period of time.

Once the biometric and PIN has been provided by the user, rather than the biometric signature being compared to all of the signatures stored in the local database 124 to determine a match, the biometric signature provided by the card user is only compared to the biometric signature stored at the memory location 607 defined by the user's PIN entered by the user into the keypad 103.

Again, once verification is confirmed, through a match of the provided biometric signature to the biometric signature stored at the memory location 607 defined by the PIN, the card information 605 is transferred from the local database 124 within the verification station 127 to the back-end processor 122 for completion of the transaction.

In the PIN arrangement, at step 401 of the enrolment process 207, a request is presented to the card holder to provide a PIN to the keypad 103. This request can be provided in an audio fashion by means of the audio interface 107 and the speaker 117, this being driven by suitable software running on the processor 105. Alternatively or in

addition, a suitable message can be displayed on the LCD display 126 by suitable software running on the processor 105. The PIN entered into the keypad 103 is stored in the local database 124 at the memory address defined by the card data 604. Again, the biometric signature, PIN and card information 605 may stored in encrypted form to reduce the probability that the signature can be acquired for unauthorised use.

Fig. 11 shows another process 1100 for performing a transaction using the described arrangement. The process 1000 may be performed by the owner of the card 601, for example, in later verification phases once the owner has previously performed the initial enrolment phase, so that their biometric signature, a copy of the card information 605 and a PIN has been stored in the local database 124. Accordingly, the stored copy of the card information 605 was read from the card 601 and together with the PIN entered by the user was stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127. In the described process 1100, in such a later verification phase, the user may present their unique biometric signature to the biometric reader 102 together with their PIN in order to perform a transaction.

In a first step 1101, the processor 105 receives a biometric signature as provided by the owner of the card 601 to the biometric reader 102. The biometric signature may be temporarily buffered in the memory 106. After the signature has been received at the step 1001, the process 1000 is directed to a step 1003. At step 1003, the processor 105 receives a PIN as provided by the owner of the card 601 to the keypad 103. The keypad 103 may be similar to a telephone where letters are also displayed on the keys together with the numbers. The keypad 103 may be in addition to another keypad (e.g., an existing keypad on an Automatic Teller Machine in which the verification station 127 has been installed.

At a step 1104 the processor 105 reads the contents of the local database 124 at an address defined by the entered PIN and compares a biometric signature stored at that address to the biometric signature received at step 1101.

At the next step 1105, if the biometric signature stored at the memory address defined by the PIN matches, to a sufficiently high degree of correspondence, the inputted biometric signature received in the step 1101, then the process 1000 follows a YES arrow to a step 1106. It is noted that if the step 1105 returns a YES value, then the biometric signature at the memory address and the PIN was written into the memory 124 in an earlier enrolment phase together with the card information 605.

At step 1106, the process 1100 indicates that the biometric signature received by the biometric reader 102 in the step 203 matches the biometric signature previously stored in the local database 124 by a previous enrolment process 207 applied for the card 601 in question. After the step 1106, a next step 1108 performs the transaction process, whatever that may be, using the copy of the card information 605 stored in the local database 124. Typically, the transaction process will require the card information 605 to be transferred from the verification station 127 to the back-end processor 122 for completion of the transaction. As an example of a transaction process, if the process 1100 of **Fig. 11** relates to the withdrawal of cash from an Automatic Teller Machine (ATM), then the step 1108 comprises the card owner specifying the required amount of cash and the relevant account information via the keypad 103 (see **Fig. 3**), and the provision of a receipt and cash by the ATM (not shown). Accordingly, the stored copy of the card information 605 used in the performed transaction process was read from the card 601 and stored in the local database 124 during a previous transaction using the card reader 112 incorporated into the verification station 127.

After completion of the step 1108, the process 1100 is directed back to step 1101, to step 1001 in Fig. 10 or to the step 201 in **Fig. 5**.

If, at step 1105, the biometric signature stored at the memory address defined by the PIN does not match the biometric signature received in the step 1001, then the process 1000 follows a NO arrow to a to step 1101, to step 1001 in Fig. 10 or to the step 201 in **Fig. 5.**

As described above, the PIN may be any number and/or letter sequence including names and easy to remember patterns. This allows the card user to select a PIN which may be memorised by recalling letters, which are associated with the numbers similar to a telephone number.

In another minimum enrolment arrangement, following the storing of the user's biometric signature and PIN in the local database 124, a copy of the user's biometric signature and PIN, together with a copy of the card information 605 read from the user's card, is broadcast over the communications network 120 to one or more of the other verification stations connected to the network. The card user's unique biometric signature and PIN, together with the card information 605 corresponding to the biometric signature is then stored in the local database (e.g., 124) of each verification station to which the biometric signature, PIN and card information 605 has been broadcast. The biometric signature, PIN and card information 605 is stored at a particular memory address, as defined by the card data 604 and PIN, in each of the local databases. The storing of the card information 605 in the each of the local databases of the verification stations allows biometric and PIN only transactions as described above to be performed.

Again, in still another alternative of the minimum enrolment arrangements described above, rather than broadcasting the individual biometric signatures, PIN and card information to each of the other verification stations connected to the network 120 upon an enrolment taking place, updates to the contents of a local database within a particular verification station 127 or indeed the entire contents of the local database may be broadcast periodically (e.g., overnight).

The PIN arrangement and the other arrangements described above can be easily integrated to a security or financial platform system, as an additional component to verify the card user at entry/excess access points. The arrangements may be performed ONLINE or OFFLINE.

In the PIN arrangement, if a unscrupulous user oversees the PIN number of the legitimate card user, the user still requires the biometric of the legitimate card user to perform a transaction. The described arrangements are secure and inexpensive to implement.

The PIN arrangement does not require extensive database searching in order to locate a matching biometric and is therefore the verification is able to be performed in an efficient manner. Further, an incorrectly entered PIN may be used to generate an warning alarm or door chime

Industrial Applicability

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the described arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards, government issued card (e.g., the Australian Medicare card) and others. The arrangements can, in general be used in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature possibly together with a PIN. For example, in the case of the Australian Medicare card, following enrolment at a verification station 127 located at a particular medical centre, the entire

card information 605 of the user's Medicare card is stored in the local database 124 of the verification station 127 located at the medical centre.

As another example, the described arrangements can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying platform. In this instance, the ATM PIN may be used to point to the stored biometric signature. Alternatively, following an initial enrolment phase, the card user may merely enter their biometric signature, possibly together with their PIN, to withdraw funds.

Furthermore, the described arrangements can be used for secure access to a hotel room or any other room, building, cabinet, or apparatus to which secure access is required.

In the hotel room example, the hotel may have a verification station 127 mounted on each door of the hotel. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining a particular room number and planned departure date. The number on the card is preferably one of an increasing sequence of numbers. The number preferably increases over a period of time and is also encrypted. A verification station 127 positioned at the door of the room corresponding to the room number may be configured so that the verification station 127 will only allow enrolments and verifications if the number stored on a presented card correctly identifies the room and is in the correct sequence. The verification station 127 may also include a real time clock to match actual time against the planned date of departure. After the guest enrols their biometric signature at the verification station 127 using the aforementioned card in the manner described above, the arrangement will give them secure access to their room for the duration of their stay.

Following enrolment, the above hotel guest may use their card and a biometric signature (e.g., a fingerprint) to enter the room. Alternatively, the guest may merely present their biometric signature, possibly together with a PIN, to enter the room as described above negating the requirement for the guests to carry the room card, plus increasing security and convenience. The verification station 127 may also be configured so that the guest may choose not to enrol their biometric signature if they do not wish to have a record of their biometric signature stored within the local database of the verification station 127.

The verification station 127 located at the door of a particular hotel room or other secure access entry as described above may also allocate memory for storage of any number of biometric signatures (e.g., fingerprints) to be associated with the new card. This allows the hotel guest and all associated guests (e.g., the hotel guest's family) to enrol their individual biometrics at the verification station 127. The enrolment may simply be achieved, for example, by inserting the card and placing a finger on the biometric reader 102, for each guest. Following this enrolment stage, the card or the biometric signature can be used to gain access to the room, again, negating the requirement for each of the guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the biometric signature (e.g., fingerprints) memory address is that the time and date of departure can also be added to the same memory location. Therefore, the hotel application also allows other related data to be added to the memory location, enhancing the capability of the described arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the described arrangements is in regard to passport control and customs. The arrangements can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to **Figs. 5** and **10.**

Finally, in each of the arrangements described above, the verification stations 127 may be configured to provide the card user with the option of performing transactions with the card 601 only. For example, the card user may not wish to provide their biometric signature. In this instance, the card user may use their card only to perform a transaction with the verification stations in a conventional manner.

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.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

In the context of this specification, the word "comprising" means "including principally but not necessarily solely" or "having" or "including", and not "consisting only of". Variations of the word "comprising", such as "comprise" and "comprises" have correspondingly varied meanings.

The claims defining the invention are as follows:

1. A method of performing a transaction process using a verification station, the method comprising the steps of:

comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

2. The method according to claim 1, wherein the card information is stored in said memory with said previously stored biometric signature.

3. A method according to claim 1, wherein the card device is one of:

a card device in which the card information is encoded in a magnetic strip;

a card device in which the card information is encoded in a bar code;

a smart card device in which the card information is stored in a solid state memory on the smart card; and

a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

4. A method according to claim 1, further comprising the step of outputting information indicating that the user of the card device is not authorised.

5. A method according to claim 4 wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

6. A method according to claim 1, wherein the stored card information and said stored biometric signature was broadcast over a communications network to which said verification station is connected, to one or more further verification stations, following said previous transaction.

7. A verification station for performing a transaction process, the verification station comprising:

means for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

means for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said

PIN during a previous transaction process using a card device reader incorporated into the verification station.

8. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for performing a transaction process using a verification station, said program comprising:

code for comparing a first biometric signature, inputted to a biometric reader incorporated into the verification station, to a biometric signature stored at a memory location in a memory incorporated into the verification station, said memory location being defined by a personal identification number (PIN) inputted into a keypad; and

code for performing the transaction process using card information stored in said memory, if the inputted biometric signature matches the biometric signature stored at the memory location, otherwise, not performing the transaction, wherein the stored card information was read from a card device and stored in said memory together with said PIN during a previous transaction process using a card device reader incorporated into the verification station.

Dated 29 March, 2007
Microlatch Pty Ltd
Patent Attorneys for the Applicant/Nominated Person
SPRUSON & FERGUSON

2007901683 29 Mar 2007

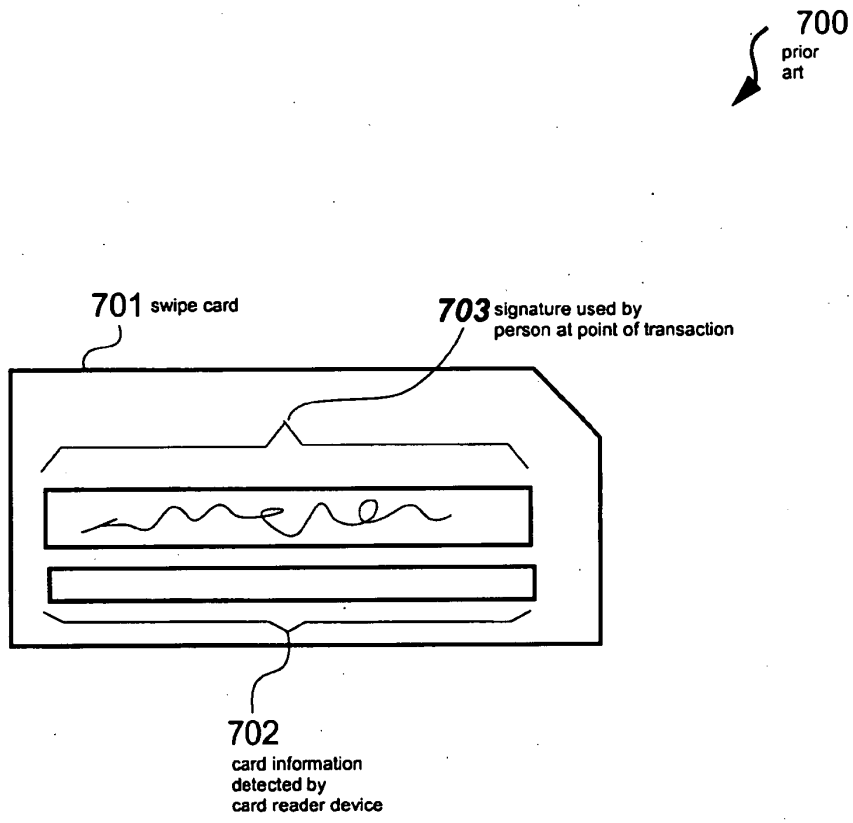


Fig. 1
prior art

2007901683 29 Mar 2007

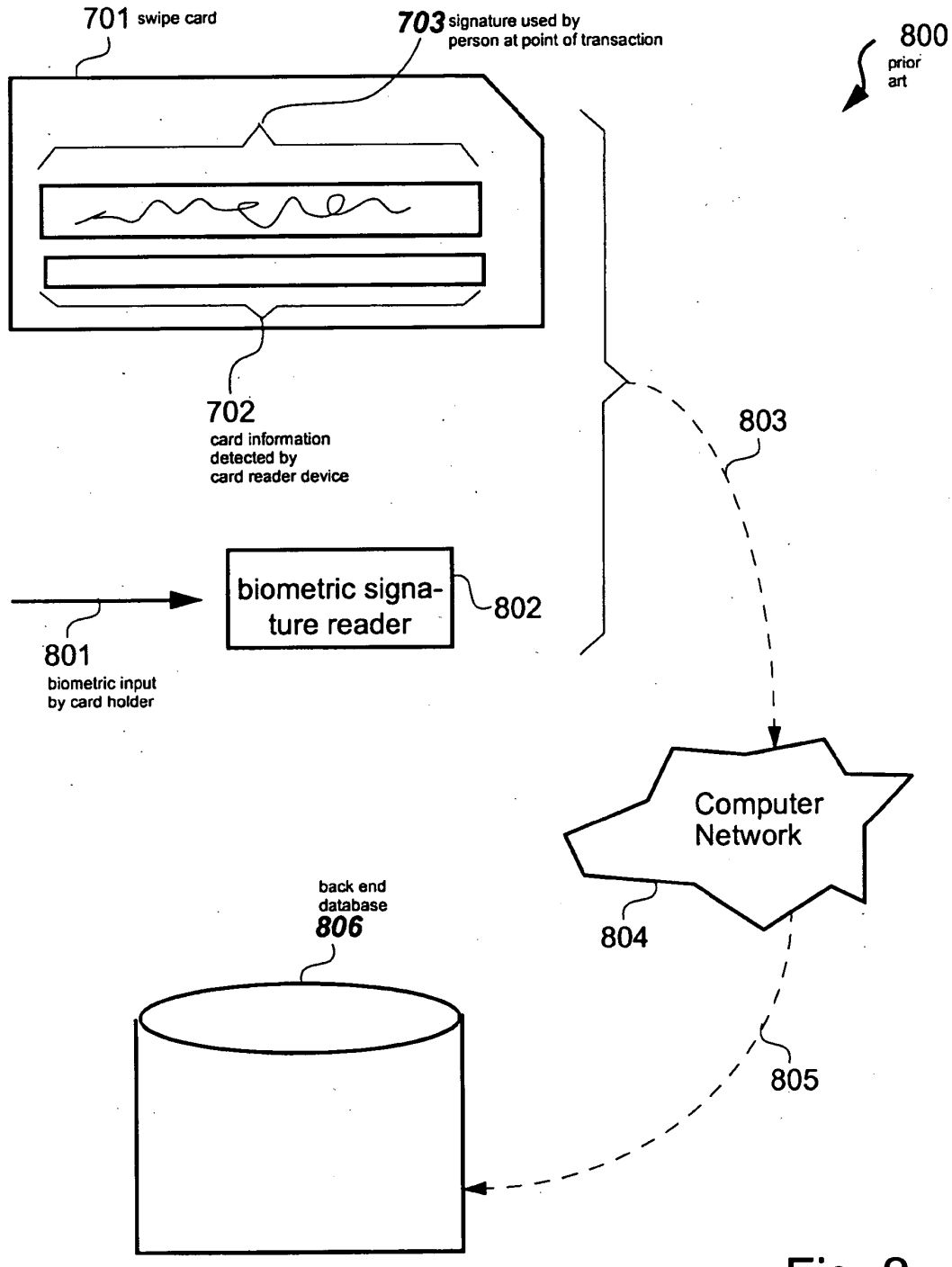


Fig. 2
prior art

29 Mar 2007 2007901683

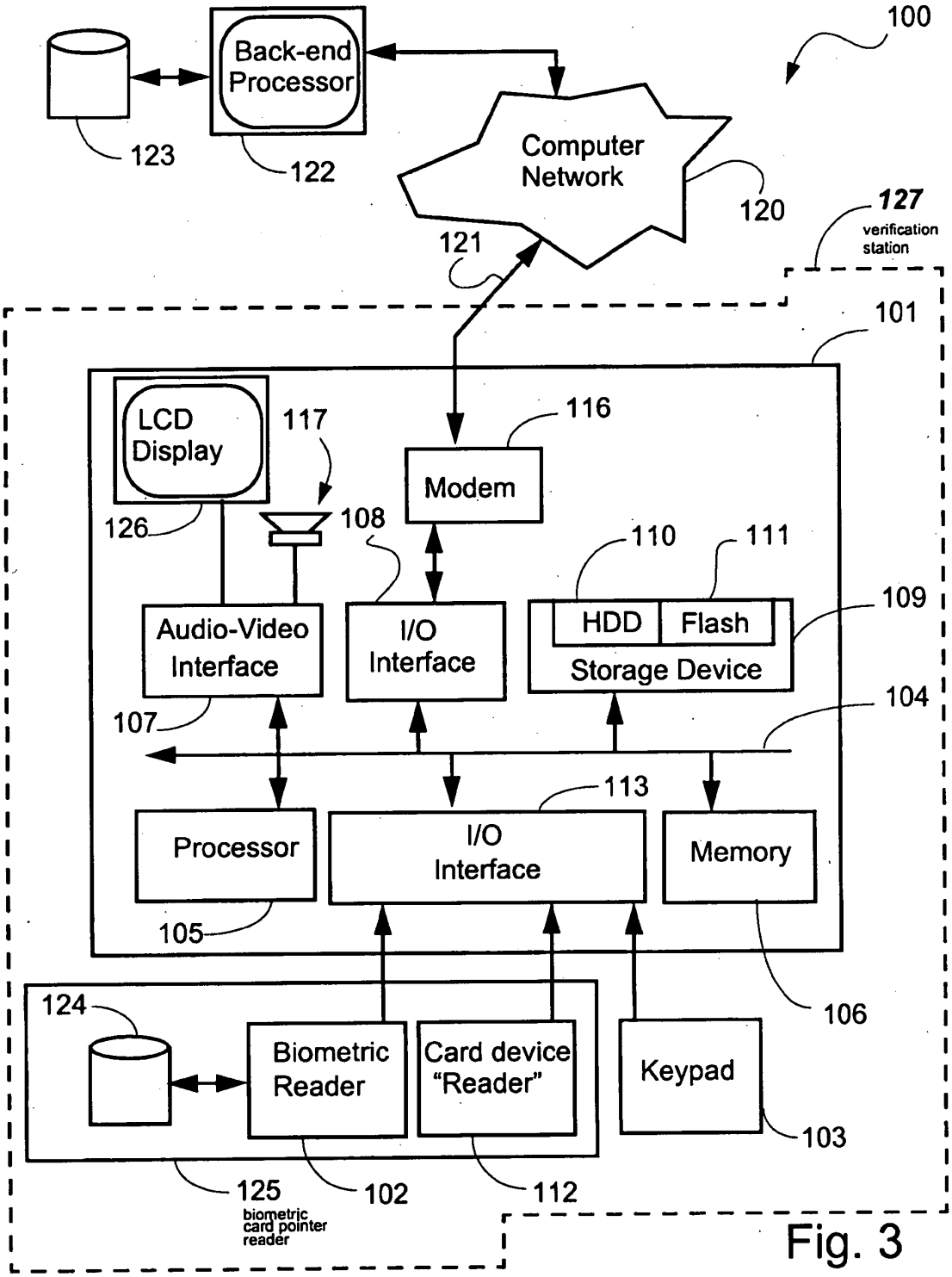


Fig. 3

2007901683 29 Mar 2007

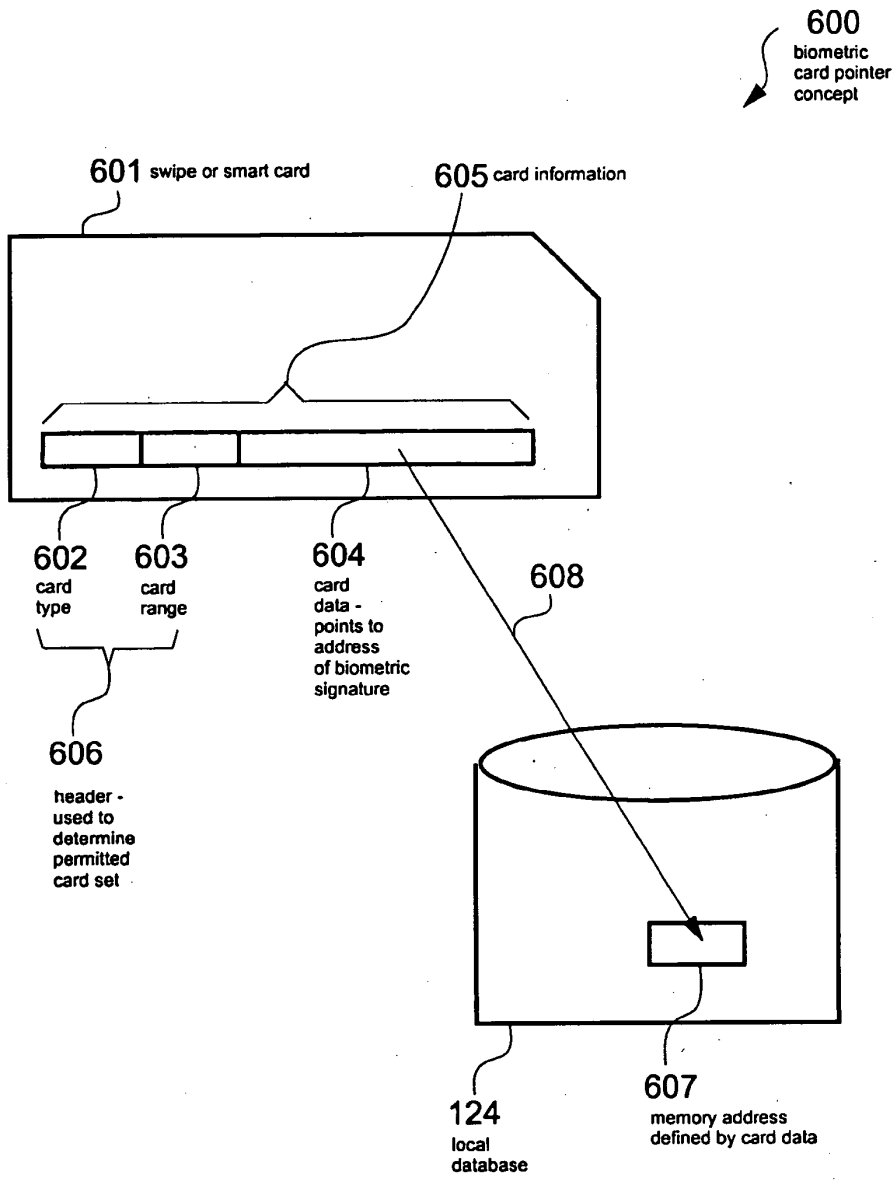


Fig. 4

2007901683 29 Mar 2007

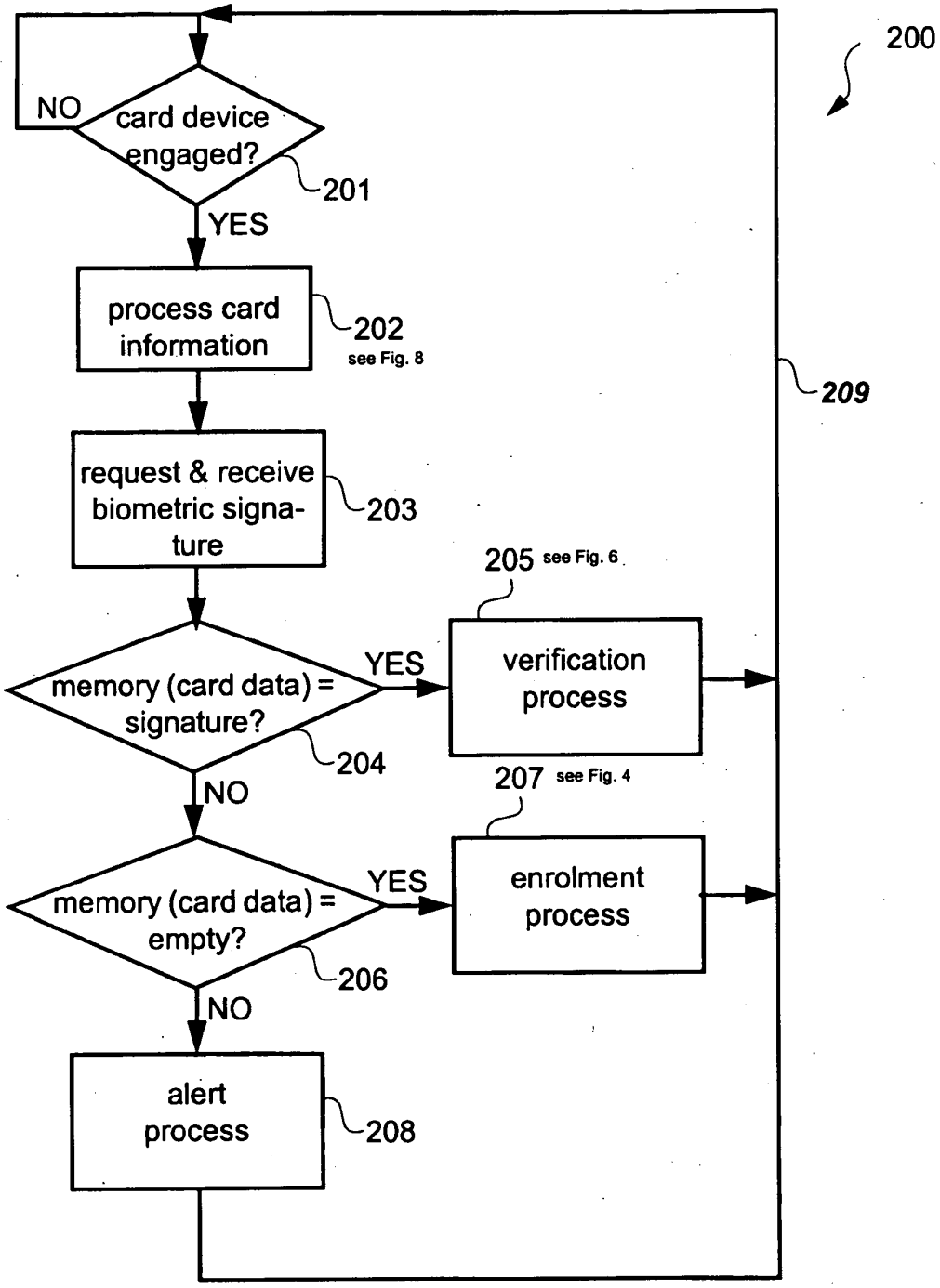


Fig. 5

2007901683 29 Mar 2007

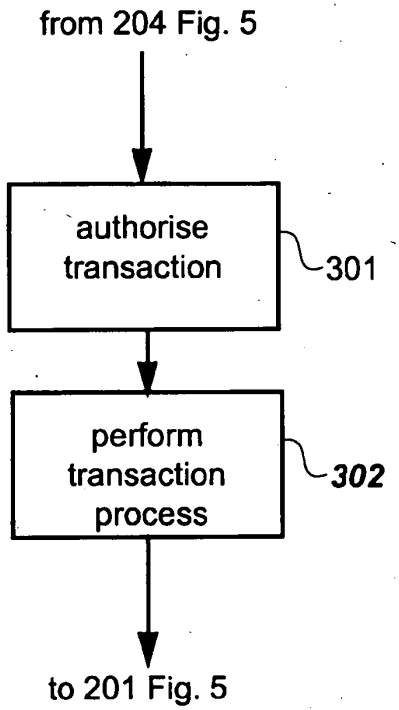
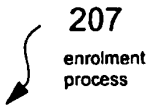


Fig. 6

2007901683 29 Mar 2007



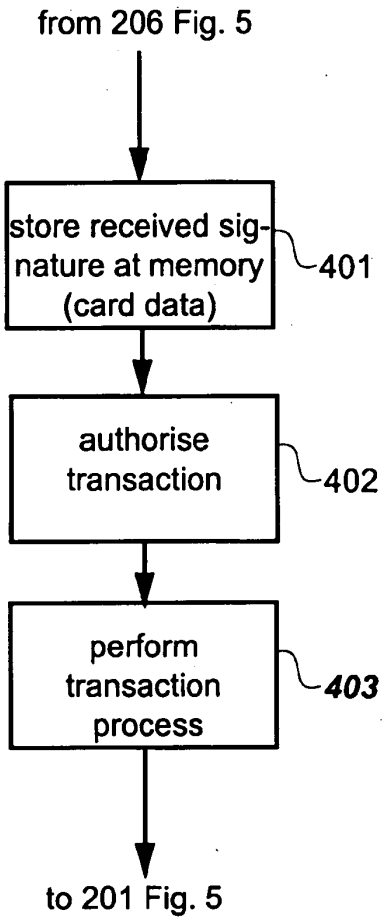


Fig. 7

2007901683 29 Mar 2007

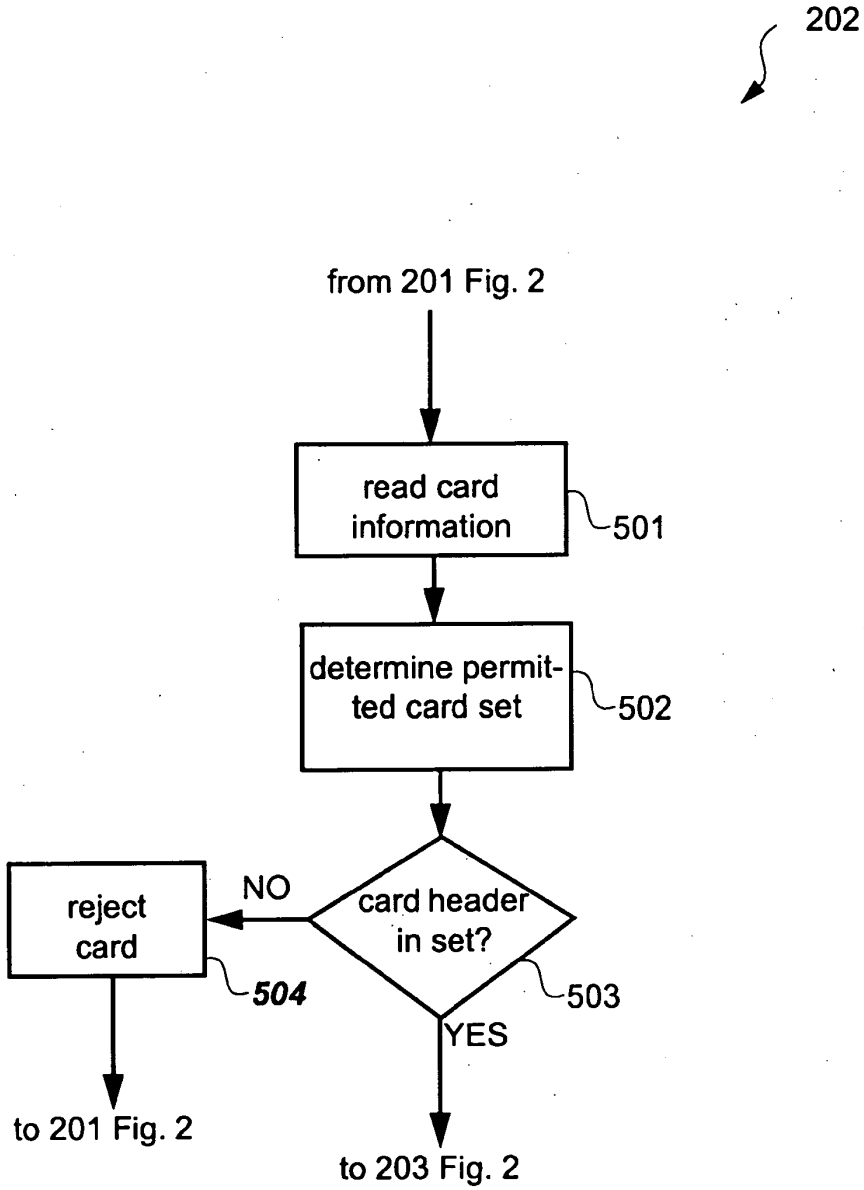


Fig. 8

2007901683 29 Mar 2007

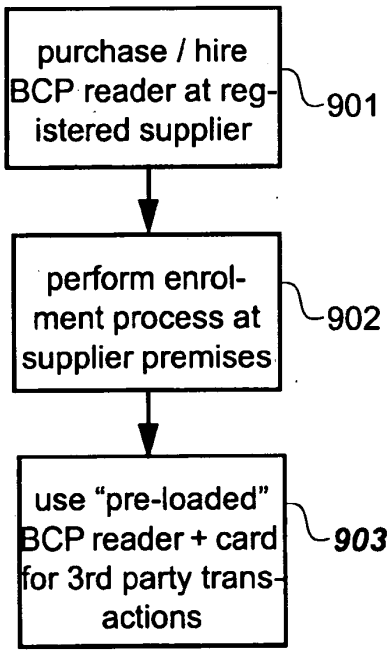


Fig. 9

29 Mar 2007 2007901683

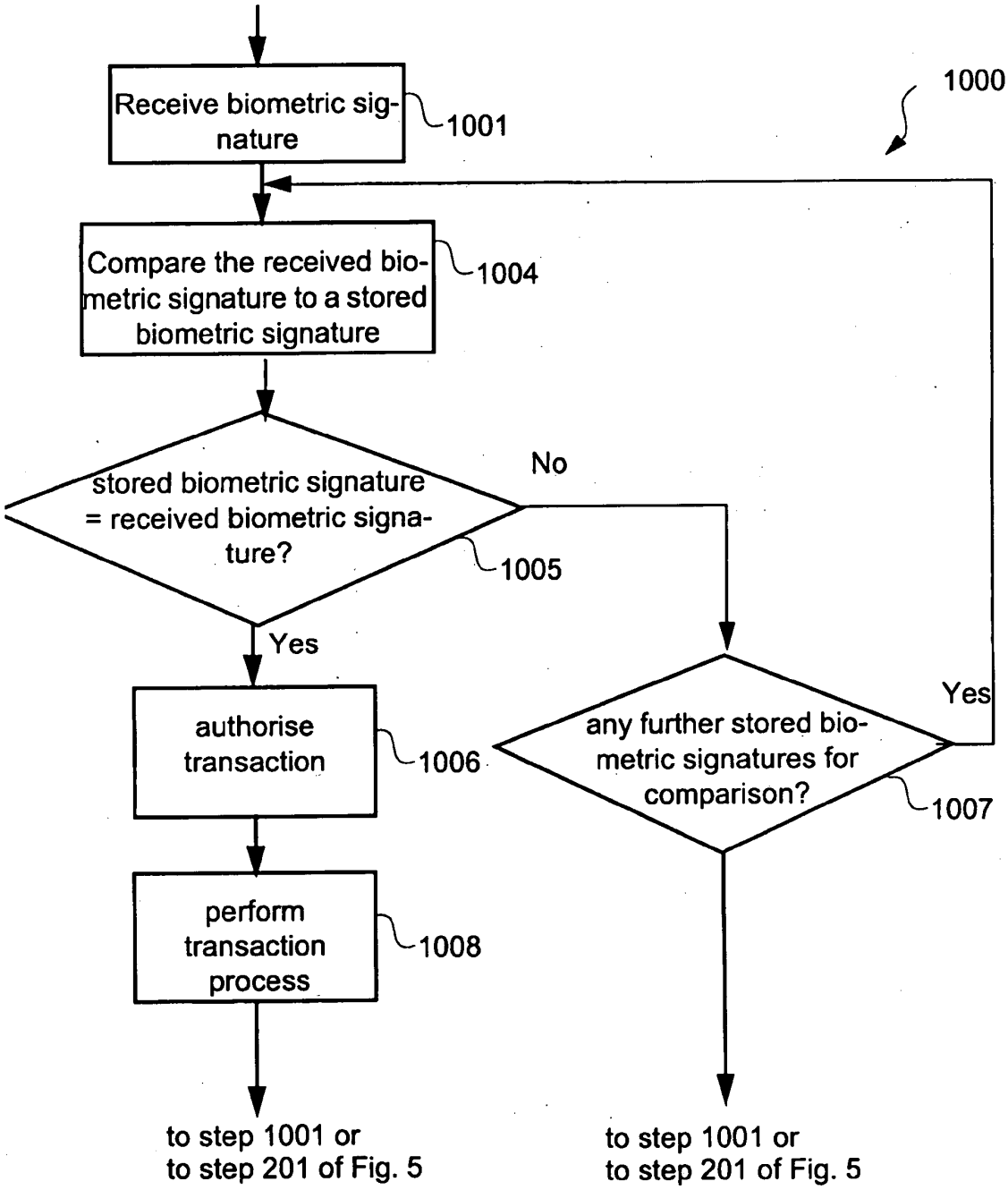


Fig. 10

2007901683 29 Mar 2007

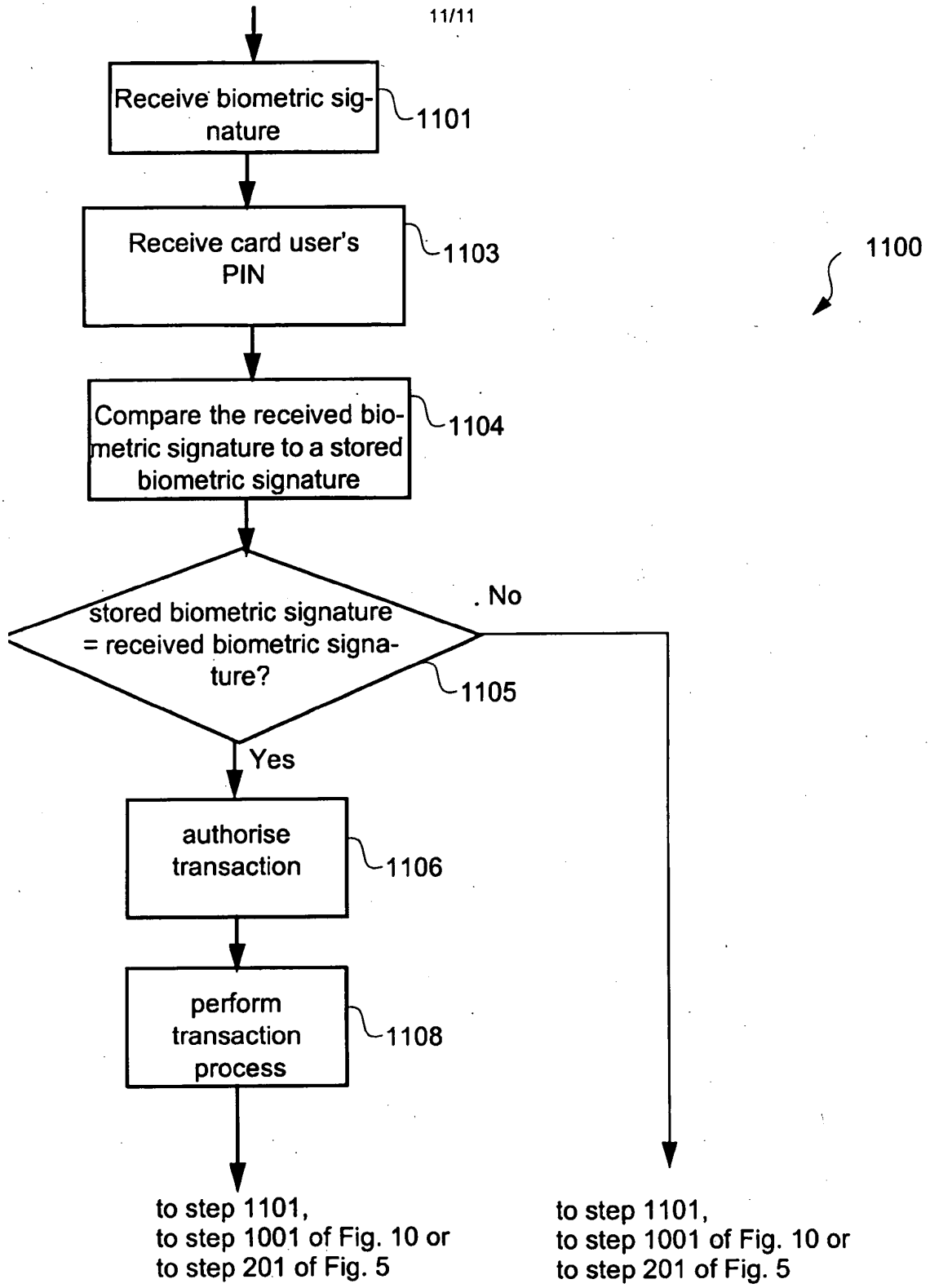


Fig. 11

Copy for (DO-EP) 31
PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

COMMUNICATION IN CASES FOR WHICH NO OTHER FORM IS APPLICABLE

To:

SPRUSON & FERGUSON
GPO Box 3898
Syndey, NSW 2001
AUSTRALIE

Date of mailing *(day/month/year)* 20 October 2008 (20.10.2008)	
Applicant's or agent's file reference 801105C	**REPLY DUE** **see paragraph 1 below**
International application No. PCT/AU2008/000366	International filing date *(day/month/year)* 14 March 2008 (14.03.2008)
Applicant MICROLATCH PTY LTD et al	

1. ☐ REPLY DUE within months/days from the above date of mailing
   ☐ NO REPLY DUE, however, see below
   ☐ IMPORTANT COMMUNICATION
   ☐ INFORMATION ONLY

2. COMMUNICATION:

It has been brought to the attention of the International Bureau that in respect of the above-identified international application, the title was erroneously indicated in the international publication dated 25 September 2008.

The International Bureau will publish a correction in Section II of the PCT Gazette. A corrected version of the corresponding PCT pamphlet will be published on that same date.

A copy of this Notification is being sent to the receiving Office (RO/AU) and to the designated Offices concerned.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 87 40

Authorized officer
Carrié Christine
e-mail pt01.pct@wipo.int
Telephone No. +41 22 338 74 01

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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2008 (25.09.2008)

PCT

(10) International Publication Number
WO 2008/113110 A1

(51) International Patent Classification:
G06K 9/00 (2006.01) *H04K 1/00* (2006.01)

(21) International Application Number:
PCT/AU2008/000366

(22) International Filing Date: 14 March 2008 (14.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007901361 16 March 2007 (16.03.2007) AU
2007901683 29 March 2007 (29.03.2007) 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, 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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING A VERIFICATION STATION

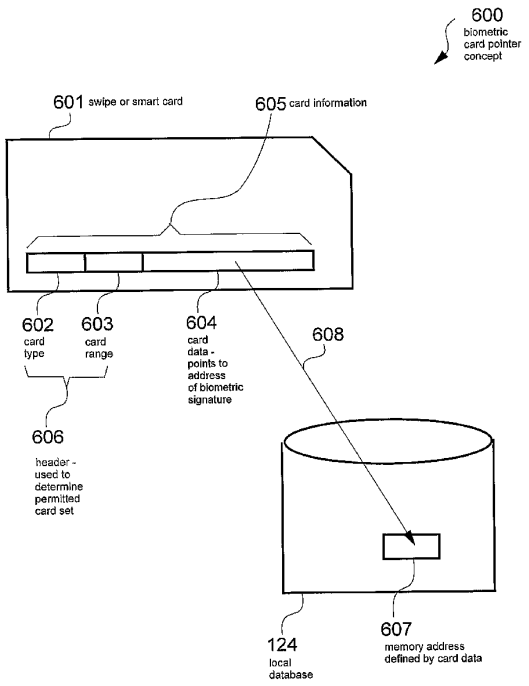


Fig. 4

(57) Abstract: A method of performing a transaction process using a verification station (127) is disclosed. The method compares a first biometric signature, inputted to a biometric reader (102) incorporated into the verification station (127), to one or more further biometric signatures stored in a memory (124) incorporated into the verification station (127). The method performs the transaction process using card information stored in the memory (124), if the inputted biometric signature matches one of the stored biometric signatures, otherwise, the transaction is not performed. The stored card information was read from a card device (112) and stored in the memory (124) during a previous transaction process using a card device reader (112) incorporated into the verification station (127).

WO 2008/113110 A1

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*

(48) Date of publication of this corrected version:
4 December 2008

(15) Information about Correction:
see Notice of 4 December 2008

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016

SPRUSON&FERGUSON
GPO Box 3898
Syndey, NSW 2001
AUSTRALIE

For any questions about this communication:
Tel.:+31 (0)70 340 45 00

Date
29.07.09

Reference	Application No./Patent No.
	08714413.5 - 1224 PCT/AU2008000366
Applicant/Proprietor	
Microlatch Pty Ltd	

Entry into the European phase before the European Patent Office

The following information describes the procedural steps required for entry into the European phase before the European Patent Office (EPO). You are advised to read it carefully because failure to take the necessary action in due time can lead to a loss of rights.

1. The above mentioned international patent application has been given the **European application No. 08714413.5**.

2. Applicants **without a residence or their principal place of business** in an EPC Contracting State may themselves initiate European processing of their international applications, provided they do so before expiry of the 31st month from the priority date.

   During the European phase before the EPO as designated or elected Office, however, such applicants **must** be represented by a professional representative (Art. 133(2) and Art. 134(1) and (8) EPC).

   Where, at the expiry of the time period laid down in Rule 163(5) EPC, the requirements of Article 133(2) EPC have not been complied with, the European patent application will be **refused**, pursuant to Rule 163(6) EPC.

   Please note that a professional representative authorised to act before the EPO and who acted for the applicant during the international phase does not automatically become the representative for the European phase. Applicants are therefore strongly advised to appoint in good time any representative they wish to initiate the European phase for them; otherwise the EPO has to send all communications directly to the applicant.

3. Applicants **with a residence or their principal place of business** in an EPC Contracting State are not obliged to appoint for the European phase a professional representative authorised to act before the EPO. However, in view of the complexity of the procedure it is recommended that they do so.

4. Applicants and professional representatives are also strongly advised to initiate the European phase using **EPO Form 1200**. It is available free of charge from the EPO or via the EPO website at **http://www.epo.org**. Similarly, it can be or generated with the epoline® Online Filing Software, obtainable free of charge from the EPO (**http://www.epoline.org**) The use of the form is not compulsory.

5. Where the EPO acts as designated or elected Office (Art. 22(1) and (3) and 39(1) PCT), to enter the European phase before the EPO, the **following acts** must be performed by the applicant within **31 months** from the date of filing of the international application or (where applicable) the earliest priority date:

   a) Supply a translation of the international application into an EPO official language, if the International Bureau did not publish the application in such language (Art. 22(1) PCT and R. 159(1)(a) EPC);

   b) Specify the application documents, as originally filed or as amended, on which the European grant procedure is to be based (R. 159(1)(c) EPC);

   c) Pay the filing fee and, where applicable, the additional fee for a European patent application comprising more than 35 pages (R. 159(1)(c) EPC, Art. 2, items 1, 1a Rules relating to Fees);

   d) Pay the search fee where a supplementary European search report has to be drawn up (R. 159(1)(e) EPC);

   e) Pay the designation fee if the time limit laid down in Rule 39(1) EPC (i.e. six months after publication of the international search report) has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(d) EPC);

   f) File the written request for examination and pay the examination fee if the time limit laid down in Rule 70(1) EPC has expired before the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(f) EPC);

   g) Pay the renewal fee in respect of the third year, if the fee has fallen due (see Rule 51(1) EPC) before expiry of the 31-month period pursuant to Rule 159(1) EPC (R. 159(1)(g) EPC);

   h) File, where applicable, the certificate of exhibition referred to in Article 55(2) and Rule 25 EPC (R. 159(1)(h) EPC);

   i) Pay the claims fees for the sixteenth and each subsequent claim when the application documents on which the European grant procedure is to be based comprise more than fifteen claims (R. 162(1) EPC). For applications entering the European phase on or after 1 April 2009, a higher amount is payable for the 51st and each subsequent claim (Decision of the Administrative Council of 14 December 2007 amending the Rules relating to Fees, OJ EPO 2008, 10).

If either the translation of the international application or the request for examination is not filed in time, or if the filing fee, the additional fee, the search fee, the designation fee or the examination fee is not paid in due time, the application shall be deemed to be withdrawn (R. 160(1) EPC).

6. Payment of fees

   The amounts of fees are set out in the Schedule of fees and expenses, which is published from time to time as a supplement to the Official Journal of the EPO. Applicants should always check the fee amounts applying at the time of payment.

   Payments can be validly made by any person. Permissible methods of payment are laid down in Article 5 RFees. Please note that payment cannot be made by cheque sent to the EPO.

   For information on the calculation of the additional fee for applications comprising more than 35 pages, see Notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure, OJ EPO 2/2009, 118, and Guidelines for Examination in the EPO, April 2009, A-III, 13.2. For an overview of search and examination fees, see Notice from the European Paten Office of 11 February 2008 (OJ EPO 2008, 130).

   The above and further fee-related information is available on the EPO website (**http://www.epo.org**).

7. If the applicant had appointed a representative during the application's international phase, the present Form will be sent to the representative, asking him to inform the applicant accordingly.

   All subsequent communications will be sent to the applicant, or - if the EPO is informed of his appointment in time - to the applicant's European representative.

8. For more details about time limits and procedural acts before the EPO as designated or elected Office, see the EPO brochure "How to get a European patent", Guide for applicants - Part 2, PCT procedure before the EPO - "Euro-PCT".

   This brochure, the list of professional representatives before the EPO as well as Form 1200 are available on the Internet under **http://www.epo.org**.

Receiving Section

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 801105C	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/AU2008/000366	International filing date *(day/month/year)* 14 March 2008 (14.03.2008)	Priority date *(day/month/year)* 16 March 2007 (16.03.2007)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant MICROLATCH PTY LTD		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 22 September 2009 (22.09.2009)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Dorothée Mülhausen e-mail: pt01.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the:
INTERNATIONAL SEARCHING AUTHORITY

To:

SPRUSON & FERGUSON
GPO Box 3898
SYDNEY NSW 2001

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

	Date of mailing *(day/month/year)* 09 MAY 2008
Applicant's or agent's file reference 801105C	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/AU2008/000366	14 March 2008	16 March 2007

International Patent Classification (IPC) or both national classification and IPC
Int. Cl.

G06K 9/00 (2006.01) ***H04K 1/00*** (2006.01)

Applicant
MICROLATCH PTY LTD et al

1. This opinion contains indications relating to the following items:

[X]	Box No. I	Basis of the opinion
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[ ]	Box No. VIII	Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA	Date of completion of this opinion	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	21 April 2008	**JYOTI SHAMDASANI** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. (02) 6283 2836

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/AU2008/000366

Box No. I Basis of this opinion

1. With regard to the **language,** this opinion has been established on the basis of:

   [X] The international application in the language in which it was filed

   [ ] A translation of the international application into, , which is the language of a translation furnished for the purposes of international search (under Rules 12.3(a) and 23.1(b)).

2. [ ] This opinion has been established taking into account **the rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

   a. type of material

      [ ] a sequence listing
      [ ] table(s) related to the sequence listing

   b. format of material

      [ ] on paper
      [ ] in electronic form

   c. time of filing/furnishing

      [ ] contained in the international application as filed.
      [ ] filed together with the international application in electronic form.
      [ ] furnished subsequently to this Authority for the purposes of search.

4. [ ] In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/AU2008/000366

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims		YES
	Claims	**1-16**	NO
Inventive step (IS)	Claims		YES
	Claims	**1-16**	NO
Industrial applicability (IA)	Claims	**1-16**	YES
	Claims		NO

2. Citations and explanations:

NOVELTY & INVENTIVE STEP:

(i) WO 2007/019605

(ii) CA 2412403

(iii) http://www.scmmicro.com/pdf/Smart_Card_Biometric_paper.pdf May 2002

(iv) WO 2006/058039

Claims 1-16 are not novel in light of the above documents (i)- (iii) as each of these documents disclose all the features of the claimed invention. For example, document (i) under Abstract and Summary of Invention, discloses "Biometric card pointer arrangements store a card user's biometric signature in *a local memory in a verification station* the first time the card user uses the verification station....The biometric signature is stored at a memory address defined by the card information on the user's card. All the future uses of the particular verification station by someone submitting the aforementioned card required the card user to submit both the card and a biometric signature which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so. Similarly document (ii), abstract discloses "a method of verifying identity which includes reading and storing indicium (which identifies a reference biometric within the reference signature...) and the reference biometric in memory and using the indicium to locate an extracted biometric within the unknown signature. The extracted biometric is compared to the reference biometric to determine if they match within predetermined threshold criteria. The reading and storing or the reference biometric and indicium, the recording of the unknown signature, the location of the extracted biometric, and the comparison of the reference and extracted biometrics are *all performed on-site*. Document (iii) on page 8 and 9 discloses Biometric System Components and Process which involves "a mechanism to scan and capture a digital or analog image of a living person's biometric characteristic, software for storing, processing and comparing the image, an interface with the applications system that will use the result to confirm an individual's identity. The authentication confirms that the credential belongs to the individual's enrolled biometric template, which may be *stored locally or centrally*.

Subsequent to above and in light of the document (iv) Claims 1-16 are not inventive either. Document (iv) discloses "an electronic transaction verification system for use with transaction tokens such as smart cards that gathers and transmits information about the transaction token and biometric data." The system transmits the transaction information data to a central processing system which is different to a "local memory or memory incorporated into the verification station" as defined in the claimed invention. However this difference is considered to be a workshop improvement only between the two documents and is disclosed in the above documents.

The appended claims are considered not to add any novel or inventive feature either. The features therein are either disclosed in the citations or considered to be the adaptations of the cited art.

Europäisches Patentamt
European Patent Office
Office européen des brevets

European Patent Office
Postbus 5818
2280 HV RIJSWIJK
NETHERLANDS
Tel. +31 (0)70 340-2040
Fax +31 (0)70 340-3016

For any questions about this communication:
Tel.:+31 (0)70 340 45 00

Microlatch Pty Ltd
Unit 13, 145-147 Forest Road
Hurstville, NSW 2220
AUSTRALIE

Date: 24-11-2009

Reference	Application No./Patent No.
	08714413.5 - 1224 PCT/AU2008000366
Applicant/Proprietor: Microlatch Pty Ltd	

Noting of loss of rights pursuant to Rule 112(1) EPC

The European patent application cited above is deemed to be withdrawn (R. 160(1) EPC) for the following reason(s):

☐ translation of the international application into one of the EPO's official languages (Art. 153(4) EPC)

☑ filing fee

☑ additional fee for 13 pages (Art. 2, item 1a, Rules relating to Fees)

.....

☑ designation fee

☑ search fee

☑ request for examination

☑ examination fee

not validly paid/not filed within the period specified in Rule 159(1) EPC.

☐ payment of the above fee(s) on ..... being after expiry of the period for payment (on 16.10.09).

For information on the calculation of the additional fee, see Notice from the European Patent Office dated 26 January 2009 concerning the 2009 fee structure, OJ EPO 2/2009, 118, and Guidelines for Examination in the EPO, April 2009, A-III, 13.2.

Means of redress

Request for a decision (R. 112(2) EPC)
If the applicant considers that the finding of the European Patent Office is inaccurate, he may, within a (non-extendable) period of **two months** after notification of this communication, apply in writing for a decision on the matter. The application can only lead to the finding being reversed if this does not actually correspond to the factual or legal situation.

Further processing (Art. 121 EPC)
The legal consequence of the failure to observe the time limit shall be deemed not to have ensued if, within a (non-extendable) period of **two months** after notification of this communication, further processing is requested by payment of the fee prescribed under Article 2(12) of the Rules relating to Fees and the omitted act is completed (R. 135(1) EPC).

Registered letter
EPO Form 1205A 04.09 ADWI 2

It should be noted that if a loss of rights occurs because the translation or the request for examination has not been filed within the time limit, the flat-rate amount of the further processing fee ("other cases") is due and, where neither has been timely filed, this fee has to be paid twice. Apart from that, for any non-payment of fees in due time, 50% of the relevant fees become payable as further processing fees. In the case of non-payment or insufficient payment of the additional fee, the fee for further processing is calculated according to the number of pages for which the additional fee was not paid within the time limit.

Request under Article 7(3) and (4) Rules relating to Fees
The fee is considered to have been paid in due time if, within a period of **two months** from notification of this communication and in accordance with the requirements under Article 7(3) and (4) Rules relating to Fees, evidence is provided to the EPO that the payment was effected in an EPC Contracting State within the period in which the payment should have been made and, if applicable, the surcharge of 10% of the relevant fee(s) is paid.

Note
For applicants not having either a residence or principal place of business within the territory of one of the EPC Contracting States, the completion of the omitted acts (other than the non-payment of fees) for the purposes of a request under Article 121 EPC, or the filing of a request under Rule 112(2) EPC may only be undertaken by a professional representative authorised to act before the EPO.

Receiving Section

Annex: Schedule of Fees

Europäisches Patentamt
European Patent Office
Office européen des brevets

Gebühren für in die europäische Phase eintretende internationale Anmeldungen in EURO *
Fees for international applications entering the European phase in EURO *
Taxes pour les demandes internationales entrant dans la phase européenne en EURO *

Anmeldegebühr **Filing fee** **Taxe de dépôt**	Das Formblatt für den Eintritt in die europäische Phase (EPA Form 1200) wird **auf Papier** eingereicht: The form for entry into the European phase (EPO Form 1200) is filed **on paper:** Le formulaire d'entrée dans la phase européenne (OEB Form 1200) est déposé **sur papier:**	**180,00**
	Das Formblatt für den Eintritt in die europäische Phase (EPA Form 1200) wird **online** eingereicht: The form for entry into the European phase (EPO Form 1200) is filed **online**: Le formulaire d'entrée dans la phase européenne (OEB Form 1200) est déposé **en ligne**:	**100,00**
Zusatzgebühr * **Additional fee *** **Taxe additionnelle ***	**Für die 36. und jede weitere Seite** Anwendbar für **ab dem 1. April 2009** in die europäische Phase eintretende internationale Anmeldungen: **For the 36th and each subsequent page** Applicable to international applications entering the European phase **on or after 1 April 2009**: **Pour chaque page à partir de la 36ième** Applicable aux demandes internationales entrant dans la phase européenne **à compter du 1er avril 2009:**	**12,00**
Recherchengebühr ** **Search fee **** **Taxe de recherche ****	Anwendbar für **vor dem 1. Juli 2005** eingereichte internationale Anmeldungen: Applicable to international applications filed **before 1 July 2005**: Applicable aux demandes internationales déposées **avant le 1er juillet 2005**:	**760,00**
	Anwendbar für **ab dem 1. Juli 2005** eingereichte internationale Anmeldungen : Applicable to international applications, filed **on or after 1 July 2005**: Applicable aux demandes internationales déposées **à compter du 1er juillet 2005**:	**1050,00**
Benennungsgebühr * **Designation fee ***	**Für jeden benannten Vertragsstaat** (siebenfacher Betrag = alle Vertragsstaaten) Anwendbar für **vor dem 1. April 2009** in die europäische Phase eingetretene internationale Anmeldungen: **For each Contracting State designated** (seven times the amount = all Contracting States) Applicable to international applications having entered the European phase **before 1 April 2009:** **Pour chaque État contractant désigné** (sept fois cette taxe = tous les États contractants) Applicables aux demandes internationales entrées dans la phase européenne **avant le 1er avril 2009:**	**85,00**
Taxe de désignation*	**Für einen oder mehr benannte Vertragsstaaten** Anwendbar für **ab dem 1. April 2009** in die europäische Phase eintretende internationale Anmeldungen: **For one or more designated Contracting States** Applicable to international applications entering the European phase **on or after 1 April 2009:** **Pour un ou plusieurs États contractants désignés** Applicable aux demandes internationales entrant dans la phase européenne **à compter du 1er avril 2009**	**500,00**
Prüfungsgebühr ** **Examination fee **** **Taxe d'examen ****	Anwendbar für **vor dem 1. Juli 2005** eingereichte internationale Anmeldungen: Applicable to international applications filed **before 1 July 2005**: Applicable aux demandes internationales **déposées avant le 1 juillet 2005**:	**1565,00**
	Anwendbar für **ab dem 1. Juli 2005** eingereichte internationale Anmeldungen: Applicable to international applications filed **on or after 1 July 2005**: Applicable aux demandes internationales déposées **à compter du 1er juillet 2005**:	**1405,00**
	Anwendbar für **ab dem 1.Juli 2005** eingereichte internationale Anmeldungen, für die **kein** ergänzender europäischer Recherchenbericht erstellt wird (Art.153(7) EPÜ): Applicable to international applications filed **on or after 1 July 2005** for which **no** supplementary European search report is drawn up (Art. 153(7) EPC): Applicable aux demandes internationales déposées **à compter du 1er juillet 2005** pour lesquelles **il n'est pas** établi de rapport complémentaire de recherche européenne (Art. 153(7) CBE):	**1565,00**
Weiterbehandlungsgebühr (R. 135 EPÜ, Art. 2 GebO) **Fee for further processing** (R. 135 EPC, Art. 2 RFees) **Taxe de poursuite de la procédure** (R. 135 CBE, Art. 2 RRT)	Bei verspäteter **Gebührenzahlung**: In the event of late **payment of a fee**: En cas de retard de **paiement de taxe**:	**50% der betreffenden Gebühr** **50% of the relevant fee** **50% de la taxe concernée**
	Bei verspäteter Einreichung des **schriftlichen Prüfungsantrags** oder der **Übersetzung**: In case the **written request for examination** or the **translation** is filed late: En cas de retard de dépôt de la **requête écrite en examen** ou de la **traduction**:	**je** **each** **210,00** **chaque**
** Ermäßigungen können zutreffen (**ABl. EPA 2008, 130**) / Reductions may apply (**OJ EPO 2008, 130**) / Des réductions peuvent s'appliquer (**JO OEB 2008, 130**)		

* = Siehe Mitteilung des Europäischen Patentamts vom 26.01.2009 über die Gebührenstruktur 2009 (**ABl. EPA 2009, 118**)
See Notice from the European Patent Office of 26.01.2009 concerning the 2009 fee structure (**OJ EPO 2009, 118**)
Voir Communiqué de l'Office européen des brevets en date du 26.01.2009, relatif à la structure des taxes 2009 (**JO OEB 2009, 118**)

Hinweis/note/avis:
Die Zahlung mittels Schecks ist nicht möglich (**ABl. EPA 2007, 626**)
Payment by cheque is not accepted (**OJ EPO 2007, 626**)
Le paiement par chèque n'est pas accepté (**JO OEB 2007, 626**)

Bankkonten der Europäischen Patentorganisation in EURO (04.09)
Bank accounts of the European Patent Organisation in EURO (04.09)
Comptes bancaires de l'Organisation européenne des brevets en EURO (04.09)

Staat Country Pays	Bankkonto Bank account Compte bancaire	Anschrift Address Adresse	Staat Country Pays	Bankkonto Bank account Compte bancaire	Anschrift Address Adresse
AT	**No.** 102-133-851/00 (BLZ 12 000) **IBAN** AT91 1200 0102 1338 5100 **BIC** BKAUATWW	Bank Austria Creditanstalt AG Am Hof 2 Postfach 52000 1010 Wien AUSTRIA	**IS**	**No.** 0101-38-710440 **IBAN** IS77 0101 3871 0440 4312 0490 80 **BIC** LAISISRE Id no. EPO 431204-9080 (compulsary)	National Bank of Iceland Main Branch Austurstraeti 11 101 Reykjavik ICELAND
BE	**No.** 310-0449878-78 **IBAN** BE69 3100 4498 7878 **BIC** BBRUBEBB	ING Belgium Marnix Business Branch 1, rue du Trône 1000 Bruxelles BELGIUM	**IT**	**No.** 936832 01 94 (conto estero) **IBAN** IT21 E030 6905 0200 0936 8320 194 **BIC** BCITITMM700 ABI 03069 / CAB 05020	Intesa Sanpaolo S.P.A. Via del Corso, 226 00186 Roma ITALY
BG	**No.** 1465104501 **IBAN** BG72 UNCR 7630 1465 1045 01 **BIC** UNCR BGSF	Unicredit Bulbank 7, Sveta Nedelya Sq. 1000 Sofia BULGARIA	**LT**	**No.** LT52 7044 0600 0559 2279 **IBAN** LT52 7044 0600 0559 2279 **BIC** CBVI LT 2X	AB SEB Vilniaus bankas Gedimino pr. 12 1103 Vilnius LITHUANIA
CH	**No.** 230-322 005 60 M **IBAN** CH49 0023 0230 3220 0560 M **BIC** UBSWCHZH80A	UBS Bahnhofstrasse 45 8021 Zürich SWITZERLAND	**LU**	**No.** 7-108/9134/200 **IBAN** LU41 0027 1089 1342 0000 **BIC** BILLLULL	DEXIA Banque Internationale à Luxembourg 69, Route d'Esch 2953 Luxembourg LUXEMBOURG
CY	**No.** 0155-41-190144-48 **IBAN** CY68 0020 0155 0000 0041 1901 4448 **BIC** BCYPCY2N	Bank of Cyprus 2-4 Them. Dervi Street P.O. Box 1472 1599 Nicosia CYPRUS	**LV**	**No.** LV40UNLA0050008873109 **IBAN** LV40UNLA0050008873109 **BIC** UNLALV2XXXX	SEB Latvijas Unibanka Unicentrs, Kekavas Pagasts 1076 Rigas Rajons LATVIA
CZ	**No.** 01841280/0300 **IBAN** CZ52 0300 1712 8010 1700 2453 **BIC** CEKOCZPP	Ceskoslovenska Obchodni Banka A.S. Na Prikope 854/14 11520 Praha 1 - Nové Mesto CZECH REPUBLIC	**MC**	**No.** 30004 09179 00025422154 91 (RIB) **IBAN** FR76 3000 4091 7900 0254 2215 491 **BIC** BNPAFRPPAMC	BNP - Paribas Agence Monaco Charles III Avenue de la Madone 98000 Monaco MONACO
DE	**No.** 3 338 800 00 (BLZ 700 800 00) **IBAN** DE20 7008 0000 0333 880000 **BIC** DRESDEFF SWIFT DRESDEFF700	Dresdner Bank Promenadeplatz 7 80273 München GERMANY	**MK**	Not yet available Noch nicht verfügbar Pas encore disponible	FORMER YUGOSLAV REPUBLIC of MACEDONIA
DK	**No.** 3001014560 **IBAN** DK94 3000 3001 0145 60 **BIC** DABADKKK	Danske Bank A/S Holmens Kanal Dept. Holmens Kanal 2-12 1092 Kopenhagen K DENMARK	**MT**	Not yet available Noch nicht verfügbar Pas encore disponible	MALTA
EE	**No.** 10220025988223 **IBAN** EE24 1010 2200 2598 8223 **BIC** EEUHEE2X	SEB Eesti Ühispank AS Tornimäe 2, Tallinn 15010 Tallinn ESTONIA	**NL**	**No.** 51 36 38 547 **IBAN** NL54 ABNA 0513 6385 47 **BIC** ABNANL2A	ABN-AMRO Bank NV Kneuterdijk 1 Postbus 165 2501 AP Den Haag THE NETHERLANDS
ES	**No.** 0182-2325-08-029-0348002 **IBAN** ES54 0182 2325 0802 9034 8002 **BIC** BBVAESMM	Banco Bilbao Vizcaya Argentaria Calle Alcalá 16, 1a Planta Oficina 2325 (Banca de Empresas) 28014 Madrid SPAIN	**NO**	Not yet available Noch nicht verfügbar Pas encore disponible	NORWAY
FI	**No.** 200118-182076 **IBAN** FI28 2001 1800 1820 76 **BIC** NDEAFIHH	Nordea Bank Finland plc, 1820 Foreign Customer Services Mannerheimintie 7, Helsinki 00020 Nordea FINLAND	**PL**	**No.** 42103015080000000504086003 **IBAN** PL42 1030 1508 0000 0005 0408 6003 **BIC** CITIPLPX	Bank Handlowy w Warszawie S.A. Senatorska 16 00-923 Warsawa POLAND
FR	**No.** 30004 00567 00020020463 29 (RIB) **IBAN** FR76 3000 4005 6700 0200 2046 329 **BIC** BNPAFRPPPOP	BNP - Paribas Agence: Paris Clientèle Internationale 2, Place de l'Opéra 75002 Paris FRANCE	**PT**	**No.** 2088391145 **IBAN** PT50 0033 0000 0208 8391 1452 2 **BIC** BCOMPTPL	Millennium bcp Banco Comercial Português Av. Fontes Pereira de Melo, 7 1050-115 Lisboa PORTUGAL
GB	**No.** 86 98 72 66 (Sorting Code 20-47-35) **IBAN** GB10 BARC 2047 3586 9872 66 **BIC** BARCGB22	Barclays Bank plc International Corporate PO Box 391 38 Hans Crescent Knightsbridge London SW1X 0LZ THE UNITED KINGDOM	**RO**	**No.** 279682 **IBAN** RO36 BACX 0000 0002 7968 2000 **BIC** BACX ROBU	Unicredit Tiriac Bank S.A. Sucursala Rosetti Str. C.A. Rosetti Nr. 36, Sectorul 2, 020015 Bucaresti ROMANIA
GR	**No.** 112002002007046 **IBAN** GR36 0140 1120 1120 0200 2007 046 **BIC** CRBAGRAAXXX	Alpha Bank Athens Tower Branch 2, Messoghion Avenue 115 27 Athens GREECE	**SE**	**No.** 6014-48857939 **IBAN** SE08 6000 0000 0000 4885 7939 **BIC** HANDSESS	SHB, HIFF-L Svenska Handelsbanken 106 70 Stockholm SWEDEN
HR	Not yet available Noch nicht verfügbar Pas encore disponible	CROATIA	**SI**	**No.** 03500-1000001709 **IBAN** SI56 0350 0100 0001 709 **BIC** SKBASI2X	SKB Banka D.D. Ajdovscina 4 1513 Ljubljana SLOVENIA
HU	**No.** 11764946-00239880 **IBAN** HU46 1176 4946 0023 9880 0000 0000 **BIC** OTPVHUHB	OTP Bank Rt. Központi Fiók Deák Ferenc utca 7-9 1052 Budapest HUNGARY	**SK**	**No.** 2920480237 (Bank code 1100) **IBAN** SK89 1100 0000 0029 2048 0237 **BIC** TATRSKBX	Tatra Banka A.S. Branch Banska Bystrica Dolna 2 97401 Banska Bystrica SLOVAKIA
IE	**No.** 309 822 01 (Bank Code 901 490) **IBAN** IE10 BOFI 9014 9030 9822 01 **BIC** BOFIIE2D	Bank of Ireland Lower Baggot Street Branch P.O. Box 3131 Dublin 2 IRELAND	**TR**	**No.** 4214-301120-1039000 **IBAN** TR89 0006 4000 0024 2141 039000 **BIC** ISBKTRIS	Türkiye IS Bankasi A.S. Gazi Mustafa Kemal Bulvari 8 06640 Kizilay / Ankara TURKEY