Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on February 12, 2008.

Robert D. Summers, Jr., Reg. No. 57,844

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371		ATTORNEY'S DOCKET NO. **12838/5 (729727US)** U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
INTERNATIONAL APPLICATION NO. **PCT/AU2006/001136**	INTERNATIONAL FILING DATE **August 10, 2006**	PRIORITY DATE CLAIMED **August 12, 2005**
TITLE OF INVENTION **IMPROVING CARD DEVICE SECURITY USING BIOMETRICS**		
APPLICANT(S) FOR DO/EO/US **BURKE, Christopher John**		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9), and (21) indicated below.
4. ☒ The US has been elected (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2)):
   - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   - b. ☐ has been transmitted by the International Bureau.
   - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application into English (35 U.S.C. 371(c)(2)):
   - a. ☐ is attached hereto.
   - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)):
   - a. ☒ are transmitted herewith (required only if not transmitted by the International Bureau).
   - b. ☐ have been transmitted by the International Bureau.
   - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An [unexecuted] Declaration for Patent.
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)) and/or amendments under Article 34.

Items 11 to 20 Below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98, PTO Form 1449; copies of cited references A3-A6.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A preliminary amendment.
14. ☐ An Application Data Sheet under 37 CFR 1.76.
15. ☐ A substitute specification.
16. ☐ A power of attorney and/or change of address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.2 and 37 CFR 1.821-1.825.
18. ☐ A second copy of the published International Application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☐ Other items or information: Return Postcard, .

SEND COMPLETED FORM TO: Mail Stop PCT, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

U.S. APPLICATION NO. (If known, see 37 CFR 1.50)	INTERNATIONAL APPLICATION NO. PCT/AU2006/001136	ATTORNEY'S DOCKET NO. 12838/5

CALCULATIONS PTO USE ONLY

The following fees are submitted:

21. ☒ Basic National Fee (37 CFR 1.492(a))..........$310

22. ☒ Examination Fee (37 CFR 1.492(c))
    - If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..........$ 0
    - All other situations..........$210

23. ☒ Search Fee (37 CFR 1.492(b))
    - If the written opinion of the ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..........$ 0
    - Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority..........$100
    - International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB..........$410
    - All other situations..........$510

Claims	Number Filed	Number Extra	Rate	CALCULATIONS	PTO USE ONLY
TOTAL OF 21, 22 and 23 =				$930	
□ Fee of **$260** for each additional 50 sheets for specification and drawings that exceed 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium) (37 CFR 1.492(j)).				$	
□ Surcharge of **$130** for furnishing oath or declaration after 30 months from earliest claimed priority date (37 CFR 1.492(h)).				$	
Total Claims	20 - 20 =		x $ 50.00	$	
Independent Claims	6 - 3 =	3	x $210.00	$ 630	
Multiple dependent claim(s) if Applicable)			+ $370.00	$	
TOTAL OF ABOVE CALCUATIONS =				$ 1560	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by one-half.				$780	
SUBTOTAL =				$	
□ Fee of **$130** for furnishing the English language translation after 30 months from earliest claimed priority date (37 CFR 1.492(i)).				$	
TOTAL NATIONAL FEE =				$	
□ Recordal Fee of **$40** (per property) for recording the attached assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31).				$	
TOTAL FEES ENCLOSED =				$780	
				Amount to be refunded	$
				Amount to be charged	$

a. □ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge Deposit Account No. 23-1925 in the amount of $780.00 to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 23-1925.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

Advisory: If filing by EFS-Web, do NOT attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is NOT recommended and by doing so your credit card information may be displayed via PAIR. To protect your information, it is recommended paying fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Send all correspondence to the address associated with
Customer No. 00757 - Brinks Hofer Gilson Lione

Signature

Name
Robert D. Summers, Jr.
Registration No. 57,844

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on February 12, 2008.

Robert D. Summers, Jr., Reg. No. 57,844

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371		ATTORNEY'S DOCKET NO. **12838/5 (729727US)** U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
INTERNATIONAL APPLICATION NO. **PCT/AU2006/001136**	INTERNATIONAL FILING DATE **August 10, 2006**	PRIORITY DATE CLAIMED **August 12, 2005**

TITLE OF INVENTION
IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

APPLICANT(S) FOR DO/EO/US
BURKE, Christopher John

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. □ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9), and (21) indicated below.
4. ☒ The US has been elected (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2)):
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ has been transmitted by the International Bureau.
   c. □ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. □ An English language translation of the International Application into English (35 U.S.C. 371(c)(2)):
   a. □ is attached hereto.
   b. □ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)):
   a. ☒ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ have been transmitted by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. □ have not been made and will not be made.
8. □ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An [unexecuted] Declaration for Patent.
10. □ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)) and/or amendments under Article 34.

Items 11 to 20 Below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98, PTO Form 1449; copies of cited references A3-A6.
12. □ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A preliminary amendment.
14. □ An Application Data Sheet under 37 CFR 1.76.
15. □ A substitute specification.
16. □ A power of attorney and/or change of address letter.
17. □ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.2 and 37 CFR 1.821-1.825.
18. □ A second copy of the published International Application under 35 U.S.C. 154(d)(4).
19. □ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. □ Other items or information: Return Postcard, .

SEND COMPLETED FORM TO: Mail Stop PCT, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

U.S. APPLICATION NO. (If known, see 37 CFR 1.50)	INTERNATIONAL APPLICATION NO. PCT/AU2006/001136	ATTORNEY'S DOCKET NO. 12838/5

The following fees are submitted:

CALCULATIONS PTO USE ONLY

21. ☒ Basic National Fee (37 CFR 1.492(a))....................$310

22. ☒ Examination Fee (37 CFR 1.492(c))
- If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)....................$ 0
- All other situations....................$210

23. ☒ Search Fee (37 CFR 1.492(b))
- If the written opinion of the ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)....................$ 0
- Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority....................$100
- International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB....................$410
- All other situations....................$510

				CALCULATIONS	PTO USE ONLY
			TOTAL OF 21, 22 and 23 =	$930	
☐ Fee of **$260** for each additional 50 sheets for specification and drawings that exceed 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium) (37 CFR 1.492(j)).				$	
☐ Surcharge of **$130** for furnishing oath or declaration after 30 months from earliest claimed priority date (37 CFR 1.492(h)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	20 - 20 =		x $ 50.00	$	
Independent Claims	6 - 3 =	3	x $210.00	$ 630	
Multiple dependent claim(s) if Applicable)			+ $370.00	$	
			TOTAL OF ABOVE CALCUATIONS =	$ 1560	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by one-half.				$780	
			SUBTOTAL =	$	
☐ Fee of **$130** for furnishing the English language translation after 30 months from earliest claimed priority date (37 CFR 1.492(i)).				$	
			TOTAL NATIONAL FEE =	$	
☐ Recordal Fee of **$40** (per property) for recording the attached assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31).				$	
			TOTAL FEES ENCLOSED =	$780	
				Amount to be refunded	$
				Amount to be charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge Deposit Account No. 23-1925 in the amount of $780.00 to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 23-1925.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

Advisory: If filing by EFS-Web, do NOT attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is NOT recommended and by doing so your credit card information may be displayed via PAIR. To protect your information, it is recommended paying fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

Send all correspondence to the address associated with **Customer No. 00757 - Brinks Hofer Gilson Lione**	Signature
	Name Robert D. Summers, Jr.
	Registration No. 57,844

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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
22 February 2007 (22.02.2007)

PCT

(10) **International Publication Number**
WO 2007/019605 A1

(51) **International Patent Classification:**
G07F 7/10 (2006.01) ***G06K 9/00*** (2006.01)
G07F 19/00 (2006.01) ***G07F 7/12*** (2006.01)

(21) **International Application Number:** PCT/AU2006/001136

(22) **International Filing Date:** 10 August 2006 (10.08.2006)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
2005904375 12 August 2005 (12.08.2005) AU

(71) **Applicant** *(for all designated States except US)*: **SECURICOM (NSW) PTY LTD** [AU/AU]; 48 Margate Street, Ramgate, NSW 2217 (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).

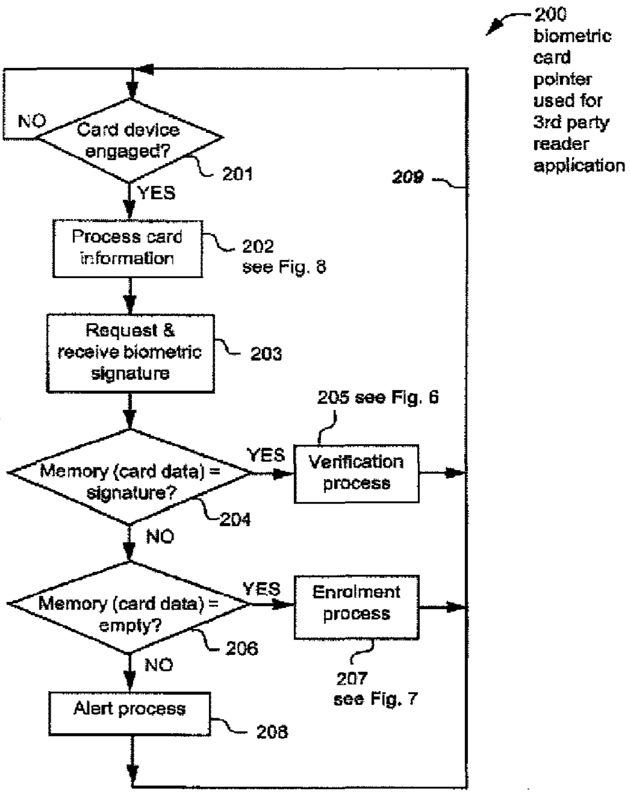
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** IMPROVING CARD DEVICE SECURITY USING BIOMETRICS



(57) **Abstract:** The disclosed Biometric Card Pointer arrangements store (207) a card user's biometric signature in a local memory (124) in a verification station (127) the first time the card user uses the verification station (127) in question. The biometric signature is stored at a memory address (607) defined by the card information (605) on the user's card (601). All future uses of the particular verification station (127) by someone submitting the aforementioned card (601) requires 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 (605) thereby determining if the person submitting the card is authorised to do so.

WO 2007/019605 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

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 secure access purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account 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 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.

Another type of card device is the wireless "key-fob" which is a small radio transmitter that emits a radio frequency (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^{TM} 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.

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 input 801, for example by pressing their thumb against a biometric (eg 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 information 801. This is cumbersome and potentially compromises the privacy 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.

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, referred to as Biometric Card Pointer (BCP) arrangements or systems, which seek to address the above problems relating to secure access and/or secure processes, 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.

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 defined by the ("unique") card information on the user's card as read by the card reader of the verification station. Clearly 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 someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, 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.

Each use of the verification station is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature (eg thumb print or retinal scan etc.) to the biometric reader.

An authorised card user will be automatically verified by the BCP arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update etc. will simply proceed as normal. An unauthorised card user (ie a card user who misappropriated the card after the initial enrolment) will not receive authorisation, and the intended transaction will not proceed. Furthermore, the biometric signature of the unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user and prove misappropriation of the card.

The disclosed BCP arrangements require little if any modification of the back-end systems or the (front-end) card. The additional administrative overheads associated with the BCP arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The BCP 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 BCP arrangements are implemented. Users of current card systems can learn to use BCP arrangements without much effort, needing only to provide a biometric signature when asked to do so at the verification station. The difference between the enrolment and verification phases are transparent to users, further reducing the effort in learning how to use the BCP arrangements.

According to a first aspect of the present invention, there is provided a method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature; and

storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to another aspect of the present invention, there is provided a method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the noted enrolment method;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

According to another aspect of the present invention, there is provided a method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to 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 of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature; and

code for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to 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 of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the noted enrolment method;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

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 BCP arrangements can be practiced;

Fig. 4 illustrates the biometric card pointer concept;

Fig. 5 is a flow chart of a process for using the biometric card pointer arrangement;

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; and

Fig. 9 shows an alternate use for the biometric card pointer arrangement.

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 disclosed BCP arrangements can be practiced. The disclosed BCP methods 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** and **9** may be implemented as software, such as a BCP application program executing within the computer system 100. In particular, the steps of the BCP processes are effected by instructions in the BCP 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 BCP software may also be divided into two separate parts, in which a first part performs the BCP methods and a second part manages a user interface between the first part and the user.

The BCP software may be stored in a computer readable medium, including the storage devices described below, for example. The BCP software is loaded into the verification station 127 from the computer readable medium, and 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 BCP arrangements.

The verification station 127 comprises, in the described arrangement, a biometric card pointer reader 125, a keypad 103, and a computer module 101. The biometric card pointer reader is made up of a biometric reader 102, a card device reader 112 and a local database 124.

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 BCP 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 BCP 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. The card information 605 can be encoded using a magnetic strip, a bar code, or a solid state memory on the card 601. Alternately, the card device can be implemented as a wireless key fob. In one example of the disclosed BCP approach, the card data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an 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 disclosed BCP system to determine if the card 601 is to be processed according to the disclosed BCP approach or not. This is described in more detail in regard to **Fig. 8**. Alternately, any segment of the card information 605 can be used as the memory reference which points to the particular memory location in the local database 124.

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 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 memory 124 where their unique biometric signature is stored.

Thereafter, in later verification phases, the user couples their card 601 to the card reader 112, after which the card user is required to again present their unique biometric to the biometric reader 102. This signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112. Once verification is confirmed, the card information 605 is transferred from 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 disclosed BCP arrangement. 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 BCP arrangement 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 an inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Fig. 5 shows a process 200 for normal use of the BCP approach. 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 processes the card information 605 that is read from the card 601 by the card reader 112. 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 memory 124 in an earlier enrolment phase. It is also noted that the step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203. There is no need to search the entire database 124 to see if there is a match. Thus the disclosed BCP arrangement provides a particularly simple and fast biometric verification check thereby securing the process associated with the step 205. Once the step 205 has completed the verification process, the process 200 is directed according to an arrow 209 back to the step 201.

In an alternate arrangement, the card data 604 can be associated with a group of memory locations, rather than being the address for a specific memory location. This arrangement allows a different biometric signature to be stored in each of the group of memory locations, and in this case, the step 204 reads the contents stored in each memory location in the group defined by the card data 604, and checks the contents of each memory location in the group against the biometric signature received in the step 203. If the contents of any member of the group of memory locations matches, 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. This arrangement allows, for example, two cards having the same card data 604 to be used at the same verification station 127 after each card holder performs their own individual enrolment process.

Returning to the step 204, if the contents 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 contents of the memory 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 contents 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 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, and can capture the card in the verification station 127, thereby removing the card from the possession of the apparently unauthorised person.

The alert process 208 can send, as part of the alert message, send all or part of the card information 605 that is input to the verification station 127 in the step 201 of **Fig. 5.**

Although in the above description the step 206 tests if the memory location defined by the card data 604 is "empty", other approaches can be used. Thus when enrolment is performed, resulting in a memory location being used to store a biometric signature (eg see step 401 in **Fig. 7**), a flag can be set to indicate that the memory location in question is occupied. The term "occupied" in this context means that the memory location in question has been used in the enrolment process for a user, and that the information stored at the memory location in question has not been deleted by a BCP system administrator. If the signature stored in the database 124 at the particular memory location is deleted by a BCP system administrator (as described in regard to **Fig. 8**) then the flag can be reset to indicate that the memory location in question is no longer occupied.

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 signal 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 (which may be viewed as a process of obtaining verified access to a protected resource), whatever that may be. Thus, for example, if the process 200 of **Fig. 5** relates withdrawal of cash from an Automatic Teller Machine (ATM) operated by one of a number of service providers, 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**. The aforementioned step 401 can store the biometric signature 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. 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. 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. A separate, or overlapping, permitted card set is defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the BCP process at any given verification station 127. This has the advantage of ensuring that the local memory 124 does not overflow, and it also provides control over which users make use of which verification stations.

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 set of permitted cards 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 BCP 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 BCP system administrator. 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. 9 shows another application 900 to which the BCP arrangement 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 another example, the holder of the card 601 takes the card 601 and the portable verification station 127 to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card 601 is able to apply the card to the card reader 112, apply their biometric signature to the biometric reader 102, and have the verification station 127 output the corresponding card information 605. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card 601 is the authorised owner.

Industrial Applicability

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

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP 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.

Thus, for example, the BCP arrangement 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.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is fist issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room, negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP 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 disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement 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 **Fig. 5.**

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.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature; and

storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

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

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

a smart card 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.

5. A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised.

9. A method according to any one of claims 6, 7 and 8 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.

10. A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader receiving the biometric signature; and

means for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

12. A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

13. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature; and

code for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

18. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

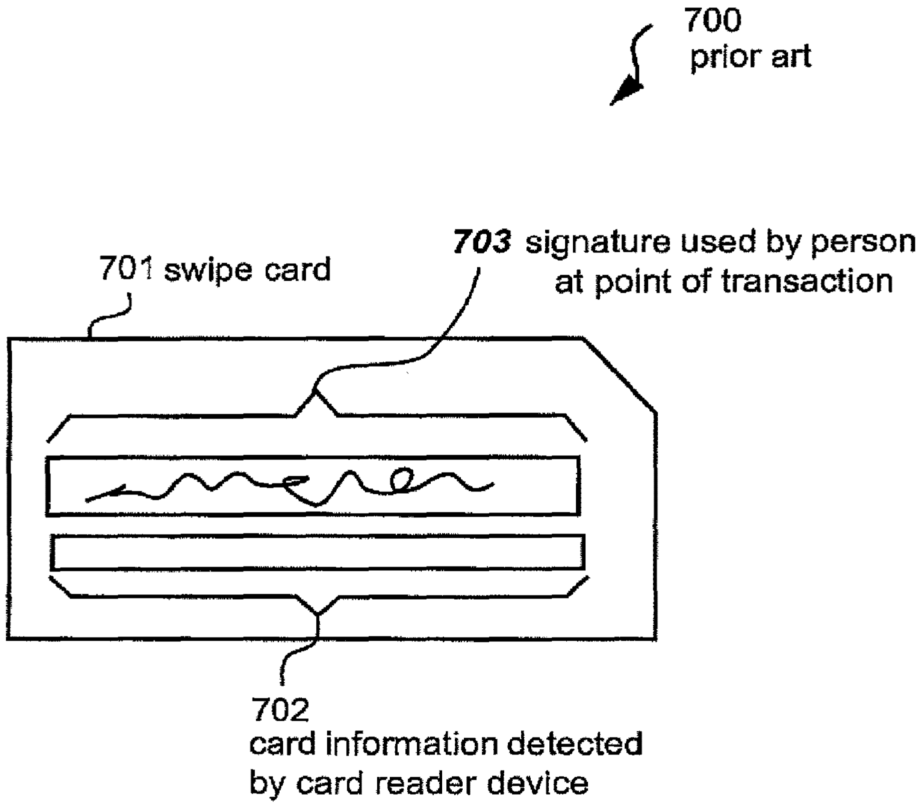


Fig. 1
prior art

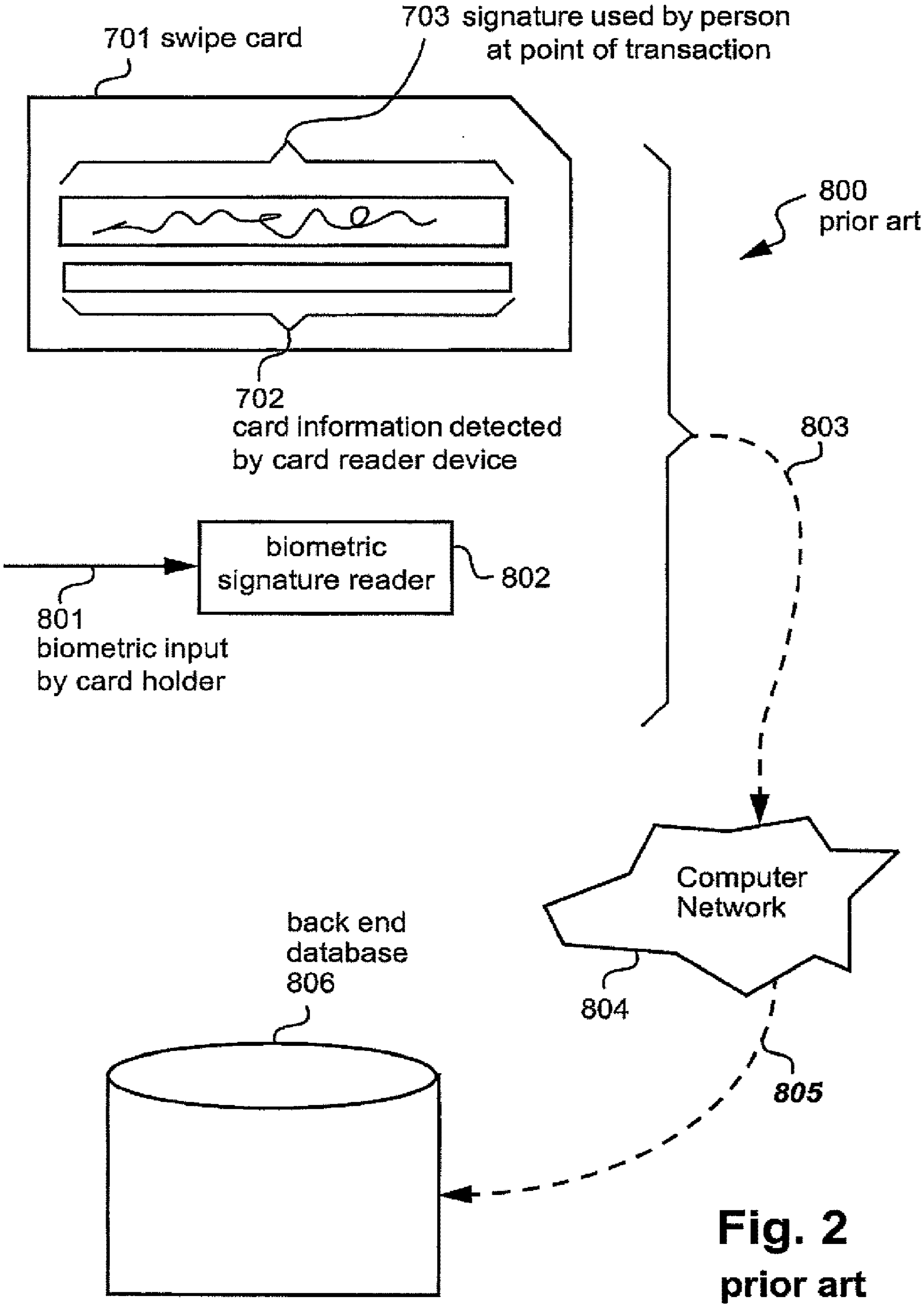

701 swipe card
703 signature used by person at point of transaction
800 prior art
702 card information detected by card reader device
803
biometric signature reader
802
801 biometric input by card holder
Computer Network
back end database 806
804
805

Fig. 2
prior art

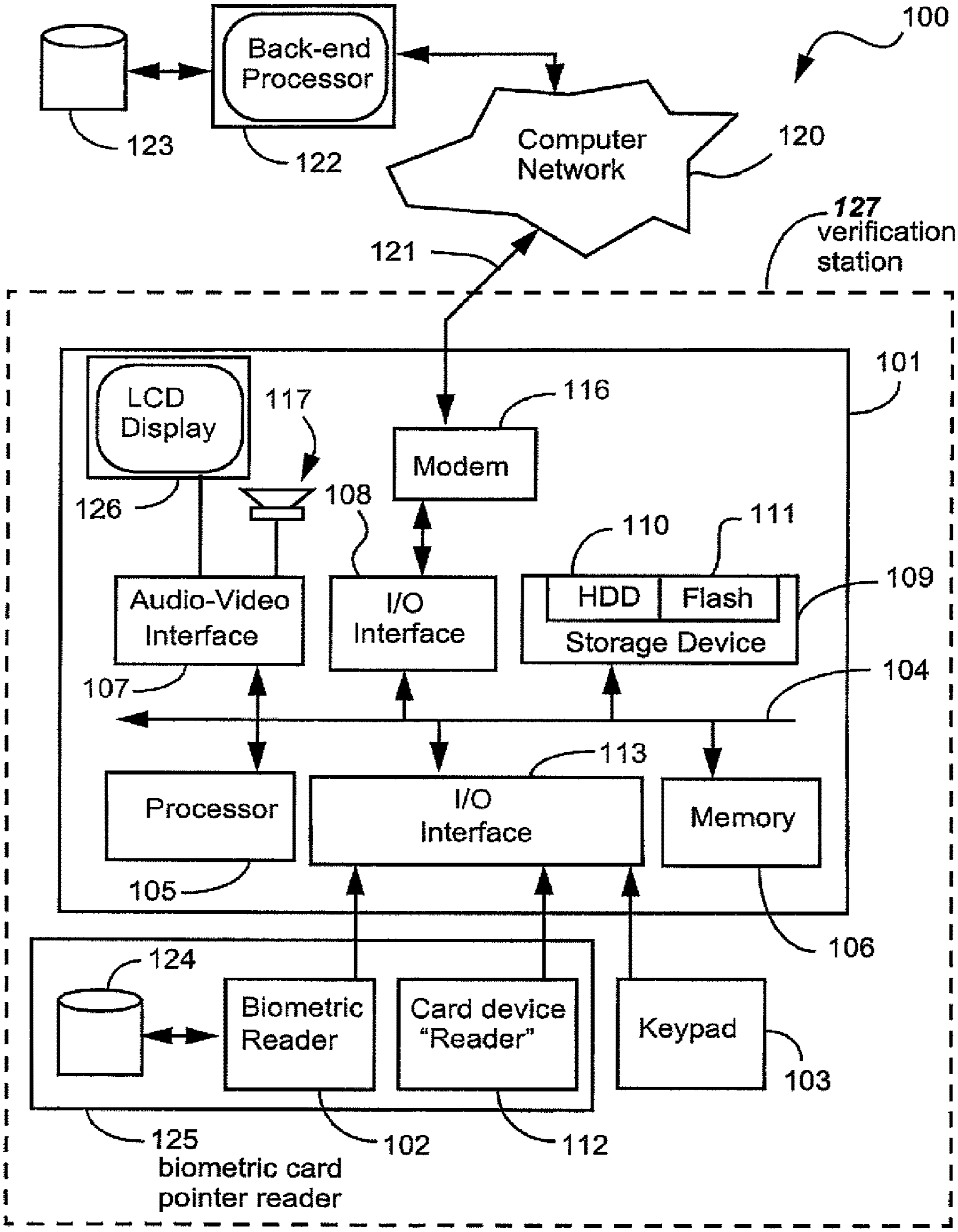

100
Back-end Processor
123
122
Computer Network
120
121
127 verification station
101
LCD Display
117
116
Modem
126
108
110
111
109
Audio-Video Interface
I/O Interface
HDD
Flash
Storage Device
107
104
113
Processor
I/O Interface
Memory
105
106
124
Biometric Reader
Card device "Reader"
Keypad
103
125 biometric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

Fig. 3

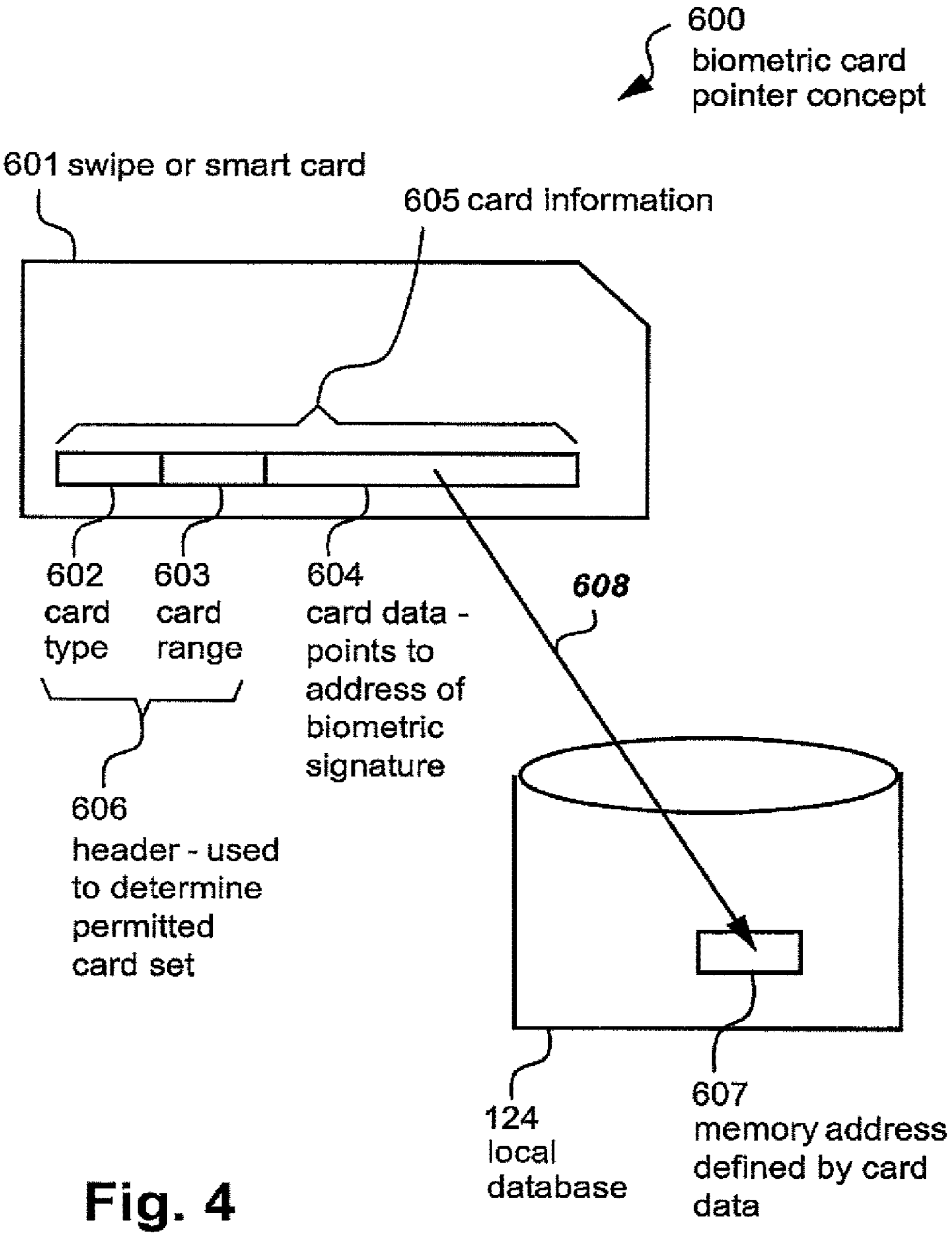

600
biometric card
pointer concept
601 swipe or smart card
605 card information
602
card
type
603
card
range
604
card data -
points to
address of
biometric
signature
608
606
header - used
to determine
permitted
card set
124
local
database
607
memory address
defined by card
data

Fig. 4

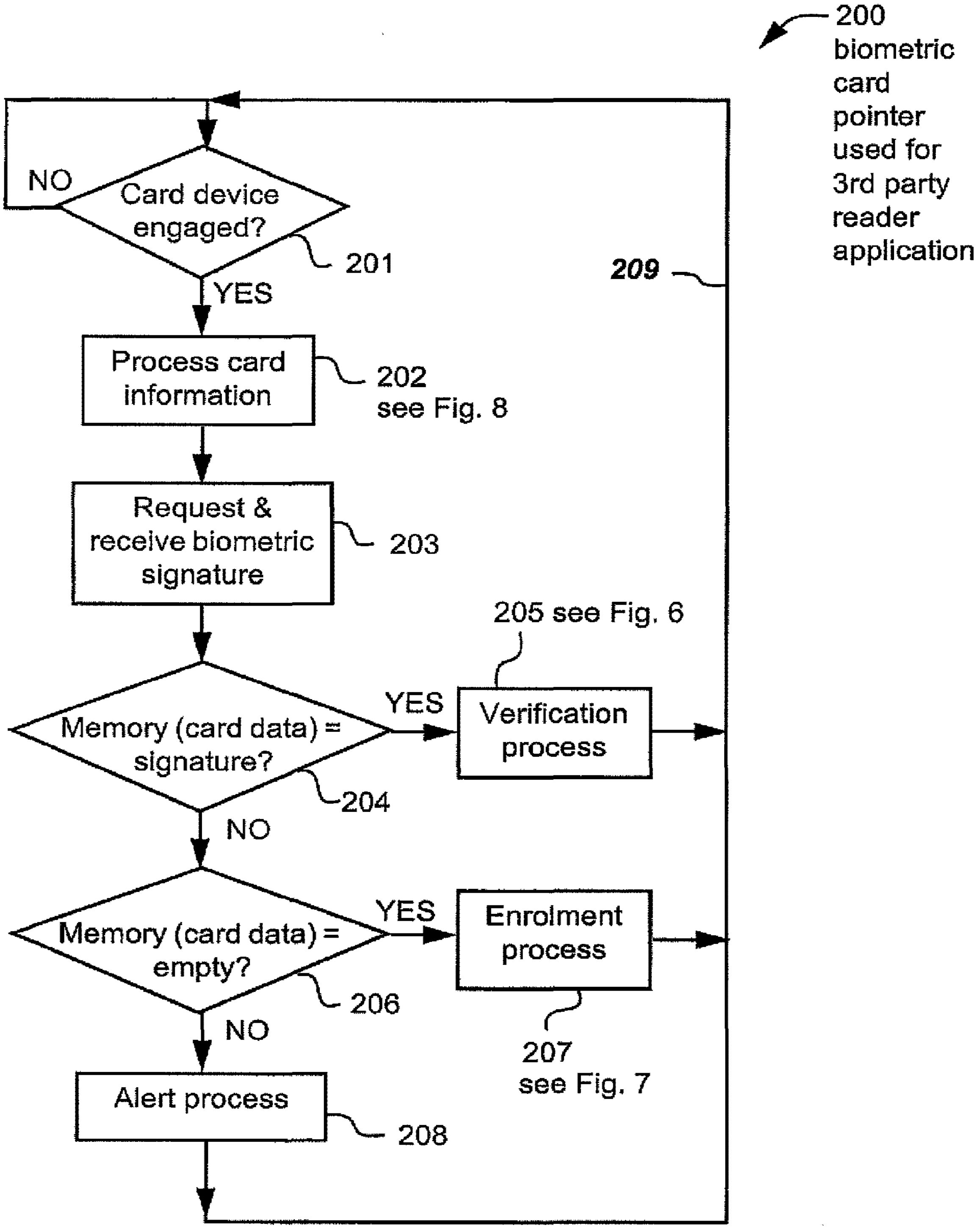

200
biometric card pointer used for 3rd party reader application
Card device engaged?
NO
YES
201
Process card information
202
see Fig. 8
Request & receive biometric signature
203
Memory (card data) = signature?
YES
204
NO
Verification process
205 see Fig. 6
Memory (card data) = empty?
YES
206
NO
Enrolment process
207
see Fig. 7
Alert process
208
209

Fig. 5

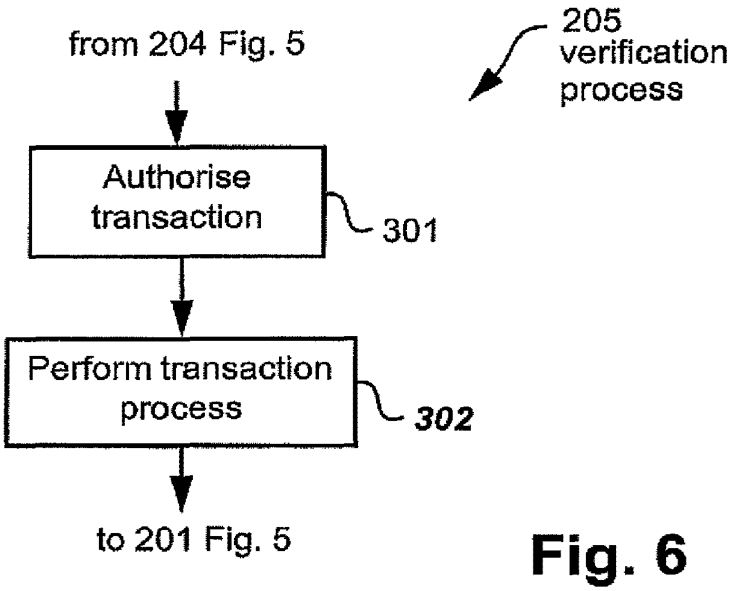

from 204 Fig. 5
205
verification
process
Authorise transaction
301
Perform transaction process
302
to 201 Fig. 5

Fig. 6

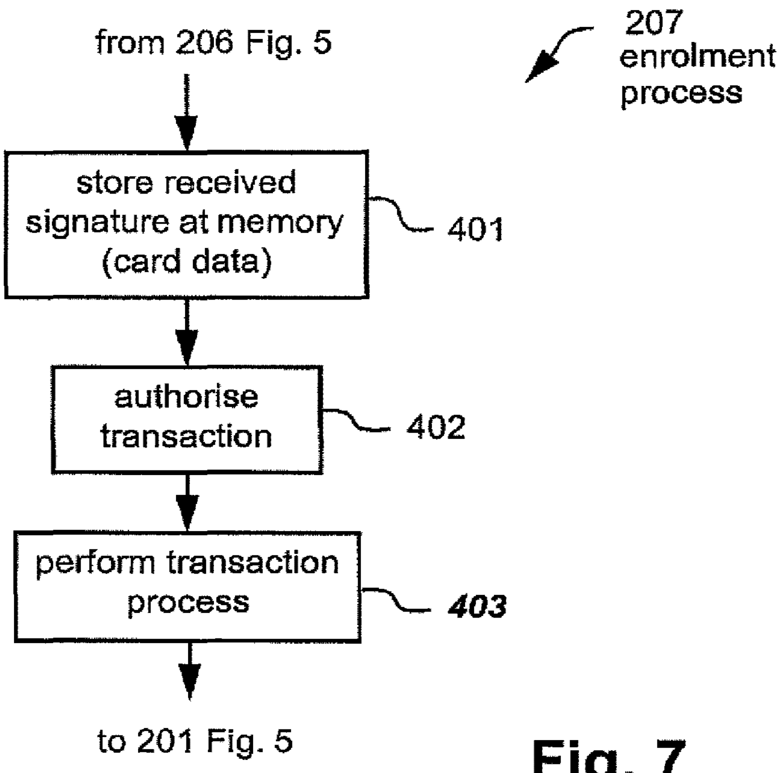

from 206 Fig. 5
207
enrolment
process
store received signature at memory (card data)
401
authorise transaction
402
perform transaction process
403
to 201 Fig. 5

Fig. 7

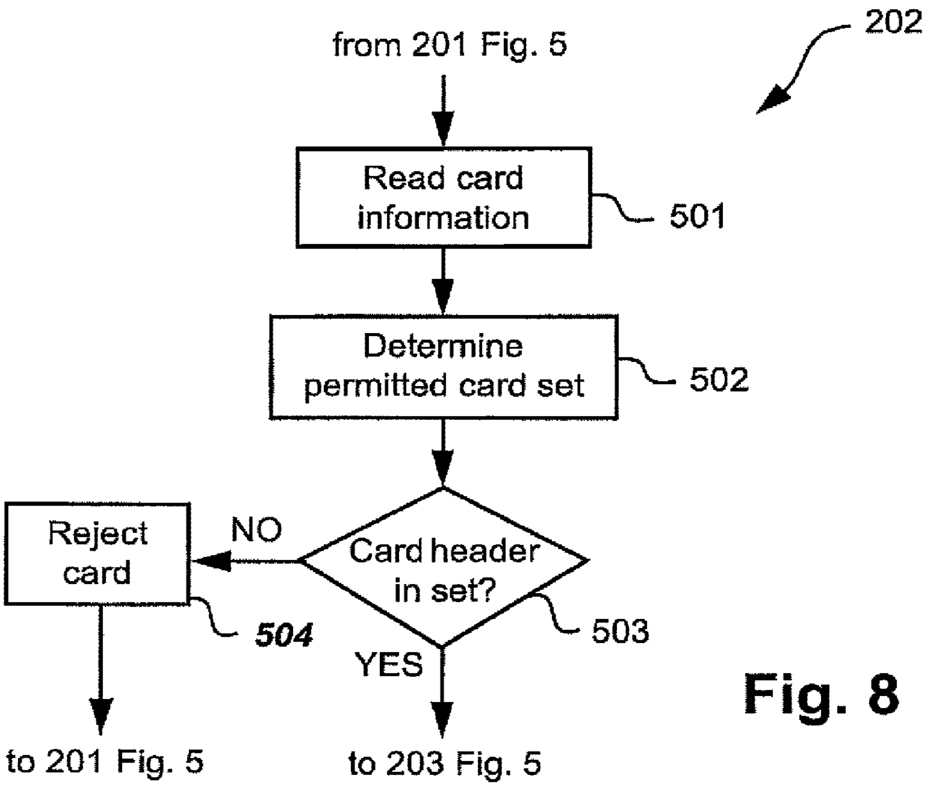

from 201 Fig. 5
202
Read card information
501
Determine permitted card set
502
Card header in set?
503
NO
Reject card
504
YES
to 201 Fig. 5
to 203 Fig. 5

Fig. 8

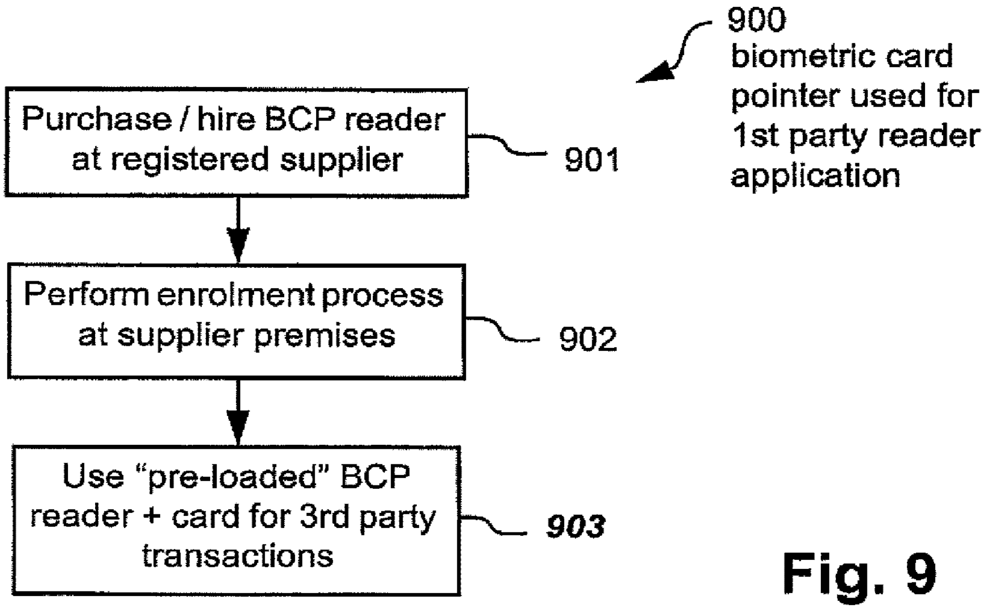

900
biometric card pointer used for 1st party reader application
Purchase / hire BCP reader at registered supplier
901
Perform enrolment process at supplier premises
902
Use "pre-loaded" BCP reader + card for 3rd party transactions
903

Fig. 9

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on February 12, 2008.

Robert D. Summers, Jr., Reg. No. 57,844

Our Case No. 12838/5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	CHRISTOPHER J. BURKE
Appln. No.:	Not Yet Assigned
Filed:	February 12, 2008
For:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

AMENDMENTS TO THE CLAIMS OF THE INTERNATIONAL APPLICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)) begin on page 2 of this communication.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

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

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

a smart card 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.

5. A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised.

9. A method according to any one of claims 6, 7 and 8 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.

10. A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader receiving the biometric signature;

means for defining, dependent upon the received card information, a memory location in a local memory external to the card;

means for determining if the defined memory location is unoccupied; and

means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

12. A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Amended Sheet
IPEA/AU

13. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature;

code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

code for determining if the defined memory location is unoccupied; and

code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

18. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature, if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Attorney Docket No. **12838/5**
Client Reference No. **729727US**

[UNEXECUTED] DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 C.F.R. §1.63)

As a below named inventor, I hereby declare:

My residence, mailing address, and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor or an original, first and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled:

IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

the specification of which (check one)

☒ is attached hereto.

☐ was filed on ______ as United States Application No. ______
and was amended on ______ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge my duty to disclose to the United States Patent and Trademark Office all information that I know to be material to patentability as defined in 37 C.F.R. §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or (f), or §365(b) of any foreign application(s) for patent or inventor's or plant breeder's rights certificate(s), or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's or plant breeder's rights certificate(s) or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application:			Priority Not Claimed
2005904375 (Number)	Australia (Country)	08/12/2005 (Filing Date, MM/DD/YYYY)	☐
(Number)	(Country)	(Filing Date, MM/DD/YYYY)	☐

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)

I hereby claim the benefit under 35 U.S.C. §120 of any United States applications(s), or §365(c) of any PCT International Application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/AU2006/001136 (Application Serial No.)	08/10/2006 (Filing Date, MM/DD/YYYY)	Pending (Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor
BURKE, Christopher John

Sole inventor's signature
Date

Residence (City, State/Foreign Country)
Ramsgate, New South Wales, 2217 Australia

Citizenship
Australia

Mailing Address
48 Margate Street, Ramsgate, New South Wales, 2217 Australia

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on February 12, 2008.

Robert D. Summers, Jr., Reg. No. 57,844

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: Not Yet Assigned

Filed: Herewith

For: IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Not Yet Assigned

Group Art Unit: Not Yet Assigned

Confirmation No.: Not Yet Assigne

INFORMATION DISCLOSURE STATEMENT

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and §§1.97-1.98, and more particularly in accordance with 37 C.F.R. §1.97(b), Applicant hereby cites the following references:

U.S. PATENT DOCUMENT

Document No.	Date	Patentee
6,796,492 B1	09/28/2004	Gatto
5,457,747	10/10/1995	Drexler et al.

FOREIGN PATENT DOCUMENTS		
DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY
CA 2 412 403 A1	05/20/2003	PCT
WO 03/036861 A1	05/01/2003	Canada

OTHER ART

International Search Report dated October 20, 2006.
International Preliminary Report on Patentability dated November 19, 2007.

Applicant is enclosing Form PTO-1449 (one sheet), along with copies of cited references A3-A6, which are required under 37 C.F.R. §1.98(a)(2). As the listed references are in English, no further commentary is believed to be necessary, 37 C.F.R §1.98(a)(3). The relevance of the references is noted in the

Applicant's International Search Report dated October 20, 2006 and International Preliminary Report on Patentability dated November 19, 2007. Applicant respectfully requests the Examiner's consideration of the above references and entry thereof into the record of this application.

By submitting this Statement, Applicant is attempting to fully comply with the duty of candor and good faith mandated by 37 C.F.R. §1.56. As such, this Statement is not intended to constitute an admission that the enclosed references, or other information referred to therein, constitute "prior art" or is otherwise "material to patentability," as that phrase is defined in 37 C.F.R. §1.56(a).

Applicant has calculated no fee to be due upon filing this Statement. However, the Director is authorized to charge any fee deficiency associated with the filing of this Statement to a deposit account, as authorized in the accompanying Transmittal.

Respectfully submitted,

Robert D. Summers, Jr. (Reg. No. 57,844)

FORM PTO-1449	SERIAL NO. Not Yet Assigned	CASE NO. **12838/5**
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT	FILING DATE Herewith	GROUP ART UNIT Not Yet Assigned
	APPLICANT: **BURKE, Christopher John**	

REFERENCE DESIGNATION **U.S. PATENT DOCUMENTS**

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
	A1	6,796,492 B1	09/28/2004	Gatto		
	A2	5,457,747	10/10/1995	Drexler et al.		

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES OR NO
	A3	CA 2 412 403 A1	05/20/2003	Canada		n/a
	A4	WO 03/036861 A1	05/01/2003	PCT		n/a

EXAMINER INITIAL	**OTHER ART – NON PATENT LITERATURE DOCUMENTS** (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	
	A5	International Search Report dated October 20, 2006.
	A6	International Preliminary Report on Patentability dated November 19, 2007.

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 412 403 (13) A1

(40) 20.05.2003
(43) 20.05.2003

(12)

(21) 2 412 403

(22) 20.11.2002

(51) Int. Cl.^{7}: G06K 9/62, A61B 5/117, H04L 9/32

(30) 2,363,372 CA 20.11.2001

(71)
TAYLOR, WAYNE,
8 Tsawwassen Beach Rd., DELTA, B1 (CA).

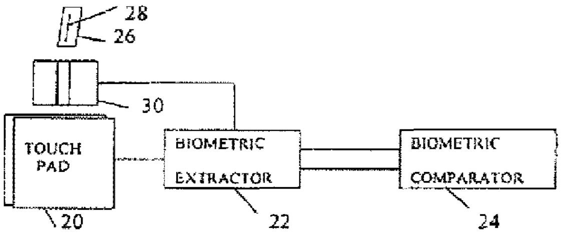
(72)
TAYLOR, WAYNE (CA).

(74)
VERMETTE & CO.

(54) SYSTEME POUR VERIFICATION D'IDENTITE
(54) SYSTEM FOR IDENTITY VERIFICATION

(57)

A method of verifying identity which includes recording coordinates of a reference signature which include two dimensional space coordinates x and y exerted by a writer's writing instrument on a recording medium. The method measures and records an indicium, which identifies a reference biometric within the reference signature having a selected characteristic. Next the reference biometric and the indicium are placed on a portable, readable substrate. The coordinates of an unknown signature which include two dimensional space coordinates x and y covered by a writer's writing instrument are also recorded. The method further includes reading and storing the indicium 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.



Office de la Propriété Intellectuelle du Canada

Un organisme d'Industrie Canada

Canadian Intellectual Property Office

An agency of Industry Canada

CA 2412403 A1 2003/05/20

(21) 2 412 403

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2002/11/20

(41) Mise à la disp. pub./Open to Public Insp.: 2003/05/20

(30) Priorité/Priority: 2001/11/20 (2,363,372) CA

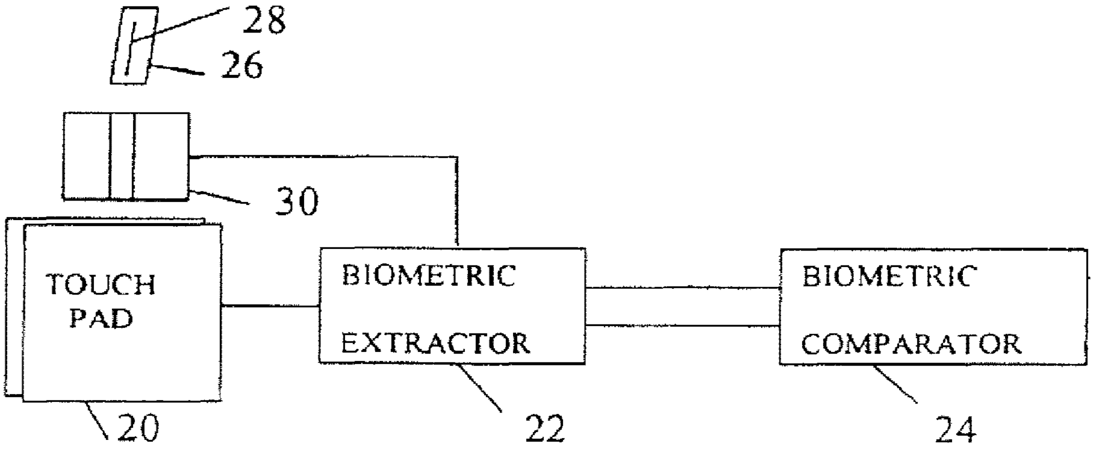
(51) Cl.Int.^{7}/Int.Cl.^{7} G06K 9/62, A61B 5/117, H04L 9/32

(71) Demandeur/Applicant:
TAYLOR, WAYNE, CA

(72) Inventeur/Inventor:
TAYLOR, WAYNE, CA

(74) Agent: VERMETTE & CO.

(54) Titre : SYSTEME POUR VERIFICATION D'IDENTITE
(54) Title: SYSTEM FOR IDENTITY VERIFICATION



(57) Abrégé/Abstract:
A method of verifying identity which includes recording coordinates of a reference signature which include two dimensional space coordinates x and y exerted by a writer's writing instrument on a recording medium. The method measures and records an indicium, which identifies a reference biometric within the reference signature having a selected characteristic. Next the reference biometric and the indicium are placed on a portable, readable substrate. The coordinates of an unknown signature which include two dimensional space coordinates x and y covered by a writer's writing instrument are also recorded. The method further includes reading and storing the indicium 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.

Canada http://opic.gc.ca · Ottawa-Hull K1A 0C9 · http://cipo.gc.ca OPIC CIPO

OPIC · CIPO 191

ABSTRACT

A method of verifying identity which includes recording coordinates of a reference signature which include two dimensional space coordinates x and y exerted by a writer's writing instrument on a recording medium. The method measures and records an indicium, which identifies a reference biometric within the reference signature having a selected characteristic. Next the reference biometric and the indicium are placed on a portable, readable substrate. The coordinates of an unknown signature which include two dimensional space coordinates x and y covered by a writer's writing instrument are also recorded. The method further includes reading and storing the indicium 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.

SYSTEM FOR IDENTITY VERIFICATION

Field

The present invention relates to a method and apparatus for verifying the identity of a person using a biometric, such as a signature or fingerprint.

Background

In credit card transactions, a major security problem exists whenever credit card information is transmitted over the Internet or telephone lines. In addition, because of the frequency with which credit cards, passports, and other personal documents, are lost and stolen, there exists a need to correctly, quickly and reliably verify the identity of the bearers of these documents.

In a typical credit card transaction, as seen in Fig. 1, a merchant **10** transmits a credit card number, the expiry date and a purchase order over the Internet or telephone lines **12** to a verification agent **14**. The agent **14** receiving this information accesses the cardholder's credit information and after comparing the latter to the purchase order amount, either accepts or rejects the transaction. If the transaction is accepted, an approval code is transmitted back to the merchant 10 via telephone line 12. Even if the transaction is accepted there is a risk that the card is stolen and is being used fraudulently. Accordingly, there is a need to be able to quickly, accurately and securely identify the bearer of the card.

Biometrics can be used to accurately verify identity, however, biometric information sent over the Internet or telephone lines can still be intercepted and subsequently utilized for fraudulent transactions.

Various approaches have been developed to identify persons by biometrics, including unique gestures such as handwriting. Such speech and handwriting recognition systems perform recognition of something that moves, leaving a "trajectory" in space and time. Typical speech recognition systems match transformed speech against a stored representation. Most speech recognition systems use some form of spectral representation, such as spectral templates or Hidden Markov Models (HMMs).

Handwriting can be analyzed in real time or after it has been formed. "Real time" or dynamic recognition systems identify handwriting as a user writes, identifying such things as number of strokes, the ordering of strokes and the direction and velocity profile of each stroke. "Real time" systems are also interactive, allowing users to correct recognition errors, adapt to the system, or see the immediate results of an editing command. Most on-line tablets capture writing as a sequence of coordinate points.

Handwriting recognition is complicated in part, because there are many different ways of generating the same character. For example, the four lines of the letter E can be drawn in any order. Handwriting tablets must also take into account character blending and merging, which is similar to the continuous speech problem. In other words, blending and merging make it difficult for a recognition system to determine where one character ends and the next one begins (or in the case of speech recognition systems, where one word ends and the next one begins). In addition, different characters can look quite similar and are, therefore, difficult to distinguish. Thus, prior to performing the character recognition, handwriting tablets pre-process the characters. Preprocessing typically involves properly spacing the characters and filtering out noise from the tablet. The more complicated processing occurs during actual character recognition.

Some character recognition processes, using binary decision trees, prune possible characters by identifying features. Normally simple features are identified first, such as searching for the dots above the letters "i" and "j". Features based on both static and dynamic features can be used for character recognition. Other character recognition processes involve the creation of zones, which define the directions a pen point can travel (usually eight), and define each character in terms of a set of zones. Look-up tables or dictionaries can be used to classify or identify the characters based on their features or sets of zones.

Another character recognition scheme relies on signal processing, in which curves from unknown forms are matched against prototype characters. They are matched as functions of time or as Fourier coefficients. To reduce errors, elastic matching schemes (stretching and bending drawn curves) may be used. However, these methods are computationally intensive and, therefore, tend to be slow and expensive.

Most handwriting examination tablets reveal that recognition of dynamic features of characters is possible, as in speech. However, for the reasons discussed above, it is easier to recognize isolated characters than strings of characters. Most systems lag recognition by about a second, and recognition rates are not very high. Reported rates of 95% are achieved only for very carefully formed writing.

For each of the types of recognition systems discussed above, a sample input (i.e. a voice or signature sample) must be processed and compared with a stored reference gesture in order to verify the identity of the subject. Normally, the reference gestures are located on a remote server and accessed by telephone lines or the Internet. The sample input must be sent to the remote server where it is compared to the reference gesture. Such a procedure is obviously exposed to the risk of security breaches. Furthermore, there is a cost associated with the maintenance of a remote server, and processing is delayed by the need to access the server. Accordingly, it is an object of the present invention to provide a quick and secure on-site method of identification, which is accurate and cost effective.

SUMMARY OF THE INVENTION

According to the present invention there is provided a method, and an apparatus for carrying out the method, for verifying a subject's identity using signatures or other biometrics. The first step of the method comprises recording a reference signature. The reference signature may be recorded by, for example, measuring two-dimensional space coordinates x and y exerted by a writer's writing instrument on a recording medium.

An indicium is selected from the coordinates, which identifies a specific portion (the reference biometric) of the reference signature, having a selected characteristic, that will be used for comparison with an unknown signature. The reference biometric and the indicium are then placed on a portable, readable substrate, such as the magnetic strip on a credit card.

The indicium of the reference signature is read from the readable substrate and the coordinates of an unknown signature are collected. The indicium is used to locate the portion (the extracted biometric) of the unknown signature that corresponds to the reference biometric. Once identified, the extracted biometric is compared to the reference biometric to determine if they match within predetermined threshold criteria.

If the reference and extracted biometrics match, the identity of the provider of the unknown signature is positively established as being the same as that of the provider of the reference signature (or in other words, the bearer of the credit card). If the reference and extracted biometrics do not match, or if no portion of the unknown signature matches the characteristics of the indicium, the identity of the provider of the unknown signature is not verified.

The foregoing steps are done on-site, without the need to access a server or to send information over telephone lines or the Internet.

Advantageously, a second indicium may be stored on the portable, readable substrate and used in the event that no identifiable portion of the unknown signature corresponds to the first indicium, or the results of the first comparison using the first indicium indicate there is no match. In the preferred embodiment the portable, readable substrate is in the form of a magnetic strip, however, it will be appreciated by those skilled in the art that it may take any of a number of alternative forms.

The present invention additionally relates to an apparatus for implementing the above method.

The coordinates of the reference and unknown signatures that are recorded and measured may additionally include time, t, and force, z, among others.

It is obvious to anyone skilled in the art that the present invention can be adapted to verify identity by applying the method of the present invention to reference and unknown samples of voice, fingerprints, or other biometrics.

BRIEF DESCRIPTION OF THE DRAWINGS

Further features and advantages will be apparent from the following detailed description, given by way of example, of a preferred embodiment taken in conjunction with the accompanying drawings, wherein:

Fig. 1 is a schematic diagram of a typical credit card transaction;

Fig. 2 is a schematic diagram of the identification scheme;

Fig. 3 is a diagram of a handwritten letter "a" showing points A and B of zero velocity; and

Fig. 4 is a diagram of a handwritten letter "a" showing entry vector C and exit vector D of a point of zero velocity.

DETAILED DESCRIPTION WITH REFERENCE TO THE DRAWINGS

Prior to evaluating an unknown signature, a reference signature must first be recorded and evaluated. The reference signature may be evaluated based on both local features and global features. Local features are those that occur within a localized region of a signature, for example, local maxima and minima, loops, points of intersection, points of zero velocity, etc. Global features are those that occur throughout the signature as a whole, for example, total signature time, average velocity of signature, length-to width ratio, etc.

If we assign the values x, y, z and t such that x is the horizontal displacement, y is the vertical displacement, z is the pressure, and t is time, then individual points of a signature can be represented by (x, y, z, t). One can normalize the values of x, y, and z in order to compensate for variations in signature sizes and recording device sizes.

Next, a selected biometric feature, in this case a local maximum, and a series of points on either side of that feature are recorded for comparison purposes. Also recorded is an indicium, which identifies the location of the local maximum, or other selected biometric feature. For example, the indicium may be the number of local maxima or points of zero velocity preceding the selected local maximum. The signatures of different individuals vary greatly and, therefore, depending on the nature of the reference signature some indicia may be more reliable than others. Therefore, it may be advisable to first test one indicium to see if it effectively identifies the selected local maximum. If not, another indicium can be chosen.

Signatures are not written in precisely the same way every time. Therefore, a given indicium may not correctly identify the selected local maximum in every instance. Accordingly, it may be advisable to use two or more indicia in parallel or to use a back-up indicium that is used in the event the first one fails.

A reference biometric, comprising the selected local maximum, which is chosen from within the reference signature, and coordinates x, y, z, and time, t, over a given range on either side of the selected local maximum are encrypted and recorded on a portable, readable substrate such as the magnetic strip on the back of a credit or identity card. The indicium, which will be used to locate the corresponding local maximum within the unknown signature, is also recorded and encrypted on the magnetic strip.

When the identity of an unknown user is being verified, the card is swiped through a card reader and the indicium and reference biometric are extracted and stored locally in memory. Next the user signs his name (the unknown signature) on a touchpad, which records the coordinates of the unknown signature so they can be stored locally. Suitable touchpads have been developed by DSI Datotech Systems Inc. of Vancouver, British Columbia. The unknown signature is first normalized to correspond with the scale of the reference signature. By reference to the indicium, the extracted biometric is identified and extracted from within the unknown signature. The extracted biometric comprises a range of values of x, y, z, and t, corresponding to the reference biometric, and falling within a range determined by the indicium. The coordinates of the extracted biometric from the unknown signature are compared with those of the reference biometric. If the difference between the y values of the extracted biometric and the y values of the reference biometric are within a threshold value, then the x, z and t values will also be compared to determine if they fall within predetermined thresholds. If the x, y, z and t values all fall within the allowable thresholds, the extracted biometric and the reference biometric, and therefore the unknown signature and the reference signature, are matched. However, if the x, y, z and/or t values do not fall within the allowable thresholds, then there is no match. In such instances a new indicium and/or biometric feature may be selected and the process repeated. Alternatively, for increased reliability, comparison of a global biometric, such as velocity, may also be made.

Referring to Fig. 2, the identification verification system of the present invention consists of a credit card or identity card **26**, on the back of which is a magnetic strip **28** containing a reference biometric and indicium. The credit card **26** is swiped through a first input device, in this case a credit card swiper unit **30**.

Gesture input device **20**, which can be a touch pad, receives the unknown signature and extracts position, velocity, acceleration and force information from the unknown signature. The gesture input device **20** and the card swiper unit **30** are connected to the biometric extractor **22**. Rather than having to store the large amount of information that would be represented by the average signature, the unknown signature is analyzed and only a small portion, the extracted biometric, (which is identified by the indicium, received from the card swiper **30**) is extracted by the biometric extractor **22**.

Although not shown in **Figure 2**, the card swiper unit **30** may also be coupled to the biometric comparator **24** so that the reference biometric may be sent directly rather than passing through the biometric extractor **22**.

The extracted biometric of the unknown signature is transmitted to the biometric comparator **24**, which also receives the reference biometric that is stored on a magnetic strip **28** on the back of a credit card or identity card **26**, which has been swiped through a credit card swiper unit **30**. Biometric comparator **24** compares the extracted biometric with the reference biometric from the card **26**. If the comparison by the biometric comparator **24** results in a match, then the person providing the unknown signature is the same person that provided the reference biometric. The accuracy of the technique is not 100 % so it may be prudent to use one or more additional biometrics or portions of a signature for comparison in parallel to determine, with an adequate level of confidence, whether there is a match. Alternatively, the identity verification procedure can be repeated.

The biometric extractor **22** and biometric comparator **24** may be incorporated into a CPU (not shown) and the results displayed on a monitor (not shown).

Any one of several conventional statistical analyses can be used determine whether there is a match between the extracted biometric and the reference biometric, such as a calculation of the average of the square of the differences between the coordinates of the extracted biometric and the reference biometric.

An alternative method of comparing reference and extracted biometrics comprises a vector analysis surrounding points of zero velocity. In a typical signature, there are likely a plurality of points where the velocity of the pen is zero. For example, referring to Figure 3, points A and B of the letter "a" will be points of zero velocity. Referring to Figure 4, point A will have two position vectors surrounding that point, a vector C entering the point A and a vector D exiting from the point A. Therefore, using these three pieces of data, a given point where the pen velocity is zero will have (x_1, y_1, z_1) indicating the point of zero velocity, (x_2, y_2, z_2) indicating the entry vector, and (x_3, y_3, z_3) indicating the exit vector. Therefore, a given point of zero velocity, identified by indicia as discussed above, can be used as a reference biometric to verify the identity of the person providing an unknown signature, by comparing the point of zero velocity, and the associated entry and exit vectors with the corresponding point of zero velocity and vectors of a reference signature.

Accordingly, while this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to this description. It is therefore contemplated that the appended claims will cover any such modifications or embodiments as fall within the true scope of the invention.

WE CLAIM:

1. A method for verifying identity comprising:

(a) recording in a machine readable format a reference signature of an individual;

(b) identifying a reference biometric within said reference signature, said reference biometric having a selected characteristic;

(c) identifying an indicium, wherein said indicium identifies said reference biometric within said reference signature;

(d) placing said reference biometric and said indicium on a portable machine readable substrate;

(e) inputting said indicium and said reference biometric from said substrate into a computer;

(f) inputting an unknown signature into said computer;

(g) using said indicium to identify an extracted biometric within said unknown signature; and

(h) comparing said extracted biometric to the reference biometric to determine if they match within predetermined threshold criteria;

wherein steps (e) to (h) inclusive are performed on-site.

2. The method of claim 1, wherein said reference signature and said unknown signature are handwritten signatures.

3. The method of claim 1, wherein said reference signature and said unknown biometric are fingerprints.

4. The method of claim 2, wherein two-dimensional space coordinates x and y, a force coordinate z, and a time coordinate t of said reference signature and said unknown signature are recorded and compared.

5. A method according to claim 2, wherein pressure sensitive pads are used to record said reference and unknown signatures.

6. A method according to claim 1, wherein said portable, machine readable substrate is a magnetic strip.

7. A method according to claim 6, wherein said magnetic strip is on a credit card.

8. A method according to claim 1, wherein a second indicium is identified and stored on said portable machine readable substrate.

9. A method according to claim 8, wherein said second indicium identifies said reference biometric within said reference signature.

10. A method according to claim 8, wherein said second indicium identifies a second reference biometric within said reference signature.

11. A method according to claim 8, wherein said second indicium is used to locate said extracted biometric in said unknown signature in the event said extracted biometric cannot be located using said first indicium.

12. A method according to claim 8, wherein said second indicium is used to locate said extracted biometric in the event that said comparison of said reference biometric and said extracted biometric indicates no match.

13. A method according to claim 1, wherein said unknown signature is normalized prior to identification of said extracted biometric.

14. An apparatus for verifying indentity comprising:

(a) a portable machine readable substrate on which is recorded a reference biometric of an individual and an indicium, wherein said indicium identifies said reference biometric within a reference signature;

(b) a first input device operative to read said reference biometric and said indicium from said machine readable substrate;

(c) a biometric input device, operative to receive an unknown signature;

(d) a biometric extraction unit coupled to said first input device and said biometric input device, said biometric extraction unit operative to identify and extract an extracted biometric within said unknown signature that is located by said indicium; and

(e) a biometric comparator coupled to said biometric extraction unit, said biometric comparator operative to receive said extracted biometric and said reference biometric, said biometric comparator additionally operative to compare said extracted biometric and said reference biometric to determine if they match within predetermined threshold criteria.

15. The apparatus according to claim 14, wherein said portable machine readable substrate is a magnetic strip.

16. The apparatus according to claim 14, wherein said magnetic strip is on a credit card.

17. The apparatus according to claim 14, wherein said reference and unknown signatures are fingerprints.

18. The apparatus according to claim 14, wherein said biometric input device is a pressure sensitive pad.

19. The apparatus according to claim 14, wherein two-dimensional space coordinates x and y, a force coordinate z, and a time coordinate t of said reference biometric are recorded on said portable machine readable substrate.

20. The apparatus according to claim 14, wherein said reference signature and said unknown signature are handwritten signatures.

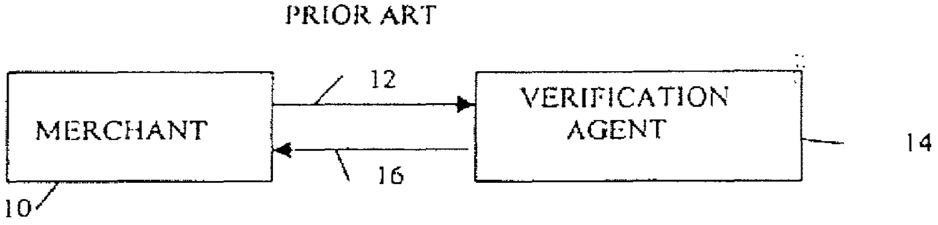

PRIOR ART
MERCHANT
VERIFICATION AGENT
12
16
10
14

Fig. 1

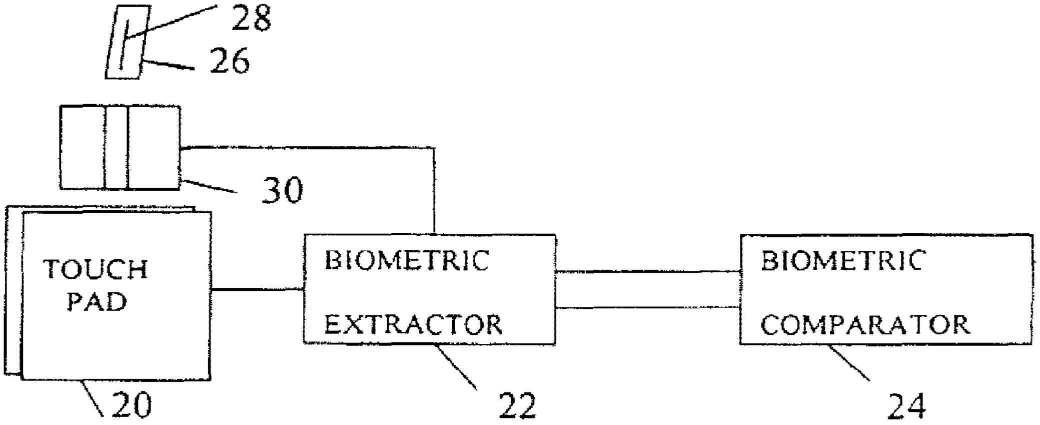

28
26
30
TOUCH PAD
BIOMETRIC EXTRACTOR
BIOMETRIC COMPARATOR
20
22
24

Fig. 2

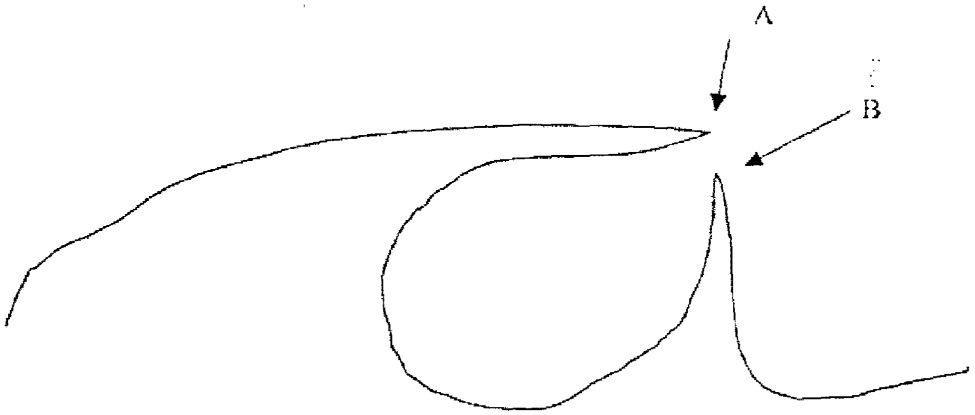


Fig. 3

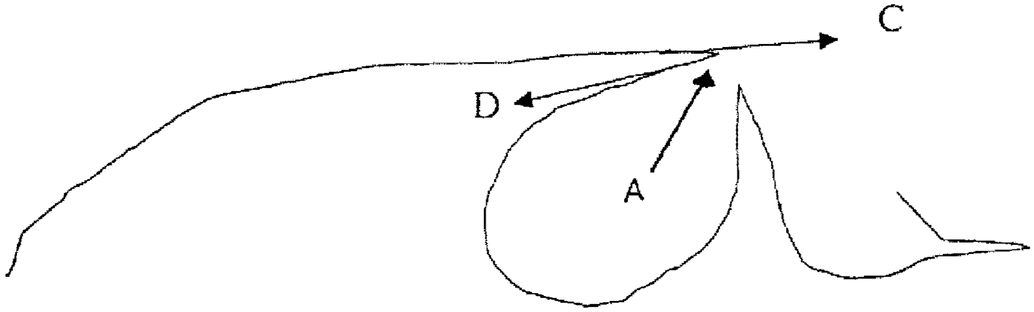


Fig. 4

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on February 12, 2008.

Robert D. Summers, Jr., Reg. No. 57,844

Our Case No. 12838/5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	CHRISTOPHER J. BURKE
Appln. No.:	Not Yet Assigned
Filed:	February 12, 2008
For:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

PRELIMINARY AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Before examination of the above-identified application, please enter the following amendment:

Amendments to the Specification begin on page 2 of this communication.

Amendments to the Claims begin on page 3 of this communication.

Remarks begin on page 12 of this communication.

AMENDMENTS TO THE SPECIFICATION:

Please insert before the first paragraph of the application:

This application is the National Stage of International Application No. PCT/AU2006/001136, filed August 10, 2006, which claims the benefit of priority to Australian Patent Application No. 2005904375, filed on August 12, 2005. All of the foregoing applications are hereby incorporated herein in their entirety in this application.

AMENDMENTS TO THE CLAIMS:

The listing of Claims will replace all prior versions and listings of the Claims in the application:

1. (Original) A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. (Original) A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. (Original) A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

4. (Original) A method according to claim 3, wherein the card device is one of:

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

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

a smart card 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.

5. (Original) A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. (Original) A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. (Original) A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and outputting at least some of the information input from the keypad.

8. (Currently Amended) A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not ~~authorised~~ authorized.

9. (Currently Amended) A method according to ~~any one of claims~~ claim 6, ~~7 and 8~~ 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.

10. (Original) A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. (Currently Amended) A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader for receiving the biometric signature;

means for defining, dependent upon the received card information, a memory location in a local memory external to the card;

means for determining if the defined memory location is unoccupied; and

means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

12. (Original) A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

13. (Original) A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. (Original) A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. (Original) A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in the verification station.

16. (Original) A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. (Original) A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature;

code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

code for determining if the defined memory location is unoccupied; and

code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

18. (Original) A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

19. (New) A method according to claim 7, 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.

20. (New) A method according to claim 8, 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.

REMARKS:

Claims 8, 9 and 11 have been amended and Claims 19 and 20 have been added. The amendments to the claims are shown with ~~strikethrough~~ for deleted matter and underlines for added matter. The claim amendments were made to conform to the United States practice and are believed to include no new matter.

Applicants respectfully submit that all of the pending claims are in condition for allowance. If for any reason the Examiner is unable to allow the application in the next Office Action and believes that a telephone interview would be helpful to resolve any remaining issues, he is respectfully requested to contact the undersigned.

Respectfully submitted,

Robert D. Summers Jr. (Reg. No. 57,844)

February 12, 2008
Date
BRINKS HOFER GILSON & LIONE
P.O. Box 10395
Chicago, IL 60610
(312) 321-4200

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 May 2003 (01.05.2003)

PCT

(10) International Publication Number
WO 03/036861 A1

(51) International Patent Classification[7]: H04L 9/14

(21) International Application Number: PCT/US02/16879

(22) International Filing Date: 28 May 2002 (28.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/865,638	25 May 2001 (25.05.2001)	US
60/299,226	19 June 2001 (19.06.2001)	US
60/308,010	26 July 2001 (26.07.2001)	US
60/317,866	10 September 2001 (10.09.2001)	US
60/326,607	1 October 2001 (01.10.2001)	US
60/340,010	6 December 2001 (06.12.2001)	US

(71) Applicant and
(72) Inventor: **BLACK, Gerald, R.** [US/US]; 30590 Southfield Rd. #160, Southfield, MI 48076 (US).

(74) Agent: **BLACK, Gerald, R.**; 30590 Southfield Road, #160, Southfield, MI 48076 (US).

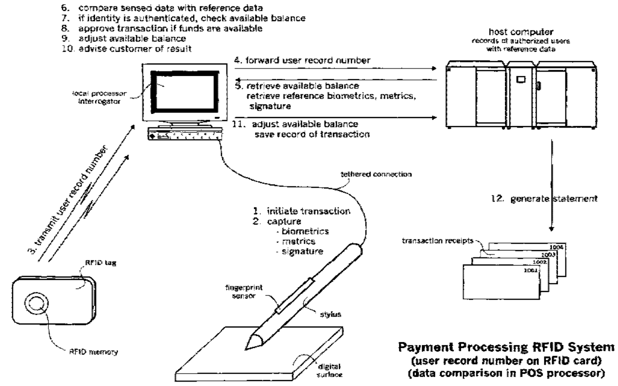
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY ACCESS SYSTEM


6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance
10. advise customer of result
4. forward user record number
5. retrieve available balance
retrieve reference biometrics, metrics, signature
11. adjust available balance
save record of transaction
host computer
records of authorized users with reference data
local processor interrogator
3. transmit user record number
tethered connection
12. generate statement
1. initiate transaction
2. capture
- biometrics
- metrics
- signature
transaction receipts
1004
1003
1002
1001
RFID tag
fingerprint sensor
stylus
RFID memory
digital surface

Payment Processing RFID System
(user record number on RFID card)
(data comparison in POS processor)

(57) **Abstract:** This identity authentication system is used in commercial transactions at a point-of-sale terminal. The system comprises a device for capturing a customer signature (signature pad or a smart pen), a sensor for capturing a biometric property of the customer during the transaction, a local processor, a wireless device carried by the customer, a device reader positioned at the point-of-sale terminal, and a host computer. The customer registers advising the system of a customer account that is to be used for payment. The customer also submits an electronic signature (written script of name) and a digital signature for reference purposes - a fingerprint. The customer is then issued a wireless device, the wireless device having memory. The memory may be an ID card, a credit card, a smart card, a transponder, a barcode, or a combination of these memories. An identifying device reader (such as a card reader, an interrogator, a scanner) is located at the point-of-sale terminal that is compatible with the wireless device. Thereafter, when the customer uses a stylus to submit written data - an electronic signature is generated. Similarly, a sensor in the stylus captures data that is used to generate a digital signature. A reference print is then accessed through the memory in the wireless device carried by the customer. The digital and electronic signatures are then compared against the reference data to authentic identity.

SECURITY ACCESS SYSTEM

FIELD OF THE INVENTION

The invention relates generally to various systems for verifying the identification of a person, and more particularly, where the person carries a wireless device for use at point-of-sale terminals, the wireless device having a memory in for example, an ID card, a credit card, a smart card, a transponder, a barcode, or a combination of these memories.

BACKGROUND OF THE INVENTION

Many identification systems are known in the art. In some cases, a photograph of a subject or his fingerprint pattern is affixed to an identification card. In other approaches, various methods are employed for storing image or password information in a magnetic stripe or in an optically encoded image or pattern, which is physically part of the identification card. Still other approaches utilize a "smart card" having its own semiconductor memory capability for information storage.

> U.S. Patent No. 6,175,922 (Wang) discloses an electronic transaction system for completing a transaction request at a point-of-sale terminal using a portable electronic authorization device carried by a user. The device first receives digital data representing the transaction request. The electronic authorization device provides information regarding an ability to approve the transaction request. When the transaction is approved, the electronic authorization device receives additional data representing the electronic service authorization token.
>
> U.S. Patent No. 6,140,939 (Flick) discloses a biometric security system for automobiles. The control system includes a controller for learning a unique biometric characteristic of an individual to define a learned individual capable of causing performance of a function associated with the vehicle. The vehicle function control system includes a biometric characteristic sensor, and a

controller at the vehicle for controlling a vehicle function responsive to the biometric characteristic sensor.

U.S. Patent No. 5,857,152 (Everett) discloses an electronic system for toll payment. The system identifies an electronic purse and effects value transfer over a communication system without the need for the vehicle to stop. The system provides for toll payment by use of a communication device and an electronic purse coupled to the device. The remote communication system communicates with mobile devices to effect toll payments by exchanging cryptographically secure messages.

U.S. Patent No. 5,706,349 (Aditham et al.) discloses a system for authenticating remote users in a distributed environment. A token is initially issued to a remote user once a security mechanism determines that the remote user is who he claims to be. Prior to access to the a connection between a remote user and an application server, the system verifies that a token associated with a connection request was issued by the security mechanism.

U.S. Patent No. 6,202,055 (Houvener, et al.) discloses a system for processing a financial instrument. A customer at a identification terminal initially submits the instrument – perhaps a check. The checking account number is communicated to a remote database containing digital photographic images of authorized users of checking accounts. The remote database is searched and any photographic images associated with the checking account number are transmitted to the identification terminal. The images are displayed and compared to the physical appearance of the customer. The on-site employee then determines if at least one of the displayed digital matches the appearance of the person initiating the transaction.

U.S. Patent No. 5,903,225 (Schmitt, et al.) discloses an access control system with fingerprint sensor enrollment. The system includes a station for enrolling a person as authorized based upon the sensed fingerprint. The system also includes a wireless device that is carried by the authorized person, and an access controller for granting access to an authorized person. The wireless device cooperates with the enrolling station to store data for an authorized person based upon the sensed fingerprint. The authorized person bearing the wireless device is unobtrusively granted access by approaching the access location.

U.S. Patent No. 5,973,731 (Schwab) discloses an identification system that provides interactive communication of text and image information between a central server and multiple remote terminals. The central server maintains a separate, centralized database of data-compressed images of the subject individuals, and subsequently transmits the data-compressed images to local terminals, on demand, during the transactions. The image may include a copy of the authorized signature, which then is used by the transaction terminal to compare to a scanned image of the signature on the authorization slip.

While a written signature is still regarded as the preferred way for a person to convey approval and a legal commitment, there still remains a need to confirm absolutely that can assure that the customer is the person authorized to make a commitment.

What is needed is a system that will utilize wireless technology (primarily) in commercial transactions of any value that is acceptable to all parties - that captures a digital signature (which is the international standard of identification) at the same time that the electronic signature (the written text) is captured, the combined signature being irrefutable; a pen-based system that is both compatible with card-based systems and independent of such systems.

SUMMARY OF THE INVENTION

The system of the present invention addresses these needs. For purposes herein, a list of key terms are hereafter set forth to clarify the scope of the authenticated payment system of the present invention.

TRANSPONDER is a wireless device that is a receiver-transmitter. The transponder is part of a transponder system – the system also including an interrogator. The transponder is capable of accepting the challenge of the interrogator by transmitting an appropriate reply. The transponder receives and transmits data in a wireless manner, generally through low frequency radio waves. The transponder is generally an ID card, a keytag, a wireless phone, a pda, or some other device that can be carried by a customer in a purse, wallet, keychain, or pocket. The transponder may be active or passive. This definition expressly excludes any data transmission by means of swiping a card through or injecting a card into a conventional cardreader.

STYLUS refers to any device that is compatible with either the hand or finger of the user for purposes of making a marking on an essentially flat surface. The flat surface may be a digital surface or a piece of paper. While the drawings depict a conventional shape of a stylus, other shapes and designs are also included within the scope of the present invention such as any attachment or thimble-like device for a finger or any implement that can be held with a hand for such purpose. The stylus may or may not include an ink cartridge.

DYNAMIC REGISTRATION refers to a process where an existing customer can register for identity into a new system by participating in a conventional transaction. For example, if an electronic signature or digital signature is to be used for reference purposes, such signature is captured when the customer grasps the stylus and signs her name. The registration is seamless and essential invisible to the customer.

The authenticated payment system of the present invention comprises a wireless device carried by the customer, a device reader for accessing customer data through the wireless device, a device for generating an electronic signature, a sensor for capturing a digital signature during the course of the commercial transaction, a point-of-sale processor for processing electronic signature data and digital signature data from the device reader, and a host computer in digital communication with the point-of-sale processor.

The method for authenticating a payment of the present invention comprises a customer approaching a point-of-sale terminal with goods to be purchased, the customer generating an electronic signature as an expression of intent to commit to the commercial transaction, capturing a digital signature of the customer when the electronic signature is being generated, comparing the captured digital signature of the customer against a reference digital signature, and approving the transaction whenever a predetermined threshold for the authentication has been met and the customer has sufficient funds to cover the transaction.

A first preferred embodiment of the identity verification system of the present invention is for use in commercial transactions. The system comprises a host computer, an interrogation device, a transponder device, and a stylus.

The host computer has access to data that links the customer with the customer's payment account. The interrogator is linked to the host computer disposed at the point-of-sale terminal. The transponder is wireless and is carried by the customer, and transmits data to the interrogator upon request. The data transmitted pertains to the identity of the customer. The stylus is attached to the point-of-sale terminal and includes a sensor disposed in the stylus grip. The sensor captures a digital signature of the customer while the customer signs her name. Access to the customer's payment account is only enabled when the sensed digital signature matches a reference digital signature.

For use in commercial transactions at a point-of-sale terminal, a customer registers selecting a customer account that is to be used for payment. The customer also submits a digital signature for reference purposes – preferably, a fingerprint. The customer is then issued a transponder that links the customer to the customer account and to the reference digital signature. When the customer is at the point-of-sale terminal for making payment, an interrogator disposed at the point-of-sale terminal transmits a radio signal requesting identity verification. The wireless transponder submits data to the interrogator. Thereafter, when the customer uses a stylus to submit written data (such as a signature), a sensor in the stylus makes incidental capture of biometric data that enables the interrogator to confirm customer identity. Similarly, the system can be used to verify identity when the customer wants to cash a personal check.

Positioned at the center of the process is a stylus with any of a number of biometric or with one or more metric sensors, that enable an incidental capture of data relative to identity verification while the stylus is being used. The identity verification processes of the present invention can be used at point-of-sale terminals, in various controlled environments, to access a computer network, in applications involving pen-based computers and smart-pens, for e-commerce, conventional writing implements, and multi-purpose writing implements.

While the systems set forth herein are described in conjunction with point-of-sale terminals for purposes of illustration, it is understood that the principles set forth herein are all applicable to a broad range of other activities where a writing or signature are required or preferred, such as Internet and Intranet commerce, access control, government activities (voting, drivers' registration, receipt of government benefits) and for use in controlled environments (such as hospitals, and banks).

Various methods of generating a digital signature may be employed:

PCT Application No. PCT/US99/17900 entitled "Identification Confirmation System" filed on April 7, 1999; U.S. Patent Application 09/490,687, entitled "Writing Implement and Identity Verification Systems" filed on January 24, 2000;U.S. Patent Application 09/535,411, entitled "Method for Identity Verification" filed on March 20, 2000; and PCT Application No. PCT/US00/19652 entitled "Identity Authentication System and Method" filed July 18, 2000 by the applicant disclose the use of fingerprint sensors disposed in the barrel of a stylus used to generate an electronic signature as the preferred digital signature.

U.S. Patent No. 6,064,751 (Smithies) discloses a method of generating a digital signature by the use of various metric and biometric sensors disposed in the barrel of the stylus. A computer-based system captures and verifies an electronic handwritten signature. The system includes a stylus with a plurality of sensors that capture biometric properties of the user, and a database of signature templates storing verified signature information. At the time of signing, a digital signature is generated comprising certain features of the writer during the act of signing, such as the size, shape and relative positioning of the curves, loops, lines, dots, crosses and other features of the signature being inscribed, as well as the relative speed at which feature is being imparted. A captured composite digital signature of signature measurements are compared with a reference set of measurements stored to obtain a similarity score.

The interrogator is in digital communication with a host computer – the interrogator being disposed at a point-of-sale terminal. The wireless device is preferably a transponder. The stylus can be attached to a point-of-sale terminal, via a pen-based computer or a signature pad. A digital signature, such as a fingerprint, is captured during a registration process and stored in a file associated with the registrant or in the wireless device.

The customer registers advising the system of a customer account that is to be used for payment. The customer also submits an electronic signature (written script of name) and a digital signature for reference purposes – a fingerprint. The customer is then issued a wireless device, the wireless device having memory. The memory may be an ID card, a credit card, a smart card, a transponder, a barcode, or a combination of these memories. A identifying device reader (such as a card reader, an interrogator, a scanner) is located at the point-of-sale terminal that is compatible with the wireless device. Thereafter, when the customer uses a stylus to submit written data - an electronic signature is generated. Similarly, a sensor in the stylus captures data that is used to generate a digital signature. A reference print is then accessed through the memory in the wireless device carried by the customer. The digital and electronic signatures are then compared against the reference data to authentic identity.

The stylus includes one or more fingerprint sensor that captures an image of a finger of the customer when the stylus is grasped. While fingerprint sensors are used herein for purposes of illustration it is expressly understood that the principles of this invention are also applicable to sensing of DNA and other biotech properties - that involve cell capture or cell analysis sensors. During routine usage of the stylus, the sensor captures the data necessary to compare with the digital signature to determine identity verification.

The preferred embodiment of the authenticated commercial transaction system of the present invention is compatible with the following systems:

Fingerprint sensor in something other than stylus (card reader, point-of-sale counter, card)

- Stylus w/ fingerprint sensors attached to point-of-sale
  - Credit cards
  - Stored value, ATM, check cards
  - Reference print, Bank, and Account number in card, keytag, or wallet
  - Bank and Account number in card, keytag or wallet
  - Personal identifier in card, keytag, or wallet
- Smart-Pen w/ fingerprint sensors attached to point-of-sale
  - Credit cards
  - Stored value, ATM, check cards
  - Reference print, Bank, and Account number in card, keytag, or wallet
  - Bank and Account number in card, keytag or wallet
  - Personal identifier in card, keytag, or wallet
- Wireless Smart-Pen w/ fingerprint sensors carried by customer
  - Reference print, Bank, and Account number in smart-pen
  - Bank and Account number in smart-pen
  - Personal identifier in smart-pen

For a more complete understanding of the authenticated payment system of the present invention, reference is made to the following detailed description and accompanying drawings in which the presently preferred embodiments of the invention are shown by way of example. As the invention may be embodied in many forms without departing from spirit of essential characteristics thereof, it is expressly understood that the drawings are for purposes of illustration and description only, and are not intended as a definition of the limits of the invention. Throughout the description, like reference numbers refer to the same component throughout the several views.

DETAILED DESCRIPTION OF THE DRAWINGS

FIGURE 1A discloses a preferred embodiment of a payment processing RFID system of the present invention comprising a wireless device (RFID memory that includes a unique customer record number), a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for authenticating identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing customer records and transaction records, and for generating monthly statements);

FIGURE 1B discloses a second preferred embodiment of a payment processing RFID system of the present invention comprising a wireless device (RFID memory that reference biometric data, metric data, and signature data), a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for authenticating identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing transaction records, and for generating monthly statements);

FIGURE 1C discloses a third preferred embodiment of a payment processing system of the present invention comprising a stylus for capturing a biometric property during the signing process, a smart card reader, a smart card, the smart card memory including reference biometric data, metric data, and signature data), identity authentication based upon comparison of the captured customer data with the reference customer data occurring in the smart card memory), and a host computer (for storing transaction records);

FIGURE 1D discloses a fourth preferred embodiment of a payment processing RFID system of the present invention comprising a wireless device (RFID memory that includes a unique customer record number), a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for collecting data from the wireless device and the stylus), and a host computer (for authenticating identity based upon comparison of the captured customer data with the reference customer data, for storing customer records and transaction records, and for generating monthly statements);

FIGURE 2A discloses a preferred embodiment of a security RFID processing system of the present invention comprising a wireless device (RFID memory that includes a unique user record number), a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for authenticating user identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing security access codes and access requests);

FIGURE 2B discloses a second preferred embodiment of a security RFID processing system of the present invention comprising a wireless device (RFID memory that includes a user biometric data, user metric data, and user signature data, and a unique user record number), a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for authenticating user identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing security access codes and access requests);

FIGURE 3 discloses a preferred embodiment of a payment processing barcode system of the present invention comprising a wireless device (barcode memory that includes a unique customer record number), a stylus for capturing a biometric property during the signing process, a local processor-barcode reader (for authenticating identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing customer records and transaction records, and for generating monthly statements);

FIGURE 4 discloses a preferred embodiment of a system for processing a conventional payment for goods and service at a point-of-sale terminal, comprising a customer ID card (RFID memory that includes a unique customer record number), a user credit or debit card from which value is drawn to pay for goods or services, a stylus for capturing a biometric property during the signing process, a local processor-interrogator (for authenticating identity based upon comparison of the captured customer data with the reference customer data), and a host computer (for storing customer records and transaction records, and for generating monthly statements), the transaction being blocked if the ID card reference data does not match the biometric, metric, or signature data captured from the stylus;

FIGURE 5A discloses a simplified logic diagram for a preferred method for registering new users into the access (account, network data, physical) security system of the present invention;

FIGURE 5B discloses a simplified logic diagram for a preferred method for registering existing users into the access (account, network data, physical) security system of the present invention, the registration occurring dynamically as an on-site access request is being processed;

FIGURE 6A discloses a simplified logic diagram for a preferred method for enabling account, network data, or physical access involving lower security identity authentication, two streams of sensed data being compared to two streams of reference data, access being enabled if either stream of sensed data matches a corresponding stream of reference data;

FIGURE 6B discloses a simplified logic diagram for a preferred method for enabling account, network data, or physical access involving medium security identity authentication, one stream of sensed data being compared to a stream of reference data, access being enabled if the sensed data matches the reference data;

FIGURE 6C discloses a simplified logic diagram for a preferred method for enabling account, network data, or physical access involving higher security identity authentication, two streams of sensed data being compared against two streams of reference data, access being enabled if and only if each stream of sensed data matches its corresponding stream of reference data;

FIGURES 7A and 7C disclose a simplified logic diagram for a preferred method for the security system of the present invention, enabling access to network data to a remote user involving higher security identity authentication a network high security request, where an acceptance threshold is adjusted (see FIGURE 18A and 18B), two streams of data being captured and processed, access being enabled if and only if each stream of sensed data matches its corresponding stream of reference data;

FIGURES 7B and 7C disclose a simplified logic diagram for a preferred method for the security system of the present invention, enabling access to network data to a remote user involving higher security identity authentication a network high security request, where an acceptance threshold is adjusted (see FIGURE 18A and 18B), two streams of data being captured and processed, access being enabled if and only if each stream of sensed data matches its corresponding stream of reference data, data misinformation being provided to the user if identity authentication is not confirmed;

FIGURE 8 discloses a simplified logic diagram for another embodiment of the security system of the present invention, wherein the reference data is used for purposes of authenticating user identity for cashing a check;

FIGURE 9 discloses a simplified logic diagram for a preferred method for enabling access to a secure area, the user carrying a wireless device having RFID memory, one stream of sensed data being compared to a stream of reference data, access being enabled if the sensed data matches the reference data;

FIGURES 10A and 11A disclose a preferred embodiment of simplified RFID memory and simplified customer record of the host computer for the payment processing system of FIGURE 1A;

FIGURES 10BA and 11B disclose a preferred embodiment of simplified RFID memory and simplified customer record of the host computer for the payment processing system of FIGURE 1B;

FIGURE 12A discloses a preferred embodiment for the stylus of the security system of the present invention for providing images of any finger image that touches the grip area of the stylus, an ultrasonic sensor being positioned along the axis of the stylus, the sensor rotating to capture finger images (like sonar), providing a wrap-around sensor configuration for capturing fingerprint images;

FIGURE 12B discloses another preferred embodiment for the stylus of the security system of the present invention for providing images of any finger image that touches the grip area of the stylus, six elongated silicon chip sensors being mounted about the surface of the grip, providing a wrap-around sensor configuration for capturing fingerprint images;

FIGURES 13A and 13B disclose exploded views of other preferred embodiments of wrap-around fingerprint sensor configurations, providing a wrap-around sensor configuration for capturing fingerprint images;

FIGURES 14A and 14B disclose a simplified user record data and a list of security access sites for use in a financial institution;

FIGURES 15A and 15 B disclose a variation of a wireless stylus for use with the security access system of the present invention, the wireless stylus including a fingerprint sensor, a magnetic stripe, and a living hinge for opening and closing a pivotal flap where the magnetic stripe is positioned;

FIGURE 16A discloses a customer identification device for the security access system of the present invention, the customer identification device being a card, wherein the card includes is an active transponder;

FIGURE 16B discloses a customer identification device for the security access system of the present invention, the customer identification device being a card, wherein the card includes a magnetic stripe credit card;

FIGURE 16C discloses a customer identification device for the security access system of the present invention, the customer identification device being a card, wherein the card includes a barcode;

FIGURE 16D discloses a customer identification device for the security access system of the present invention, the customer identification device being a card with two memories, wherein one memory is the passive transponder and the second memory is the barcode;

FIGURE 16E discloses a customer identification device for the security access system of the present invention, the customer identification device being a card with three memories, wherein one memory is the magnetic stripe, the second memory is a passive transponder, and the third memory is the barcode;

FIGURE 16F discloses a customer identification device for the security access system of the present invention, the customer identification device being a card with two memories, wherein one memory is the magnetic stripe and the second memory is the barcode;

FIGURE 17 discloses still another preferred embodiment of the wireless device of the present invention, the wireless device being, commercial paper with RFID memory disposed therewithin, the memory enabling tracking of the commercial paper, and enabling identity authentication at transfer sites. For purposes of discussions herein, there are two types of RFID devices (1) a token that is issued to a party for use by that party; and (2) a token that is issued and can be readily and freely exchanged between parties (like currency). The latter may take the form of a plastic card, a paper note, or a coin.

FIGURE 18A discloses a simplified threshold graph for authenticating lower-risk commercial transactions; and FIGURE 18B discloses a simplified threshold graph for authenticating higher-risk commercial transactions.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, FIGURE 1A, 1B, and 1C disclose generally the security access system of the present invention. The authenticated commercial transaction system comprises a wireless device carried by the customer, a device reader for accessing customer data through the wireless device, a device for generating an electronic signature, a sensor for capturing a digital signature during the course of the commercial transaction, a point-of-sale processor for processing electronic signature data and digital signature data from the device reader, and a host computer in digital communication with the point-of-sale processor.

The preferred embodiment of the identity verification system of the present invention is for accessing account data, for accessing network data, and for physical access. The host computer has access to data that links the customer with the customer's payment account. The interrogator is linked to the host computer disposed at the point-of-sale terminal. The transponder is wireless and is carried by the customer, and transmits data to the interrogator upon request. The data transmitted from the transponder enables the system to make an initial customer identification. The stylus is attached to the point-of-sale terminal and includes a sensor disposed in the stylus grip. The sensor captures and generates a digital signature of the customer while the customer signs his name. Access to the customer's payment account is only enabled after identity has been verified – by matching the digital and/or electronic signatures with the reference data previously submitted by the customer.

In the two-step process of the identity verification process of the present invention, customer identity is initially made by data transmitted from the transponder to the interrogator. The second step involves the capture of data used to generate digital and electronic signatures. Only after the captured data is compared against the reference data, will the transaction be allowed to proceed.

The method for authenticating a commercial transaction of the present invention comprises a customer approaching a point-of-sale terminal with goods to be purchased, the customer generating an electronic signature as an expression of intent to commit to the commercial transaction, capturing a digital signature of the customer when the electronic signature is being generated, comparing the captured digital signature of the customer against a reference digital signature, and approving the transaction whenever a predetermined threshold for the authentication has been met and the customer has sufficient funds to cover the transaction.

This identity authentication system is used in commercial transactions at a point-of-sale terminal. The customer registers advising the system of a customer account that is to be used for payment. The customer also submits an electronic signature (written script of name) and a digital signature for reference purposes – a fingerprint. The customer is then issued a wireless device, the wireless device having memory. The memory may be an ID card, a credit card, a smart card, a transponder, a barcode, or a combination of these memories. A identifying device reader (such as a card reader, an interrogator, a scanner) is located at the point-of-sale terminal that is compatible with the wireless device. Thereafter, when the customer uses a stylus to submit written data - an electronic signature is generated. Similarly, a sensor in the stylus captures data that is used to generate a digital signature. A reference print is then accessed through the memory in the wireless device carried by the customer. The digital and electronic signatures are then compared against the reference data to authentic identity.

FIGURES 2A and 2B disclose simplified methods for registration for new and existing customers, respectively. For a new customer, the customer record must be created. For an existing customer, the customer record already exists. One primary advantage of having the reference data in the customer record (rather than the transponder) is that the amount of memory available reference signature store is not a primary concern. When the reference signature data is to be stored within the transponder, the amount of memory within the transponder may not be sufficient to store such data. For the existing customer, the customer record is already in existence but a confirmation check is needed to confirm that the customer has authorized access to the account.

The method overcomes the inconvenience of having to re-register all existing customers, Existing customers can use a "dynamic registration" during a routine transaction. Digital and electronic signatures are captured during a routine commercial transaction, using the stylus. Thereafter, during a commercial transaction, the sensed print is compared to the reference print as part of the identity verification process whenever the card is submitted through a cardreader. Similarly, if a transponder is used, perhaps to buy gasoline and other items in a convenience store affiliated with the gas station, the stylus captures the digital signature and uses it as a reference print.

For example in a branch office of a bank, the styluses of the present invention are placed at all tellers' windows, all ATMs, and all officers' desks. New customers are given a debit/check/ATM card upon filling out an application. The customer uses a stylus similar to the styluses at the tellers' windows. The customer's reference print is captured during registration, preferably within a branch office of the bank and digital and electronic signature data is encrypted is stored in the customer's bank record. Such cards can actually be issued and distributed to customers once registration is completed, much the same as hotels use to issue room keys upon registration – the cards are preprinted and certain data is loaded onto the card prior to issuance.

The stylus can be attached to a point-of-sale terminal, attached to a pen-based computer, or a signature pad. In addition, the stylus can be wireless, whereby the transponder is incorporated into the wireless stylus (see FIGURES 1B and 1C). Each stylus also includes one or more fingerprint sensors that capture an image of a finger of the customer when the stylus is grasped.

The transponder responds to a radio signal by emitting its own radio signal. Each transponder is tagged with a unique serial number. That serial number can be linked with a credit or debit account. A typical sale may require a matching of digital signatures; require a matching of electronic signatures, and require a matching of both digital signatures and electronic signatures. The customer selects goods and proceeds to a point-of-sale terminal. The point-of-sale terminal indicates that the transaction will be paid through a transponder. An interrogator disposed at the point-of-sale terminal collects data from the transponder. A light advises the customer that the payment has been accepted. Payment is made instantly from the customer's registered account. The interrogator emits a low-frequency transmission, generally via its antenna. The transponder is inactive until it's activated by the interrogator. When a transponder passes within range, the transponder is excited, causing the transponder to transmit its data in response to the inquiry. The interrogator submits the inquiry to the transponder and receives back data from the transponder.

In one preferred embodiment, the transponder has enhanced memory (akin to a smart card), in which case the encrypted reference fingerprint is stored within the transponder memory. Also, the memory may contain account number, balance – and customer data to be stored in the transponder memory. FIGURE 6A discloses the corresponding customer bank record. The comparison of the sensed print with the reference print for purposes of identity authentication preferably occurs in the transponder. One significant advantage to this system is that the transaction can be completed at the point-of-sale terminal with minimal access/input from the driver. Another advantage is that the driver and account data are updated after the transaction is completed

In another preferred embodiment, the transponder has limited memory (akin to a magnetic stripe). The writing device is a tethered stylus attached to the point-of-sale terminal and the digital and electronic signatures are stored in the customer record. The customer bank and account number are in the transponder. The reference signatures are in the customer record at the customer bank. The comparison of the sensed signatures with the reference signatures for purposes of identity authentication preferably occurs either in the driver (where the sensed print is transmitted) or in the point-of-sale terminal (where the reference print is transmitted). In a variation of this embodiment, the transponder has an index reference to the customer bank and account number. For increased security the index reference number in the account index and on the transponder change with each transaction. The reference print is in the customer record at the customer bank. One significant advantage is that since there is minimal information on the transponder device, if the transponder is lost or stolen it is of little use to thieves and hacks. While they can locate the customer's bank and account number (which they can learn from a personal check), they cannot gain access to such funds since the digital and/or electronic signatures don't match. Another advantage is that the transmission of data is through wired connections (more secure).

A passive transponder (does not include a power supply) carried by the customer on his/her person is disposed in a card carried in a wallet or on a keychain – it may need to be removed and swiped through a cardreader or a near an interrogator. An active transponder (includes a power supply) can also be pda, jewelry, glasses, clothing, or the like.

A transponder of choice is commercially available from AMSKAN of Mulgrave, Victoria in Australia - the InfraRed Datalink allows serial "through the windscreen' data transfer between a vehicle and the roadside in daylight with high reliability and is presently used for capturing information from vehicles as they re-fuel, re-load, or at highway speeds. The IRD is comprised of two main components, the interrogator and the wireless transponder. The interrogator is mounted either at the point-of-sale terminal. The size of the transponder is 130 x 80 x 50 mm.

Another transponder of choice is Miotec's mPollux – that is developed on a SIM card and its integrated security solutions offer a flexible and secure platform with a sufficient capacity for a wireless PKI system. The SIM platform is a FLASH microcontroller, which has a separate RISC processor for RSA operations. MioCOS operating system is compliant with both GSM and PKI standards. Furthermore, the integrated biometric functions enable, among other things, replacing the PIN code in an electronic ID card with fingerprint matching.

In still yet another preferred embodiment of the pen-based verification systems of the present invention, a transponder is used in a smart card. The smart is compatible with both contactless and contact transactions. Such a card is presently commercially available and known as a "Digital Pusan Card." The Digital Pusan Card is one of the first to combine contact and contactless smart card functionality on a single chip. Supporting a wide array of services, it combines credit, debit and prepaid card functions. Compatible with smart pagers the card is used within the existing Hanaro Transportation scheme. Cardholders can recharge their e-purses at reloading machines and at ATMs.

As well as proven and secure dual interface technology, operating in both contact and contactless mode. The card is loaded by either its contact or contactless interface. This allows many recharging possibilities including at bank terminals, bus stations or, with a PC and card reader, over the Internet - and this also permits electronic purchasing via the Internet.

The use of this transponder as a component of the pen-based verification system of the present invention enables the transponder to be compatible with both card-based and cardless systems. In the card-based system, the device is swiped through a cardreader at the point-of-sale terminal – and the customer signs her name using the fingerprint stylus. The reference fingerprint image is stored in the smart card/transponder device, which is also where the matching of the sensed print (from the pen) is compared with the reference fingerprint image. This embodiment enabling compatibility with both cardreaders and transponders also is key in enabling a transition to a cardless system.

The preferred embodiment of the security access system of the present invention is compatible with the following systems:

- Fingerprint sensor in something other than stylus (card reader, point-of-sale counter, card)
- Stylus w/ fingerprint sensors attached to point-of-sale
  - Credit cards
  - Stored value, ATM, check cards
  - Reference print, Bank, and Account number in card, keytag, or wallet
  - Bank and Account number in card, keytag or wallet
  - Personal identifier in card, keytag, or wallet
- Smart-Pen w/ fingerprint sensors attached to point-of-sale
  - Credit cards
  - Stored value, ATM, check cards
  - Reference print, Bank, and Account number in card, keytag, or wallet
  - Bank and Account number in card, keytag or wallet
  - Personal identifier in card, keytag, or wallet
- Wireless Smart-Pen w/ fingerprint sensors carried by customer
  - Reference print, Bank, and Account number in smart-pen

Bank and Account number in smart-pen
Personal identifier in smart-pen

When wireless devices are used, system security becomes even more of a concern, since an integral part of the system, in this instance the transponder, is not attached to the system, but rather is wireless and carried by a customer. The reference digital and electronic signature data is stored in both the transponder and the customer record. During a request for a point-of-sale transaction, a comparison of the reference data on the transponder is compared with the reference data in the customer record to determine if the transponder has been altered or replaced with a counterfeit transponder. This check need not be done each time but either randomly or in the event that the transaction involves a large value amount. There are other ways. When the reference print is stored inside a transponder that is carried by the customer, either of the following technologies may also be employed:

U.S. Patent No. 5,619,025 (Hickman, et al.) discloses a method for tamper-proof identification using photo refractive crystals. The method for document authentication exploits a temporally variable physical process to generate a reproducible effect that cannot be copied. A document such as a credit card is provided with a spot or stripe that incorporates at least one, and preferably a large plurality of photo refractive crystals arrayed in a random manner. The document authenticating apparatus includes a coherent light source such as a diode laser to illuminate the photo refractive crystals, and a photosensor to receive light scattered from the photo refractive crystals. The random distribution and orientation of photo refractive crystals comprises a unique characteristic for each card or document, and this characteristic is not based on any assigned number or code. The response of photo refractive crystals to the coherent illumination comprises a time-varying characteristic that is dependent upon the intensity and temporal nature of the illumination itself. Input to the laser illuminator may be varied to elicit differing responses from the photo refractive crystals, and this factor may be very difficult for a counterfeiter to ascertain. Also, for any given illumination intensity or temporal pattern, the image received by the photosensor varies with time. The time at which the photosensor signal is sampled to obtain an identifying image may also be varied, thereby further compounding the difficulty for a counterfeiter to overcome. A large number of "snapshots" of the time-varying image of the document is electronically captured, digitized, and stored in an electronic media. The photosensor signal is compared to the stored data; a match indicates a valid document, and no match indicates an invalid or unauthorized document. The image recognition process can be enhanced by comparing the rate of change in a sequence of images elicited by the laser illuminator.

U.S. Patent No. 5,834,748 (Litman) discloses a card that includes magnetic particles and is difficult to counterfeit. The signal strength, period, amplitude and/or alignment of the magnetic field may be read as coded information by a magnetic reading head. The encoding of this information can be made increasingly difficult to imitate or forge by varying parameters within these (and other) mechanically readable inscriptions. The apparatus readable (mechanically readable) security means to prevent forgery of identification cards, (including the new smart cards with readable chips therein) and pens. The security of the pens is enhanced by the implementation of a mechanically readable security system, which includes a mechanically readable magnetic marking embedded in the transactional item. The marking also may be visually notable or readable, but it at least must be readable by a reading head capable of reading the passage of a magnetic material by the head. The marking is preferably in the form of at least two magnetic filaments or strips and preferably includes a multiple number of filaments of differing coerciveness, magnetic field strength, magnetic field alignment, size or spacing so that when the stylus is passed at a defined and preferably constant speed through the reading device, approval will be given only when the proper signal is provided by the ordered array of appropriate magnetic elements in the pen.

When the digital signature is generated through fingerprint data, registration can also occur without the pen, but rather with a fingerprint sensor that captures essentially a complete fingerprint of the finger for references purposes. Subsequently, when the stylus is used, the partial print is compared to the complete fingerprint for matching purposes.

Just as a transponder that is compatible with existing cardreaders enables the system of the present invention to be compatible with card-based systems and pen-based (cardless) systems as shown above, utilization of a stylus that is compatible with existing cardreaders offers many similar advantages for a wireless stylus, that is compatible with card-based systems and pen-based systems. FIGURES 15A and 15B disclose a first preferred embodiment of a stylus grip for use with the identity authentication system of the present invention, the grip having a rotatable flap that includes a magnetic stripe that can be read by a conventional card reader.

The fingerprint sensors of choice are either of the following:

> The FingerTIP$_{TM}$ sensor from Infineon enables the integration of a miniature fingerprint sensor into a wide variety of end-products including PCs, notebook computers, handheld devices, set-top boxes, ATM's, point of sale terminals, ticketing kiosks, building access systems, or any other application that would benefit from replacing PIN and password identification with biometric-based verification. The chip is compact, reliable and robust enough to convert a previously exotic technology-biometric user ID into an everyday reality. The FingerTIP chip is a small (18mm x 21mm x 1.5mm) IC embedding a 288 x 224 pixel contact sensor array that images the lines and ridges of a human fingerprint when a user touches the device. Each pixel has an 8-bit data depth, enabling evaluation of subtle gradations (256 shades of gray) of a fingertip and their translation into a set of indices - the key identifying features of an individual fingerprint. Imaging and data transfer of an impression takes only 100 milliseconds.
>
> STMicroelectronics has developed a fingerprint sensor of substantially the same size as the Infineon sensor and that use capacitive-sensor-array technology; building silicon IC's containing an array of sensor plates. ST's TouchChip technology uses a

capacitive sensing technique to capture, in less than one tenth of a second, a high-resolution image of a fingerprint when the finger is applied directly to the chip surface. The output of the chip is a digital representation of the fingerprint, which can be processed by the algorithms developed by 5AGEM, which immediately confirm or invalidate the recognition of pre-identified persons and then be further processed by application-dependent software.

A transponder of choice is commercially available from AMSKAN of Mulgrave, Victoria in Australia - the InfraRed Datalink allows serial "through the windscreen' data transfer between a vehicle and the roadside in daylight with high reliability and is presently used for capturing information from vehicles as they re-fuel, re-load, or at highway speeds. The IRD is comprised of two main components, the interrogator and the wireless transponder. The interrogator is mounted either at the point-of-sale terminal. The size of the transponder is 130 x 80 x 50 mm.

Another transponder of choice is Miotec's mPollux – that is developed on a SIM card and its integrated security solutions offer a flexible and secure platform with a sufficient capacity for a wireless PKI system. The SIM platform is a FLASH microcontroller, which has a separate RISC processor for RSA operations. MioCOS operating system is compliant with both GSM and PKI standards. Furthermore, the integrated biometric functions enable, among other things, replacing the PIN code in an electronic ID card with fingerprint matching.

One skilled in the art will also recognize the application of the principles of the identity verification system of the present invention to electronic commerce, where the party seeking to enter or access data, or simple to correspond with another. When the party seeking to make the transaction is remote from the host computer terminal (or second party), the remote party can generally not be seen, and so the race, ethnicity, gender, or even species cannot be ascertained. In such instances, the need for identity verification takes on increased importance. Accordingly, the identity verification process of the present invention requires that the remote party have access to a signature pad – the signature pad having means to generate a digital and an electronic signature. The digital and/or electronic signatures compared against reference data before allowing the transaction to go forward, and the digital and electronic signatures are captured and preserved in a transaction record.

Throughout this application, various U.S. Patents, Patent Applications, and PCT Applications are referenced by number and inventor. The disclosures of these Patents and Applications in their entireties are hereby incorporated by reference into this specification in order to more fully describe the state of the art to which this technology pertains.

Throughout this application, various U.S. Patents, Patent Applications, and PCT Applications are referenced by number and inventor. The disclosures of these Patents and Applications in their entireties are hereby incorporated by reference into this specification in order to more fully describe the state of the art to which this technology pertains. It is evident that many alternatives, modifications, and variations of the authenticated commercial transaction system of the present invention will be apparent to those skilled in the art in light of the disclosure herein. It is intended that the metes and bounds of the present invention be determined by the appended claims rather than by the language of the above specification, and that all such alternatives, modifications, and variations which form a conjointly cooperative equivalent are intended to be included within the spirit and scope of these claims.

CLAIMS

1. A method for processing an access request, the method comprising:

   a. capturing user reference data (involving user biometric data or user metric data) from a wireless device carried by a user, the user reference data having been submitted in a registration process;

   b. capturing user sensed data (involving user biometric data or user metric data) as the user writes a name, the name being written with a stylus;

   c. transmitting the user sensed data and the user captured data to a processor system, the user reference data being transmitted to the processor by means of radio-frequency transmission;

   d. comparing the user sensed data against the user reference data in the processor;

   e. authenticating the identity of the user based upon the results of the comparison; and

   f. enabling user access (account, network data, or physical) if the processor confirms user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

2. A method for processing an access request, the method comprising:

   a. capturing a user record number from a wireless device carried by a user, the user record number having been submitted in a registration process;

b. capturing user sensed data (involving user biometric data or user metric data) as the user writes a name, the name being written with a stylus;

c. transmitting the user sensed data and the user record number to a processor system, the user record number being transmitted to the processor by means of radio-frequency transmission;

d. using the user record number to retrieve user reference data (involving user biometric data, user metric data, or user signature data);

e. comparing the user sensed data with the user reference data in the processor;

f. authenticating the identity of the user based upon the results of the comparison; and

g. enabling user access (account, network data, or physical) if the processor confirms user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

3. A method for processing an access request, the method comprising:

a. capturing user reference data (involving user biometric data or user metric data) from a wireless device carried by a user, the user reference data being embedded in a barcode, the user reference data having been submitted in a registration process;

b. capturing user sensed data (involving user biometric data or user metric data) as the user writes a name, the name being written with a stylus;

c. transmitting the user sensed data and the user captured data to a processor system, the user reference data being transmitted to the processor by means of a barcode reader;

d. comparing the user sensed data against the user reference data in the processor;

e. authenticating the identity of the user based upon the results of the comparison; and

f. enabling user access (account, network data, or physical) if the processor confirms user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

4. A method for processing an access request, the method comprising:

a. capturing a user record number from a wireless device carried by a user, the user record number, the user record number being embedded in a barcode having been submitted in a registration process;

b. capturing user sensed data (involving user biometric data or user metric data) as the user writes a name, the name being written with a stylus;

c. transmitting the user sensed data and the user record number to a processor system, the user record number being transmitted to the processor by means of a barcode scanner;

d. using the user record number to retrieve user reference data (involving user biometric data, user metric data, or user signature data);

e. comparing the user sensed data with the user reference data in the processor;

f. authenticating the identity of the user based upon the results of the comparison; and

g. enabling user access (account, network data, or physical) if the processor confirms user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

5. A system comprising:

a. a stylus for capturing user biometric, metric, or signature data of a user as the stylus is being used to submit user data;

b. a wireless device carried by the user, the wireless device having memory, the memory including user data, the user data including a user data record number;

c. a processing system that captures the user data record number from the wireless device by means of radio frequency transmission, the radio frequency transmission occurring from the wireless device to the processor, the processing system accessing user reference data by use of the user record number, the user data record including reference data involving user biometric data, user metric data, or user signature data, the processing system using the captured data processed from the stylus for comparison against the user reference data processed from the wireless device, user authentication being based upon the comparison, user access (account, network data, or physical) being permitted if the processor confirms the user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

6. A system comprising:

a. a stylus for capturing user biometric data, metric data, or signature data as the stylus is being used to submit user data;

b. a wireless device carried by the user, the wireless device having memory, the memory including user reference data (involving user biometric data, user metric data, or user signature data); and

c. a processing system that captures the user reference data from the wireless device by means of radio frequency transmission, the radio frequency transmission occurring from the wireless device to the processor, the processing system using the captured data processed from the stylus for comparison against the user reference data processed from the wireless device, user authentication being based upon the comparison, user access (account, system, or physical) being permitted if the processor confirms the user identity and other system criteria (fund availability, clearance) confirms that the access request should be approved.

7. A system comprising:

a. a stylus for capturing user biometric, metric, or signature data of a user as the stylus is being used to submit user data;

b. a wireless device carried by the user, the wireless device having memory, the memory including user data, the user data including a user data record number, the user data being embedded in a barcode; and

c. the processing system capturing the user data record number from the wireless device by means of a barcode reader, the processing system accessing user reference data by use of the user record number, the user data record including reference data involving user biometric data, user metric data, or user signature data, the processing system using the captured data processed from the stylus for comparison against the user reference data processed from the wireless device, user authentication being based upon the comparison, user access (account, network data, or physical) being permitted if the processor confirms the user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

8. A system comprising:

a. a stylus for capturing user biometric data, metric data, or signature data as the stylus is being used to submit user data;

b. a wireless device carried by the user, the wireless device having memory, the memory including user reference data (involving user biometric data, user metric data, or user signature data); and

c. a processing system that captures the user data record number from the wireless device by means of a barcode reader, the processing system using the captured data processed from the stylus for comparison against the user reference data processed from the wireless device, user authentication being based upon the comparison, user access (account, system, or physical) being permitted if the processor confirms the user identity and other system criteria (fund availability, clearance) confirms that the access request should be approved.

9. A method for enabling a user to process a payment for goods or services from a provider, the method comprising:

a. tendering funds sufficient to pay for the goods or services, fund tendering being by a payment card and through a cardreader

b. capturing user reference data (involving user biometric data or user metric data) from a wireless device carried by the user, the wireless device being separate and apart from the payment card, the user reference data having been submitted in a registration process;

c. capturing user sensed data (involving user biometric data or user metric data);

d. transmitting the user sensed data and the user reference data to a processor system, the user reference data being transmitted to the processor by means of radio-frequency transmission;

e. comparing the user sensed data against the user reference data; and

f. advising the provider of the goods or services when user identity is denied resulting from the comparison of the user sensed data with the user reference data.

10. A method for processing an access request, the method comprising:

a. capturing user sensed data (involving user biometric data or user metric data) as the user writes a name, the name being written with a stylus;

b. transmitting the user sensed data to a smart card, the smart card including a smart-card processor, the smart-card processor including memory, the memory including user reference data (involving user biometric data or user metric data);

c. comparing the user sensed data against the user reference data in the smart-card processor;

d. authenticating the identity of the user based upon the results of the comparison; and

e. enabling user access (account, network data, or physical) if the processor confirms user identity and other system criteria (fund availability, clearance) confirms the access request should be approved.

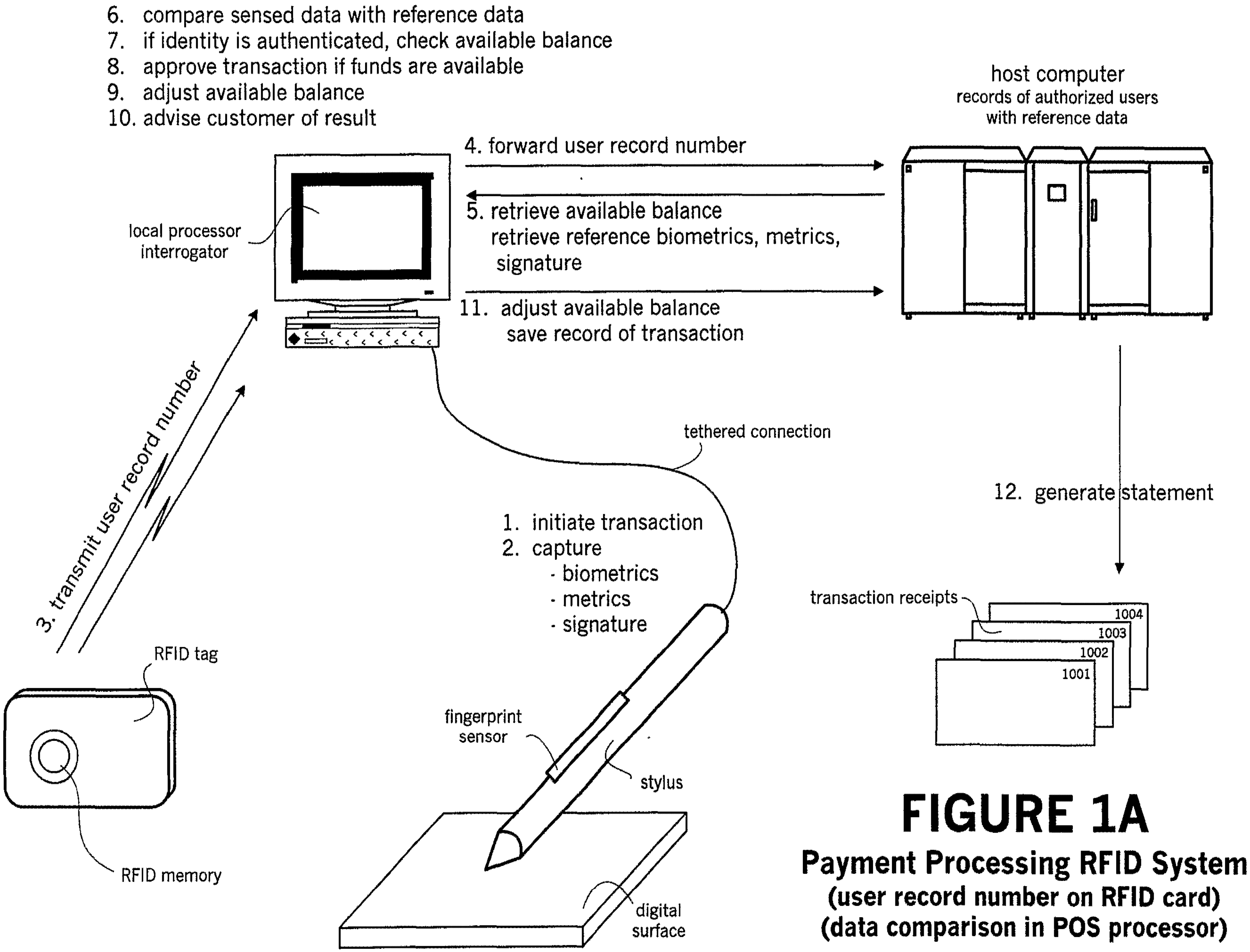

6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance
10. advise customer of result
host computer
records of authorized users
with reference data
4. forward user record number
5. retrieve available balance
retrieve reference biometrics, metrics,
signature
local processor
interrogator
11. adjust available balance
save record of transaction
3. transmit user record number
tethered connection
12. generate statement
1. initiate transaction
2. capture
· biometrics
· metrics
· signature
transaction receipts
1004
1003
1002
1001
RFID tag
fingerprint
sensor
stylus
RFID memory
digital
surface

FIGURE 1A

Payment Processing RFID System
(user record number on RFID card)
(data comparison in POS processor)

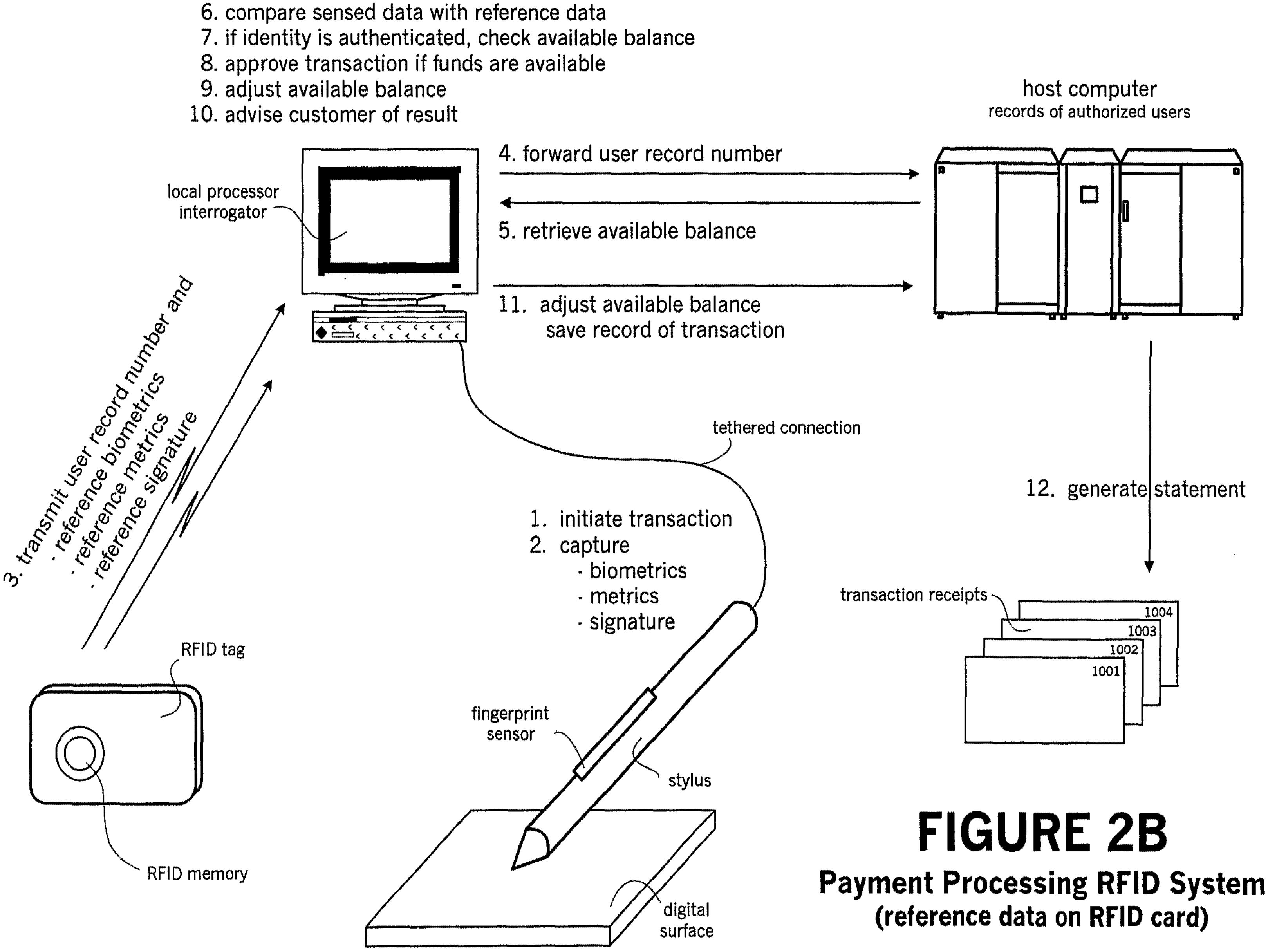

6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance
10. advise customer of result
host computer
records of authorized users
4. forward user record number
local processor
interrogator
5. retrieve available balance
11. adjust available balance
save record of transaction
3. transmit user record number and
· reference biometrics
· reference metrics
· reference signature
tethered connection
12. generate statement
1. initiate transaction
2. capture
- biometrics
- metrics
- signature
transaction receipts
1004
1003
1002
1001
RFID tag
fingerprint
sensor
stylus
RFID memory
digital
surface

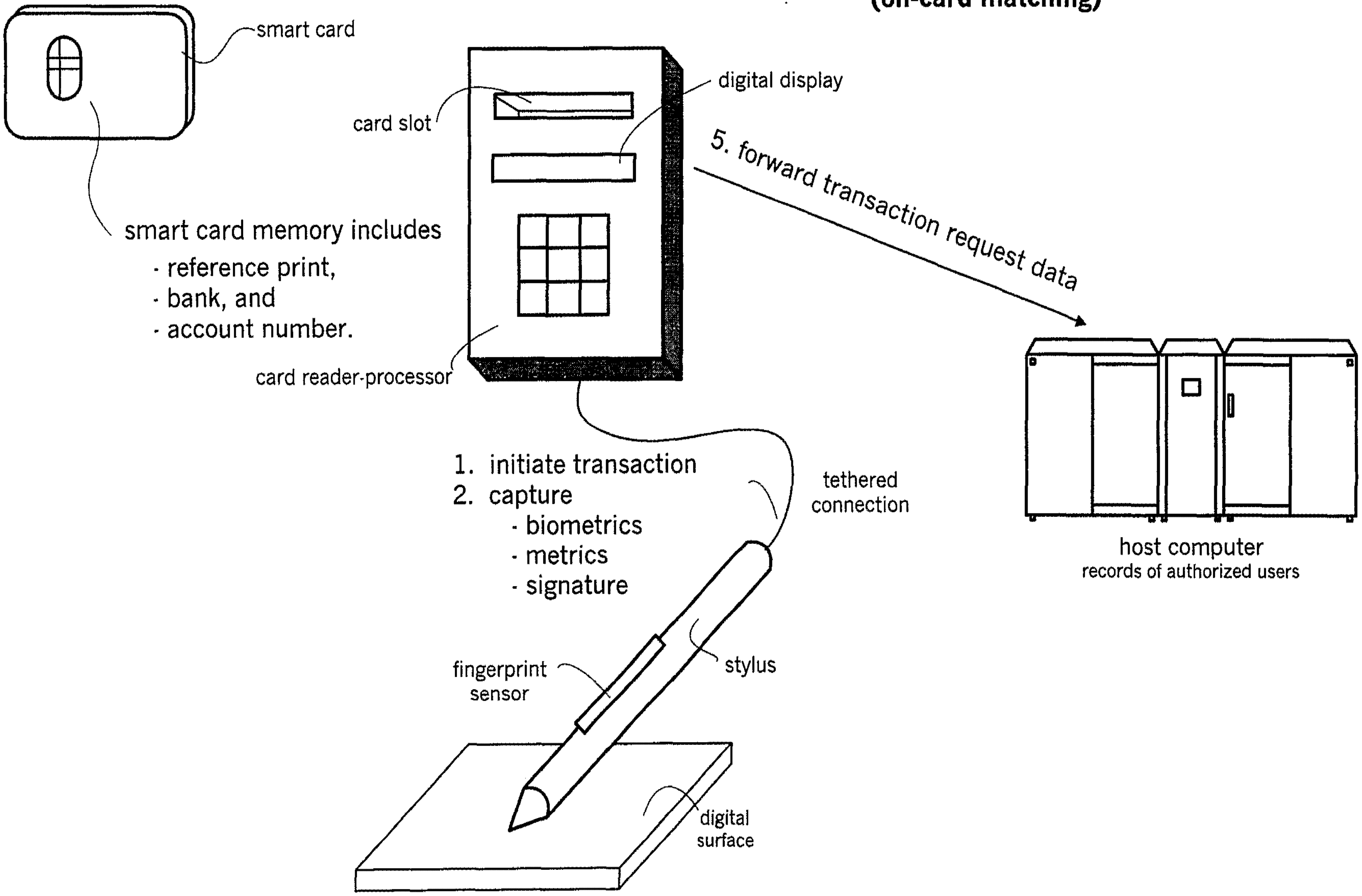
FIGURE 2B

Payment Processing RFID System
(reference data on RFID card)

3. swipe card
4. receive captured data from cardreader
6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance on card
10. advise customer of result

FIGURE 1C

Payment Processing Smart Card System
(on-card matching)



smart card memory includes
- reference print,
- bank, and
- account number.

5. forward transaction request data

1. initiate transaction
2. capture
   - biometrics
   - metrics
   - signature

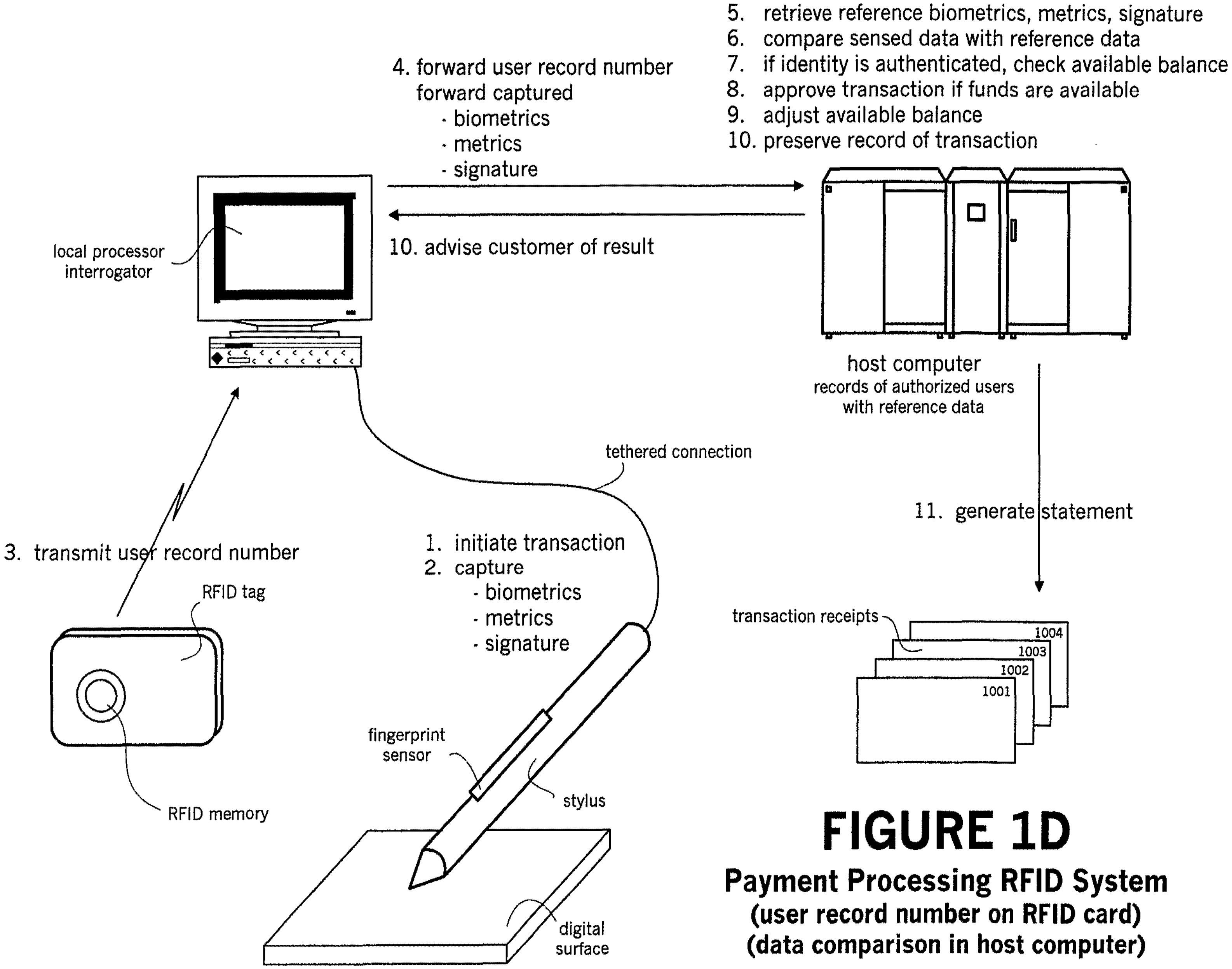

5. retrieve reference biometrics, metrics, signature
6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance
10. preserve record of transaction
4. forward user record number
forward captured
· biometrics
· metrics
· signature
10. advise customer of result
local processor interrogator
host computer
records of authorized users with reference data
tethered connection
11. generate statement
3. transmit user record number
1. initiate transaction
2. capture
- biometrics
- metrics
- signature
RFID tag
transaction receipts
1004
1003
1002
1001
fingerprint sensor
stylus
RFID memory
digital surface

FIGURE 1D

Payment Processing RFID System
(user record number on RFID card)
(data comparison in host computer)

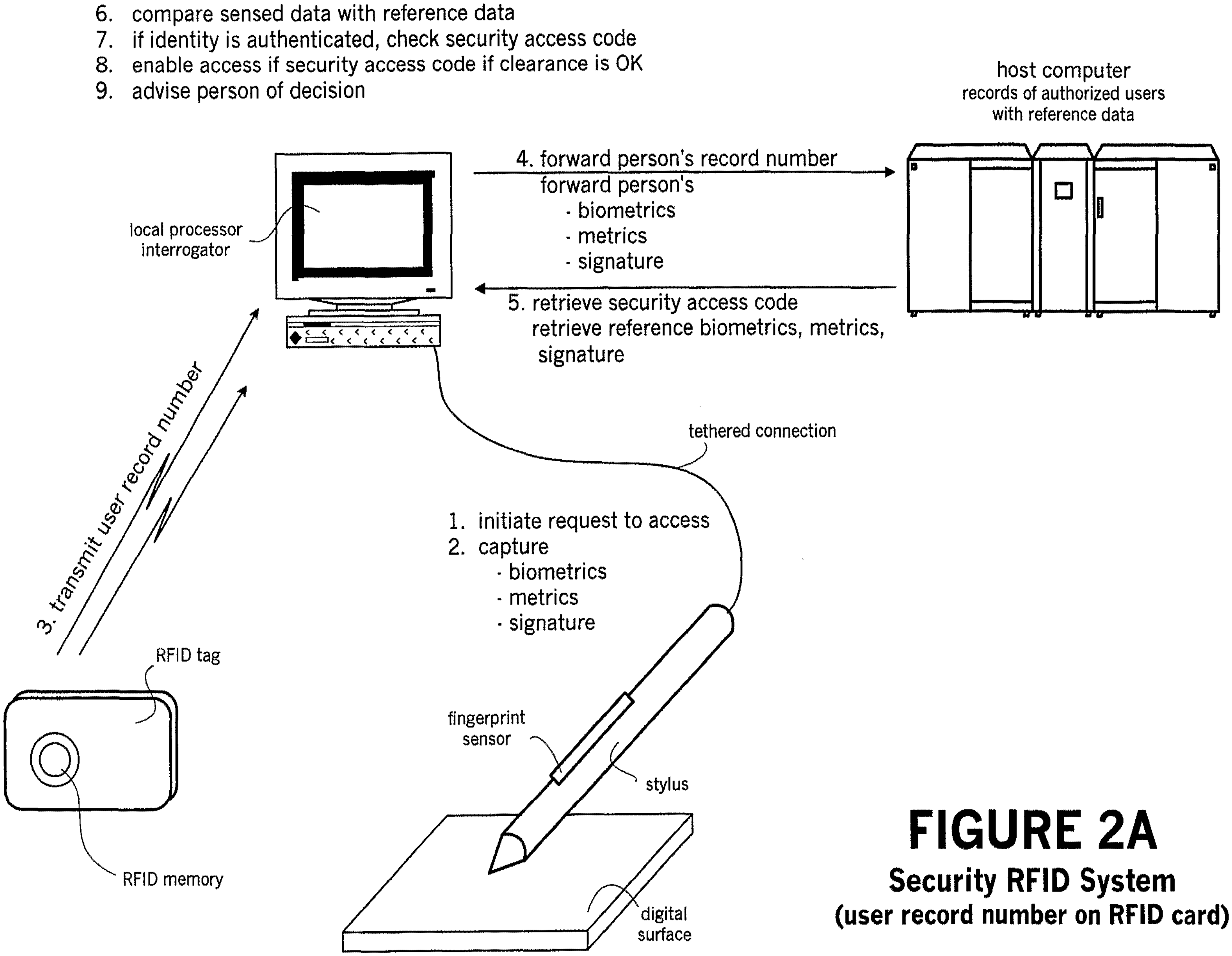

6. compare sensed data with reference data
7. if identity is authenticated, check security access code
8. enable access if security access code if clearance is OK
9. advise person of decision
host computer
records of authorized users
with reference data
local processor
interrogator
4. forward person's record number
forward person's
· biometrics
· metrics
· signature
5. retrieve security access code
retrieve reference biometrics, metrics,
signature
3. transmit user record number
tethered connection
1. initiate request to access
2. capture
· biometrics
· metrics
· signature
RFID tag
RFID memory
fingerprint
sensor
stylus
digital
surface

FIGURE 2A

Security RFID System
(user record number on RFID card)

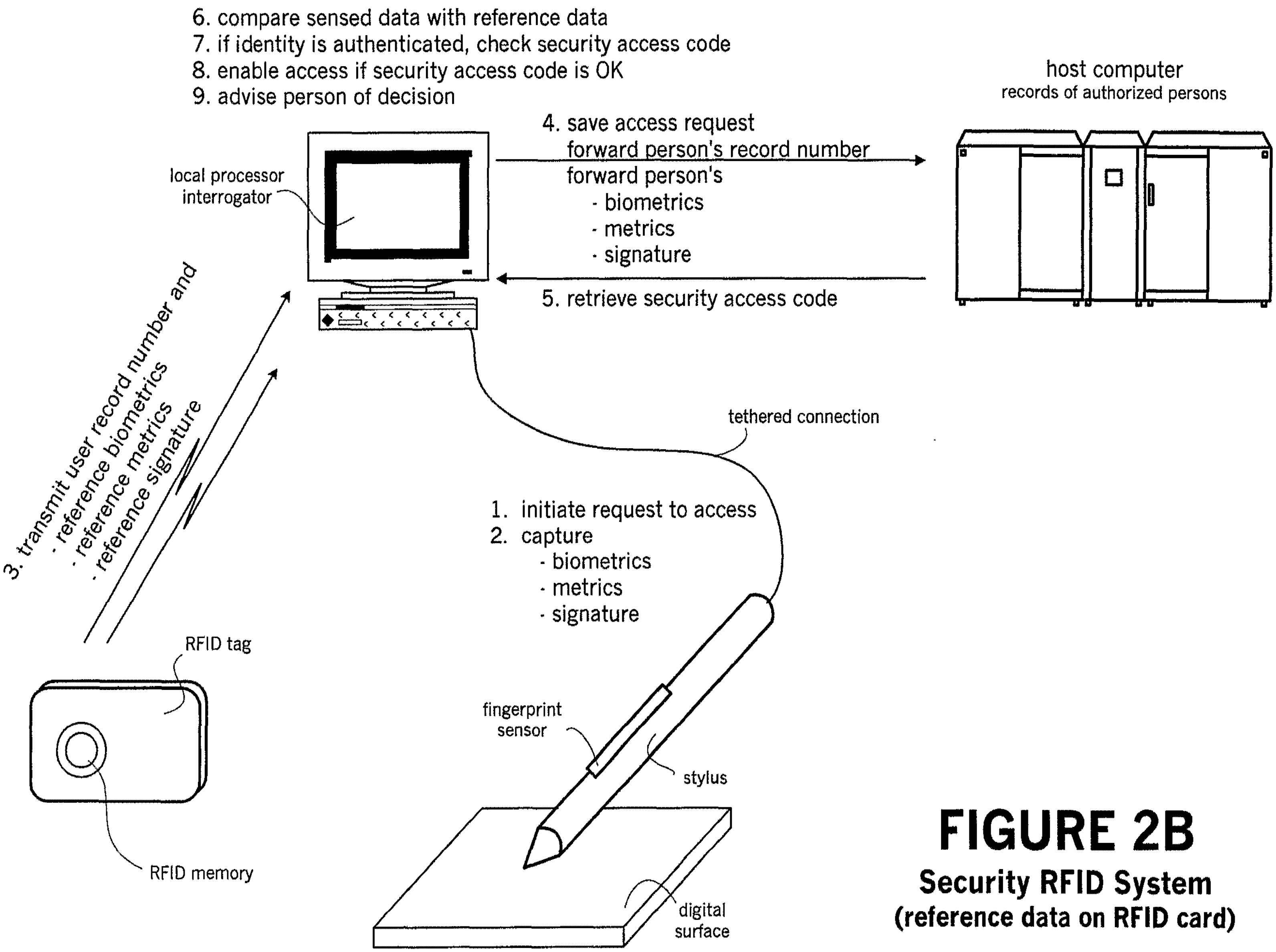

6. compare sensed data with reference data
7. if identity is authenticated, check security access code
8. enable access if security access code is OK
9. advise person of decision
host computer
records of authorized persons
4. save access request
forward person's record number
forward person's
- biometrics
- metrics
- signature
5. retrieve security access code
local processor
interrogator
3. transmit user record number and
- reference biometrics
- reference metrics
- reference signature
tethered connection
1. initiate request to access
2. capture
- biometrics
- metrics
- signature
RFID tag
fingerprint
sensor
stylus
RFID memory
digital
surface

FIGURE 2B

Security RFID System
(reference data on RFID card)

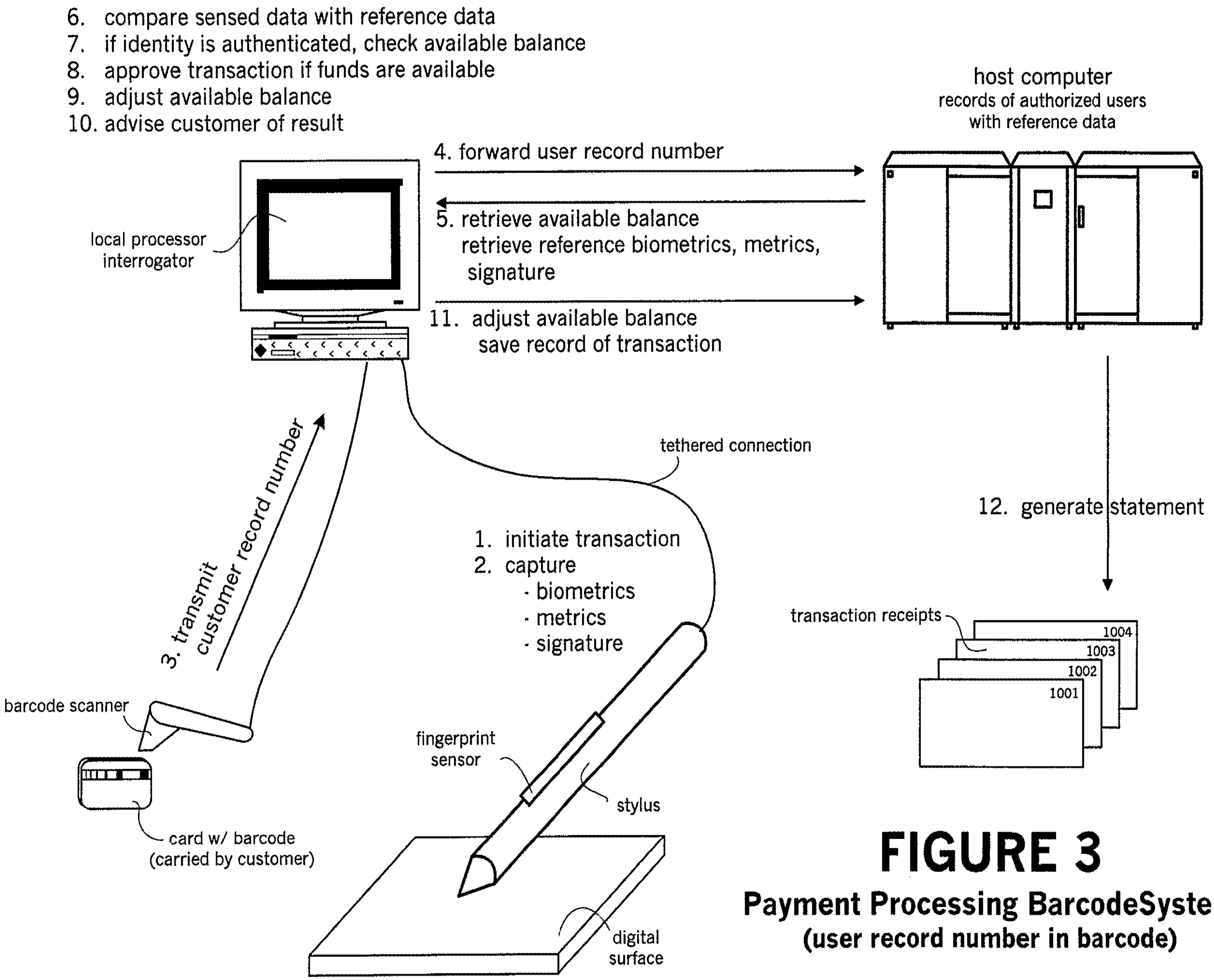
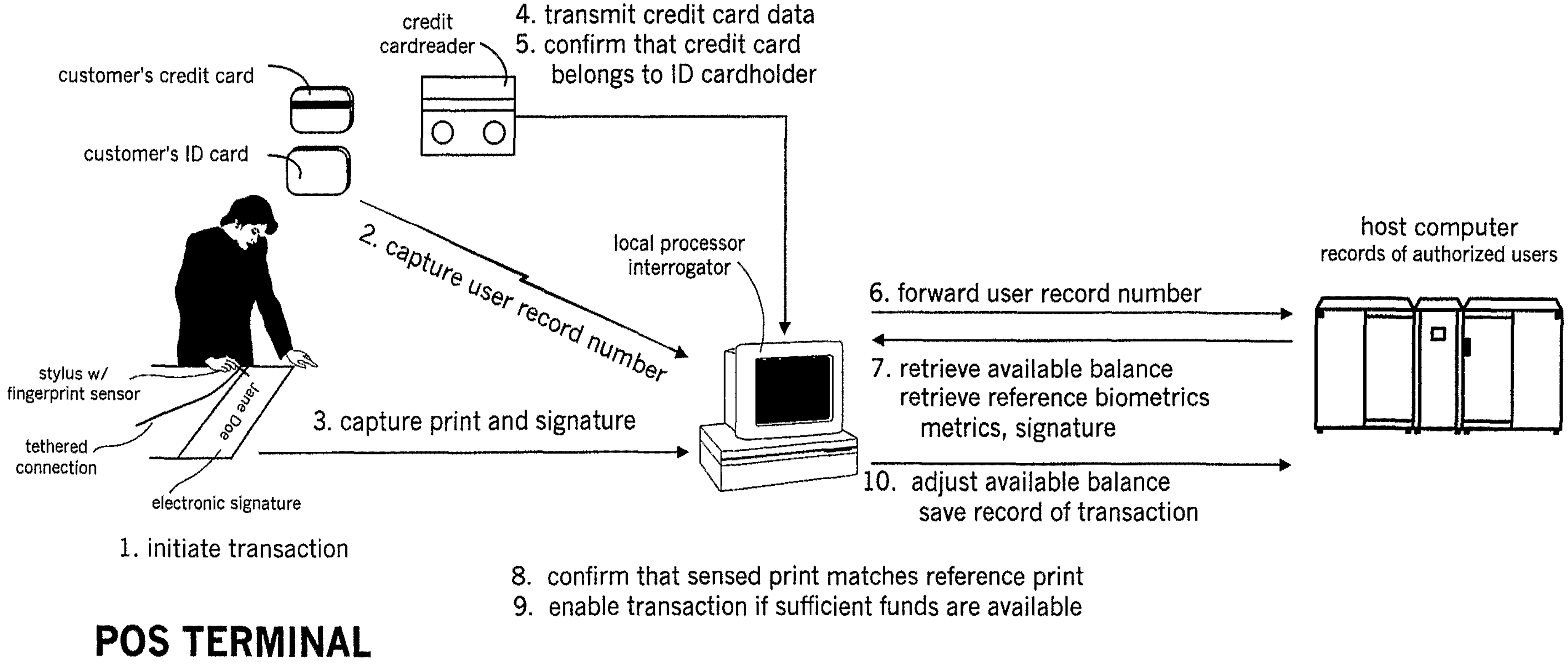

6. compare sensed data with reference data
7. if identity is authenticated, check available balance
8. approve transaction if funds are available
9. adjust available balance
10. advise customer of result
host computer
records of authorized users
with reference data
4. forward user record number
5. retrieve available balance
retrieve reference biometrics, metrics, signature
11. adjust available balance
save record of transaction
local processor
interrogator
3. transmit
customer record number
tethered connection
12. generate statement
1. initiate transaction
2. capture
· biometrics
· metrics
· signature
transaction receipts
1004
1003
1002
1001
barcode scanner
fingerprint
sensor
stylus
card w/ barcode
(carried by customer)
digital
surface

FIGURE 3

Payment Processing BarcodeSystem
(user record number in barcode)

FIGURE 4

POS Payment Transaction System
authentication w/ ID card
payment w/ credit card
(customer records in host computer)


credit cardreader
4. transmit credit card data
5. confirm that credit card belongs to ID cardholder
customer's credit card
customer's ID card
2. capture user record number
local processor interrogator
host computer
records of authorized users
6. forward user record number
7. retrieve available balance retrieve reference biometrics metrics, signature
stylus w/ fingerprint sensor
Jane Doe
tethered connection
3. capture print and signature
10. adjust available balance save record of transaction
electronic signature
1. initiate transaction
8. confirm that sensed print matches reference print
9. enable transaction if sufficient funds are available
POS TERMINAL

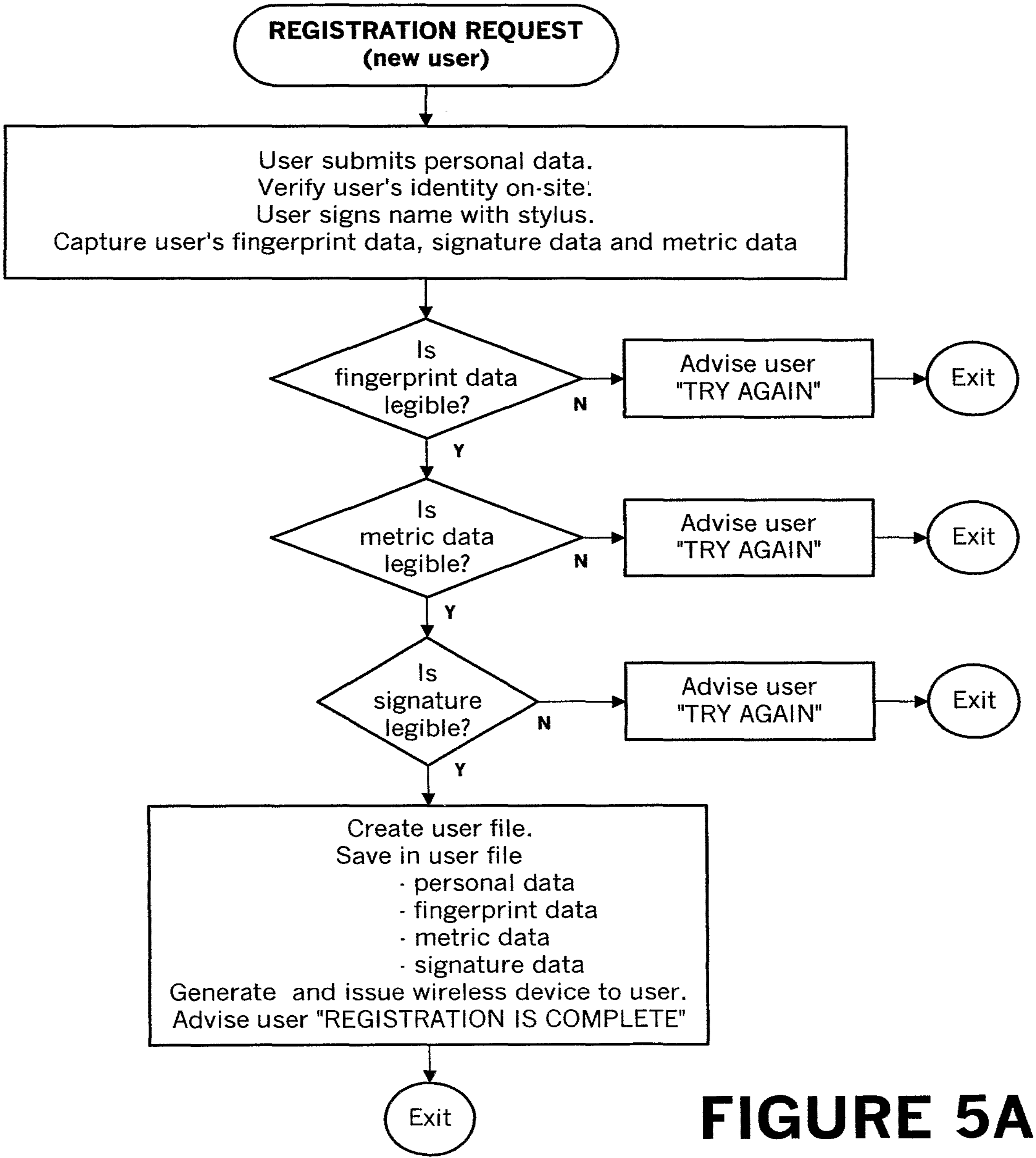


FIGURE 5A
NEW USER

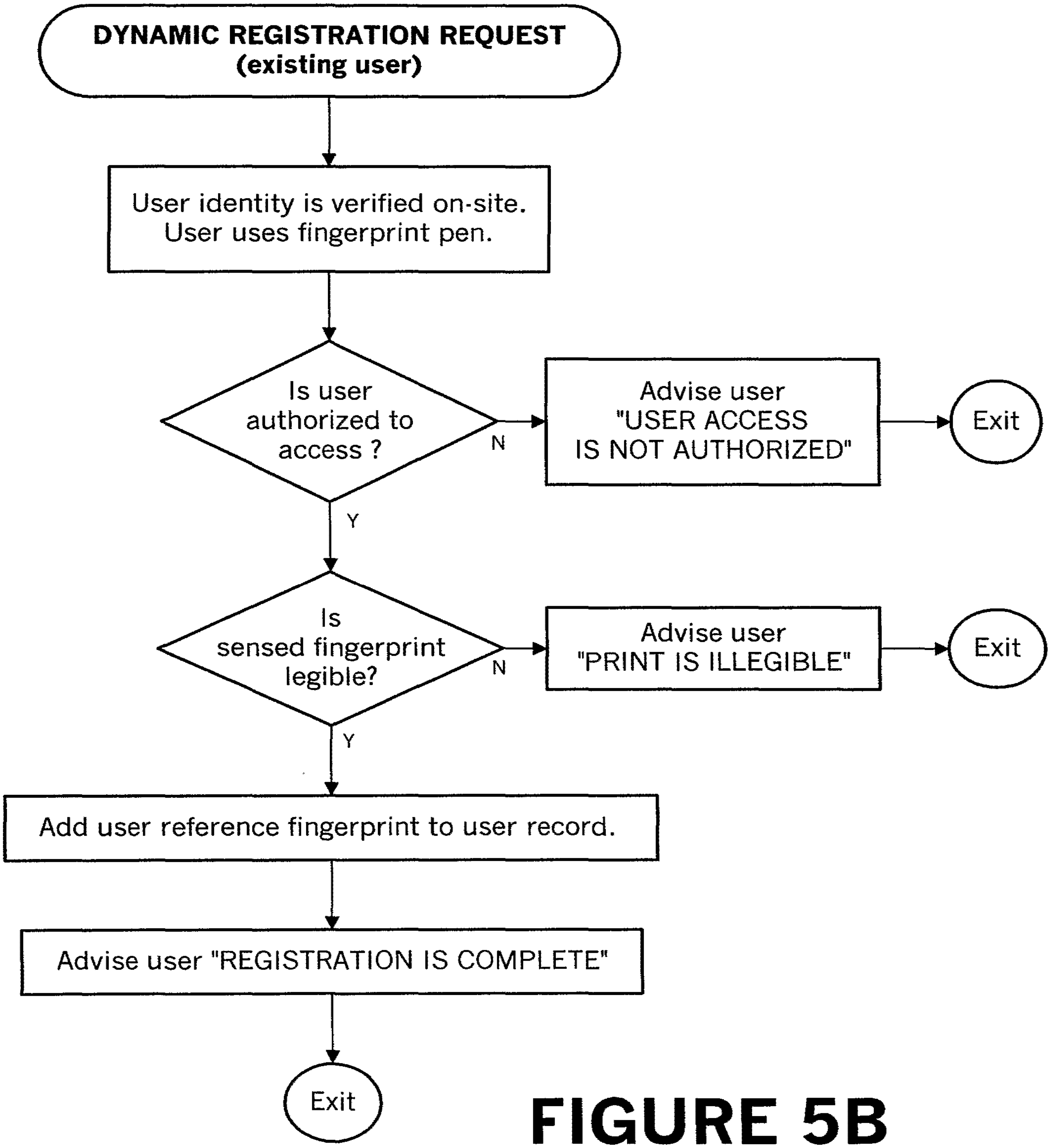

DYNAMIC REGISTRATION REQUEST
(existing user)
User identity is verified on-site.
User uses fingerprint pen.
Is user authorized to access ?
N
Advise user "USER ACCESS IS NOT AUTHORIZED"
Exit
Y
Is sensed fingerprint legible?
N
Advise user "PRINT IS ILLEGIBLE"
Exit
Y
Add user reference fingerprint to user record.
Advise user "REGISTRATION IS COMPLETE"
Exit

FIGURE 5B
DYNAMIC REGISTRATION REQUEST
(existing user)

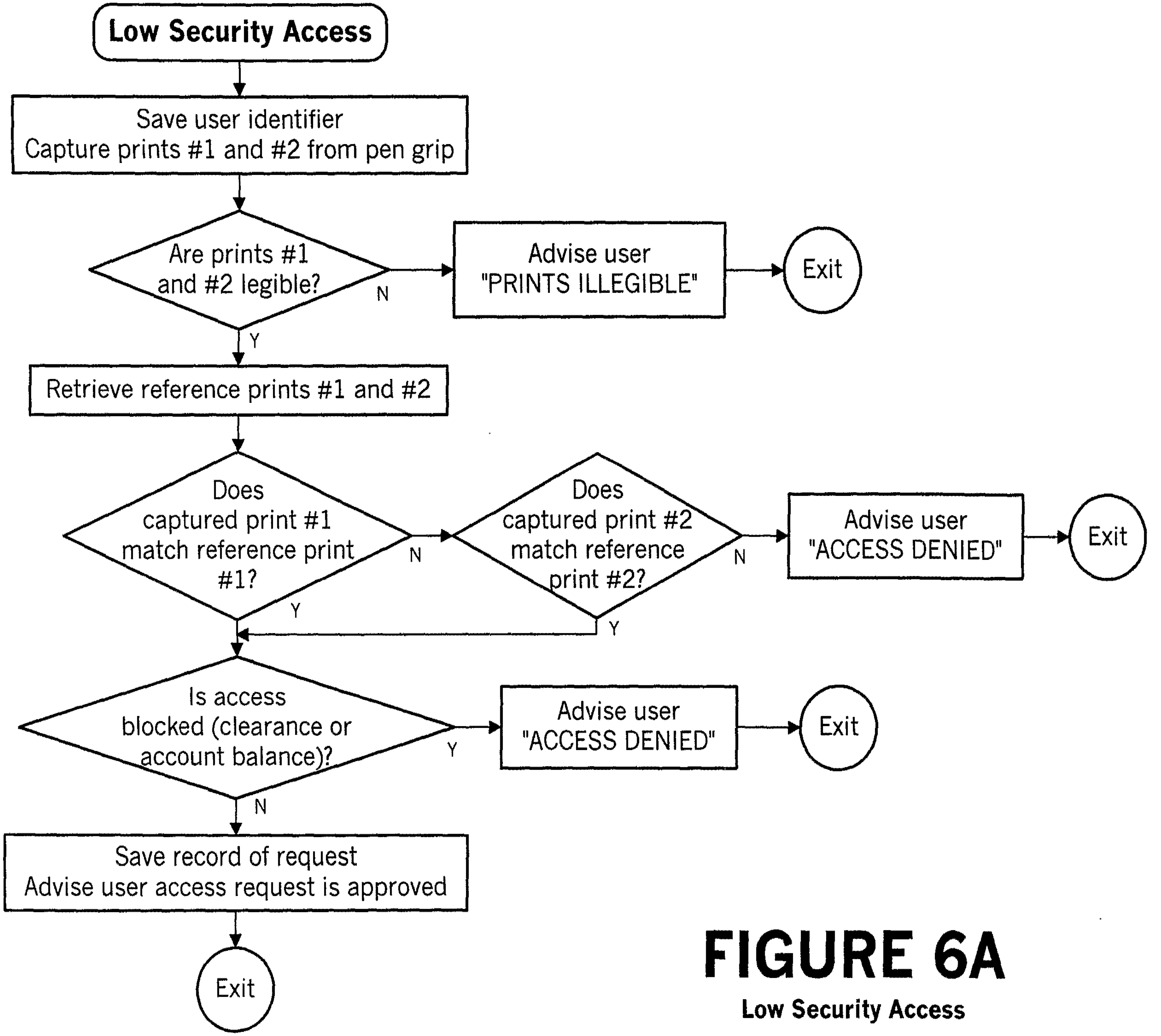

Low Security Access
Save user identifier
Capture prints #1 and #2 from pen grip
Are prints #1 and #2 legible?
N
Advise user "PRINTS ILLEGIBLE"
Exit
Y
Retrieve reference prints #1 and #2
Does captured print #1 match reference print #1?
N
Does captured print #2 match reference print #2?
N
Advise user "ACCESS DENIED"
Exit
Y
Y
Is access blocked (clearance or account balance)?
Y
Advise user "ACCESS DENIED"
Exit
N
Save record of request
Advise user access request is approved
Exit

FIGURE 6A

Low Security Access

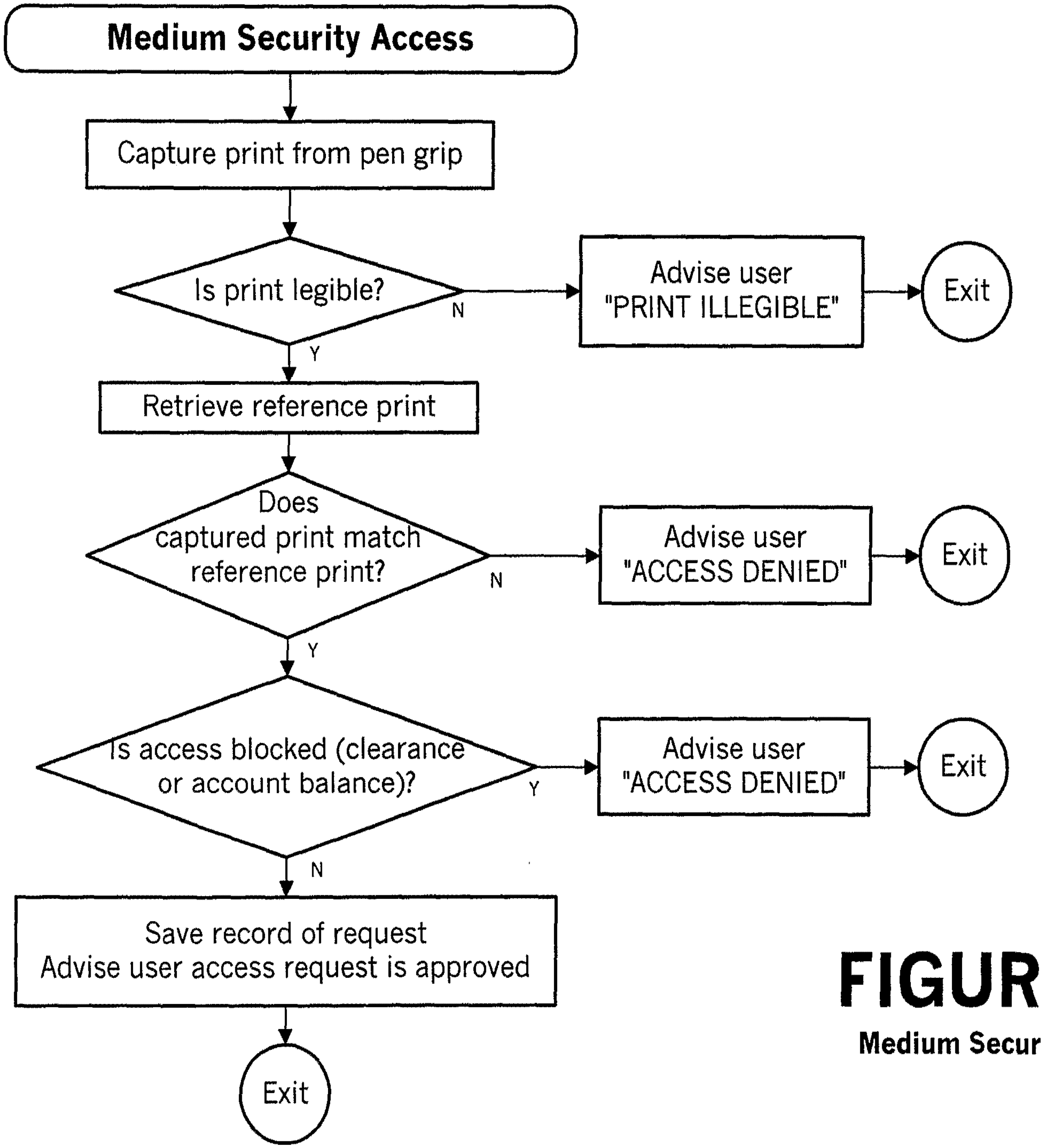

Medium Security Access
Capture print from pen grip
Is print legible?
N
Advise user "PRINT ILLEGIBLE"
Exit
Y
Retrieve reference print
Does captured print match reference print?
N
Advise user "ACCESS DENIED"
Exit
Y
Is access blocked (clearance or account balance)?
Y
Advise user "ACCESS DENIED"
Exit
N
Save record of request
Advise user access request is approved
Exit

FIGURE 6B

Medium Security Access

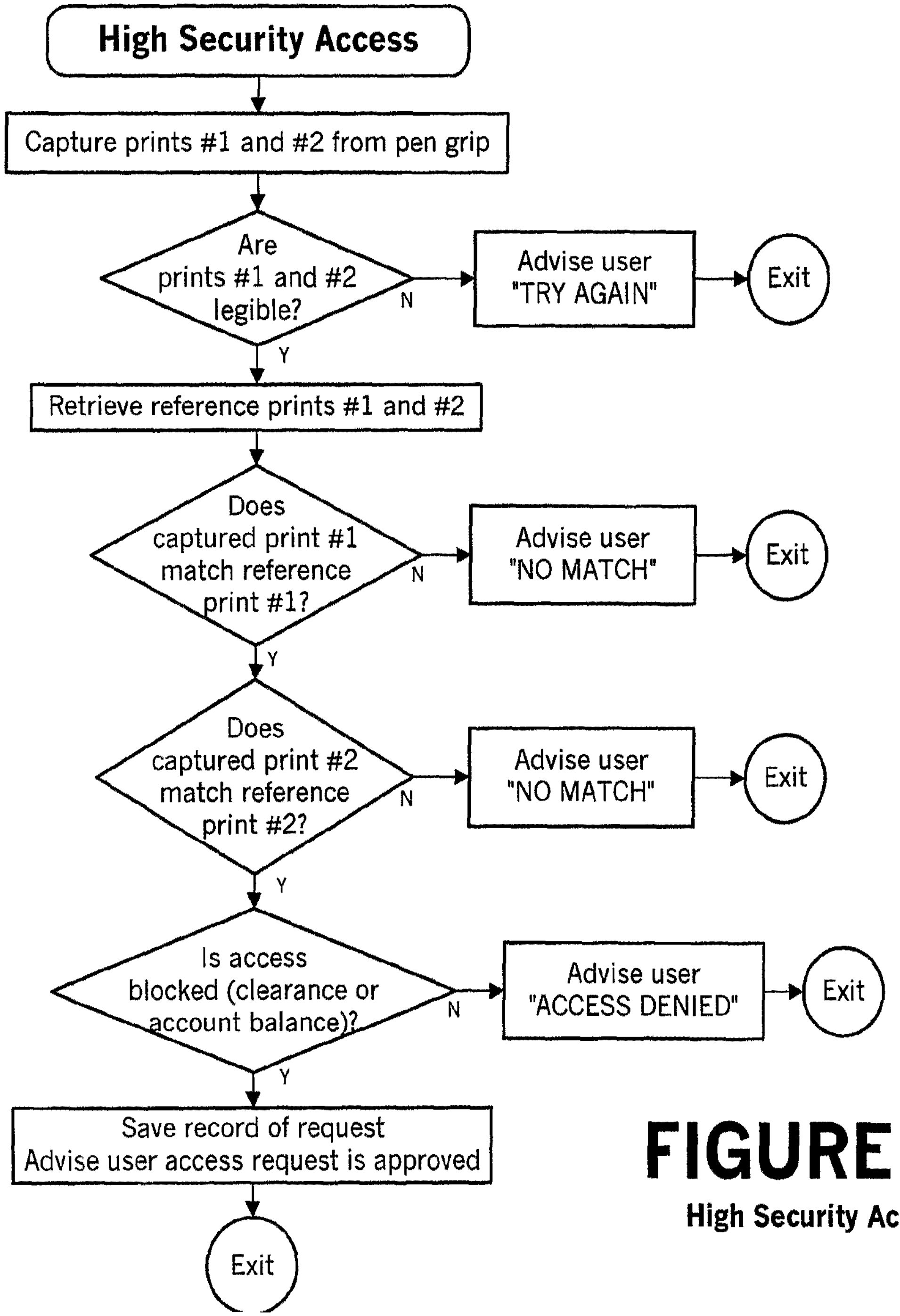

High Security Access
Capture prints #1 and #2 from pen grip
Are prints #1 and #2 legible?
N
Y
Advise user "TRY AGAIN"
Exit
Retrieve reference prints #1 and #2
Does captured print #1 match reference print #1?
N
Y
Advise user "NO MATCH"
Exit
Does captured print #2 match reference print #2?
N
Y
Advise user "NO MATCH"
Exit
Is access blocked (clearance or account balance)?
N
Y
Advise user "ACCESS DENIED"
Exit
Save record of request
Advise user access request is approved
Exit

FIGURE 6C

High Security Access

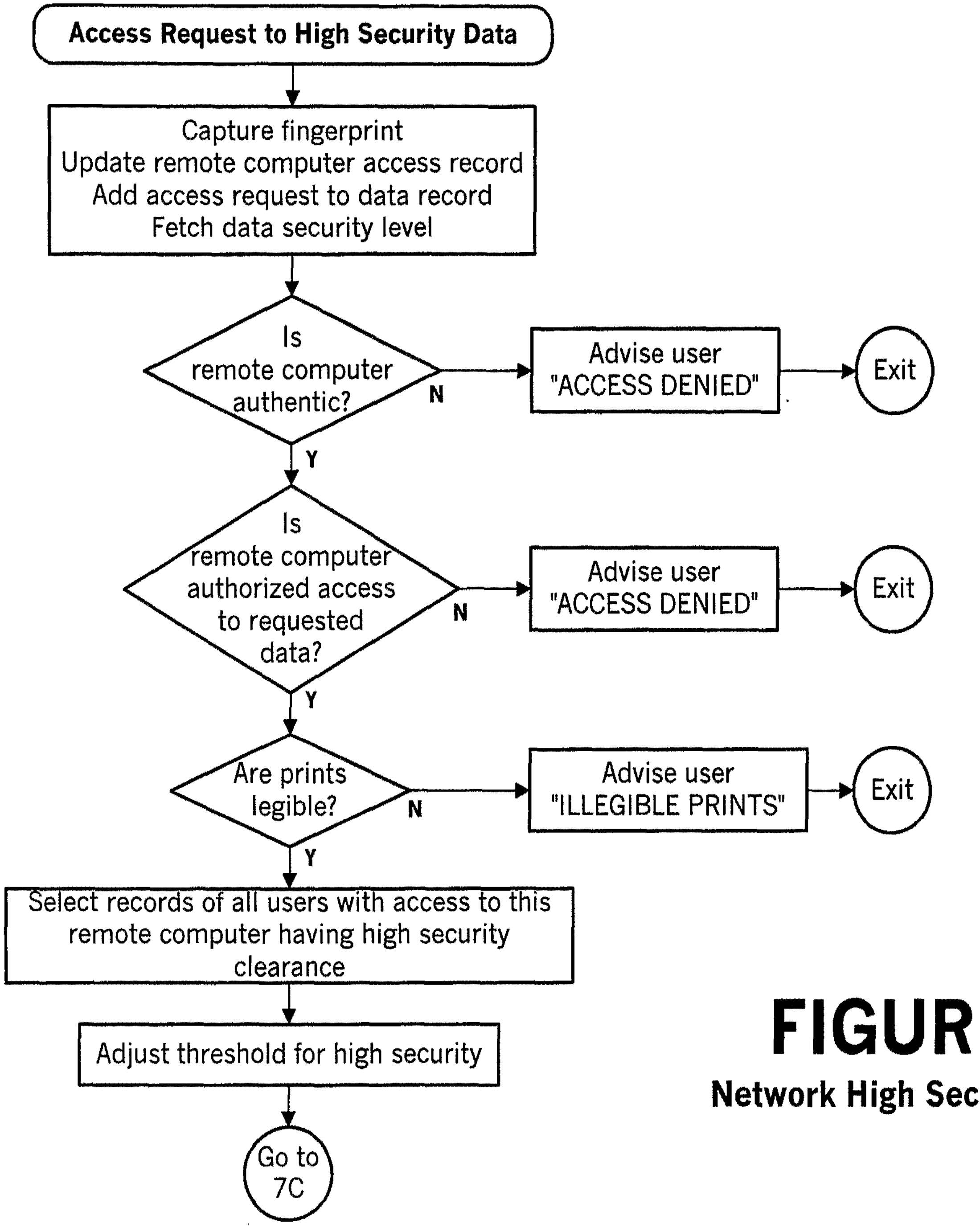

Access Request to High Security Data
Capture fingerprint
Update remote computer access record
Add access request to data record
Fetch data security level
Is remote computer authentic?
N
Advise user "ACCESS DENIED"
Exit
Y
Is remote computer authorized access to requested data?
N
Advise user "ACCESS DENIED"
Exit
Y
Are prints legible?
N
Advise user "ILLEGIBLE PRINTS"
Exit
Y
Select records of all users with access to this remote computer having high security clearance
Adjust threshold for high security
Go to 7C

FIGURE 7A

Network High Security Request

FIGURE 7B

Access Request to High Security Data w/ Misinformation for Counterfeit Remote

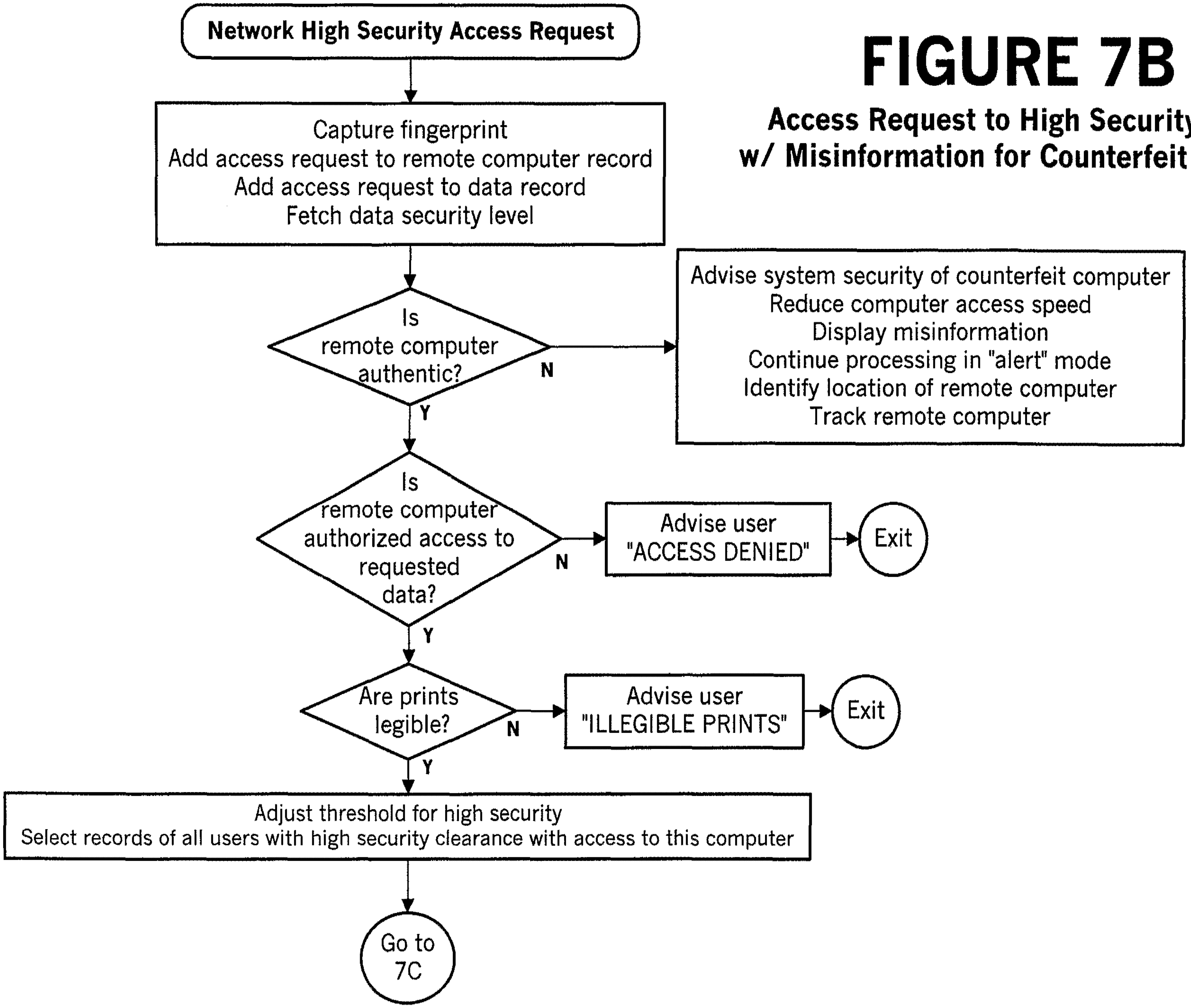
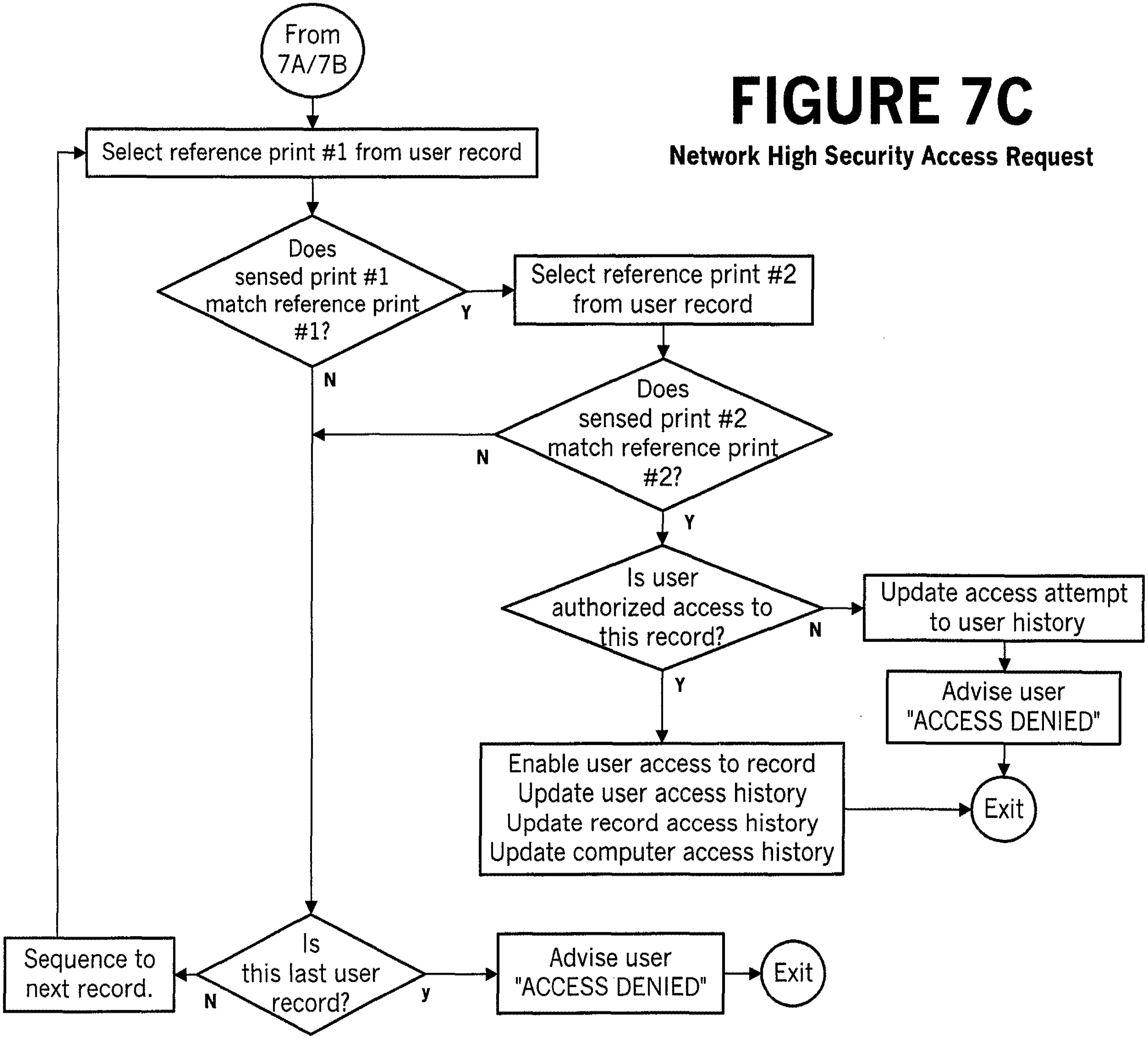

Network High Security Access Request
Capture fingerprint
Add access request to remote computer record
Add access request to data record
Fetch data security level
Is remote computer authentic?
N
Y
Advise system security of counterfeit computer
Reduce computer access speed
Display misinformation
Continue processing in "alert" mode
Identify location of remote computer
Track remote computer
Is remote computer authorized access to requested data?
N
Y
Advise user "ACCESS DENIED"
Exit
Are prints legible?
N
Y
Advise user "ILLEGIBLE PRINTS"
Exit
Adjust threshold for high security
Select records of all users with high security clearance with access to this computer
Go to 7C

FIGURE 7C

Network High Security Access Request


From 7A/7B
Select reference print #1 from user record
Does sensed print #1 match reference print #1?
Y
N
Select reference print #2 from user record
Does sensed print #2 match reference print #2?
N
Y
Is user authorized access to this record?
N
Y
Update access attempt to user history
Advise user "ACCESS DENIED"
Exit
Enable user access to record
Update user access history
Update record access history
Update computer access history
Sequence to next record.
Is this last user record?
N
y
Advise user "ACCESS DENIED"
Exit

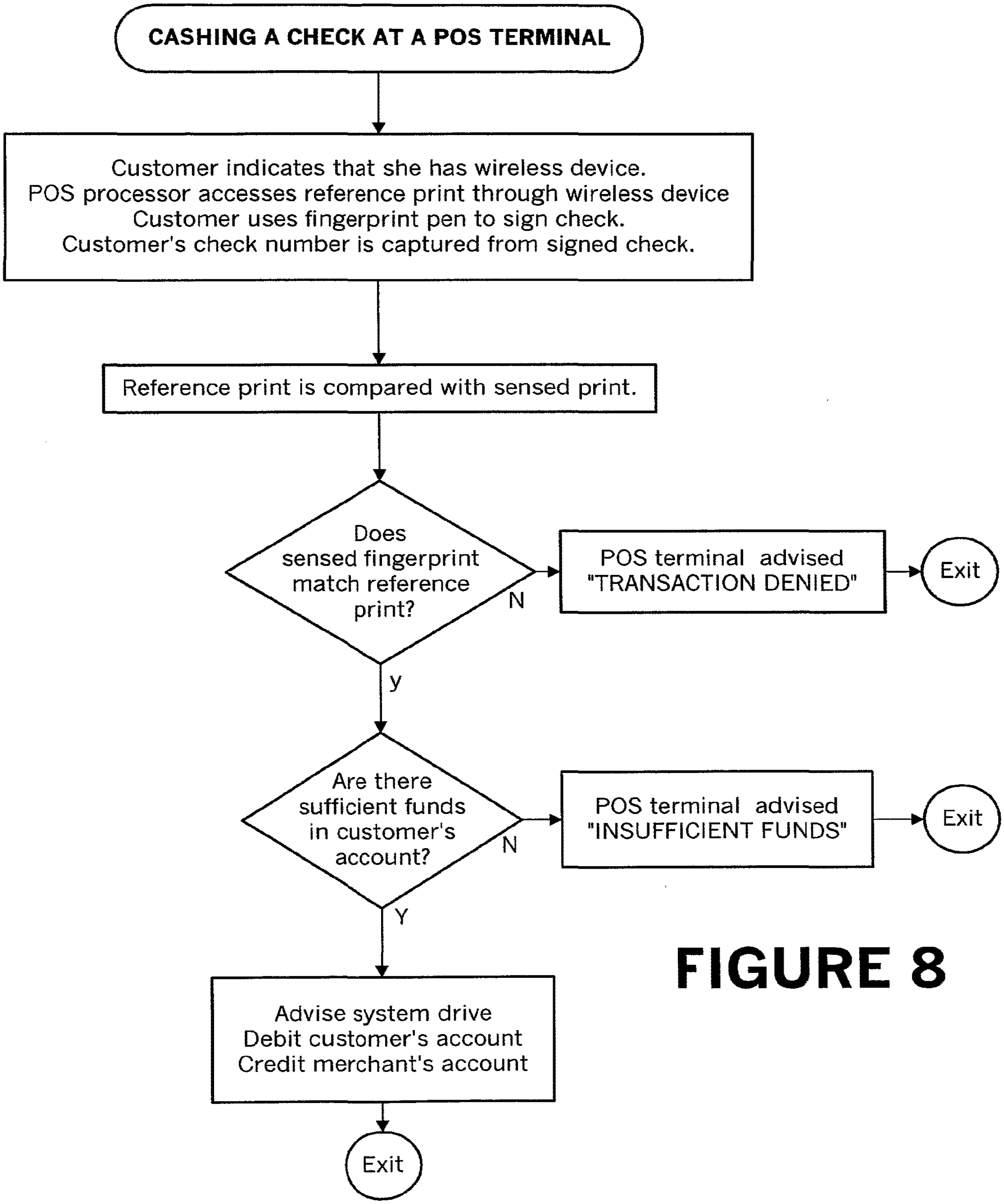
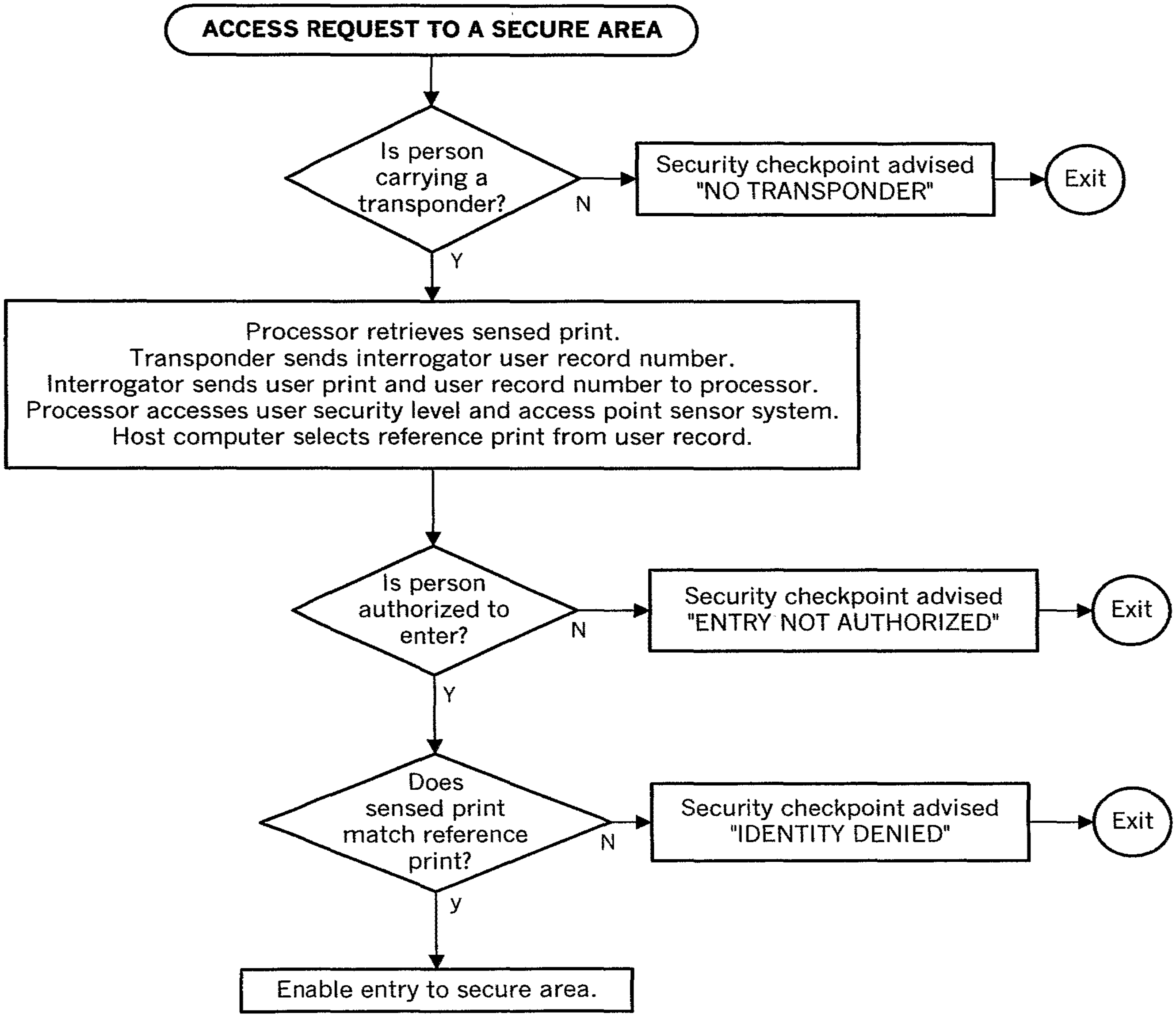

CASHING A CHECK AT A POS TERMINAL
Customer indicates that she has wireless device.
POS processor accesses reference print through wireless device
Customer uses fingerprint pen to sign check.
Customer's check number is captured from signed check.
Reference print is compared with sensed print.
Does sensed fingerprint match reference print?
N
POS terminal advised "TRANSACTION DENIED"
Exit
y
Are there sufficient funds in customer's account?
N
POS terminal advised "INSUFFICIENT FUNDS"
Exit
Y
Advise system drive
Debit customer's account
Credit merchant's account
Exit

FIGURE 8

FIGURE 9

access request
one reference print


ACCESS REQUEST TO A SECURE AREA
Is person carrying a transponder?
N
Security checkpoint advised "NO TRANSPONDER"
Exit
Y
Processor retrieves sensed print.
Transponder sends interrogator user record number.
Interrogator sends user print and user record number to processor.
Processor accesses user security level and access point sensor system.
Host computer selects reference print from user record.
Is person authorized to enter?
N
Security checkpoint advised "ENTRY NOT AUTHORIZED"
Exit
Y
Does sensed print match reference print?
N
Security checkpoint advised "IDENTITY DENIED"
Exit
y
Enable entry to secure area.

CUSTOMER RECORD NO.
CUSTOMER'S BANK
ACCOUNT NO.
ACCOUNT BALANCE
REFERENCE PRINT
REFERENCE SIGNATURE

FIGURE 10A

RFID MEMORY
W/ REFERENCE DATA IN TRANSPONDER

CUSTOMER RECORD NO.
CUSTOMER'S BANK

FIGURE 10B

RFID MEMORY
W/ REFERENCE DATA IN CUSTOMER RECORD

CUSTOMER RECORD NO.
CUSTOMER'S BANK
ACCOUNT NUMBER
ACCOUNT BALANCE
REFERENCE SIGNATURE

FIGURE 11A

CUSTOMER DATABASE RECORD
W/ REFERENCE DATA IN TRANSPONDER

CUSTOMER RECORD NO.
CUSTOMER'S BANK
ACCOUNT NO.
ACCOUNT BALANCE
REFERENCE PRINT
REFERENCE SIGNATURE

FIGURE 11B

CUSTOMER DATABASE RECORD
W/ REFERENCE DATA IN RECORD

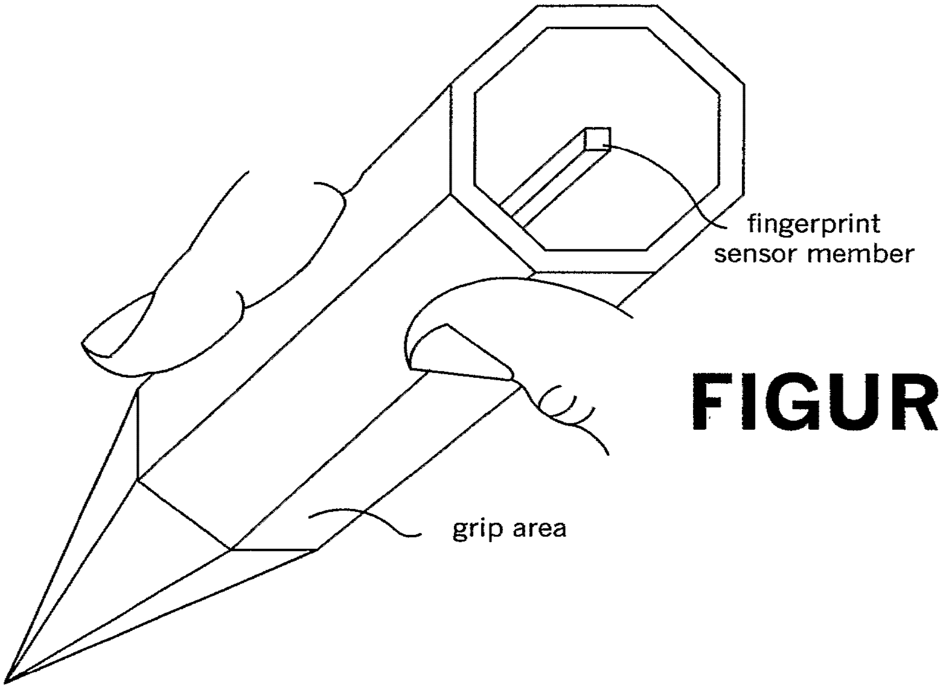


FIGURE 12A

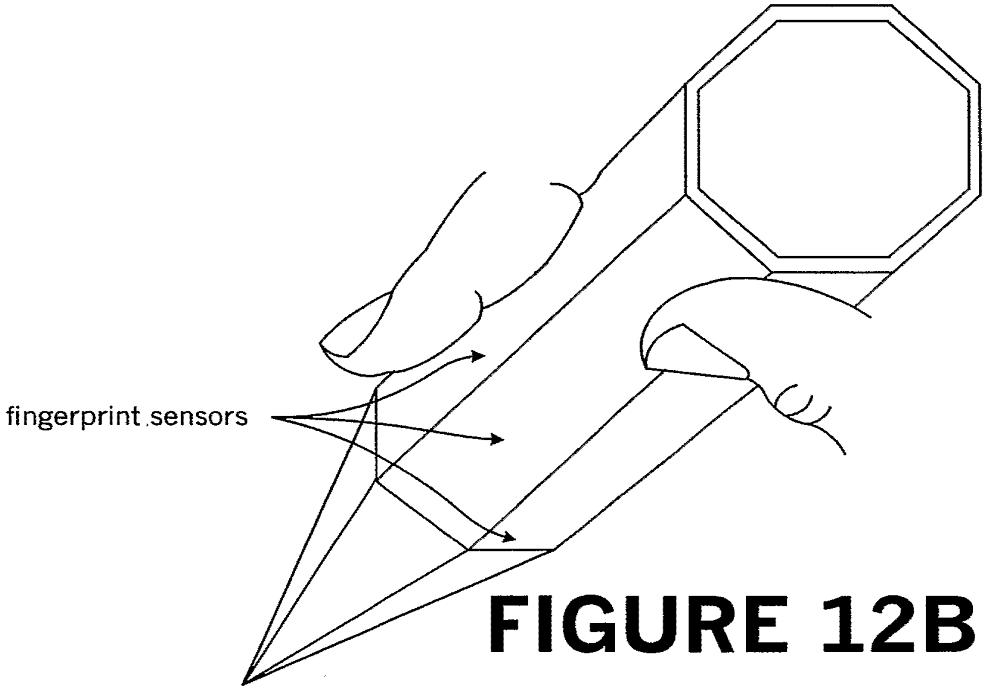


FIGURE 12B

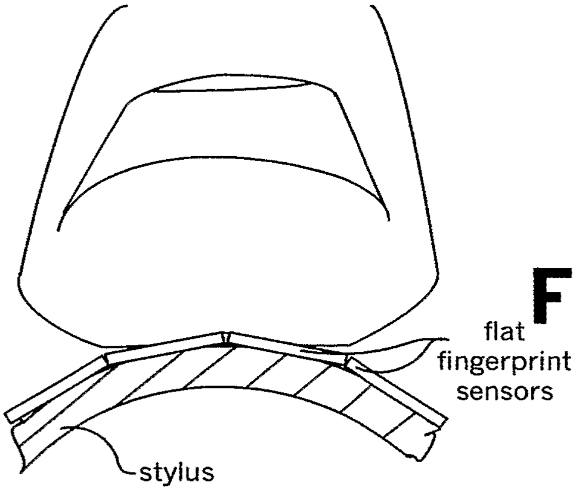


FIGURE 13A

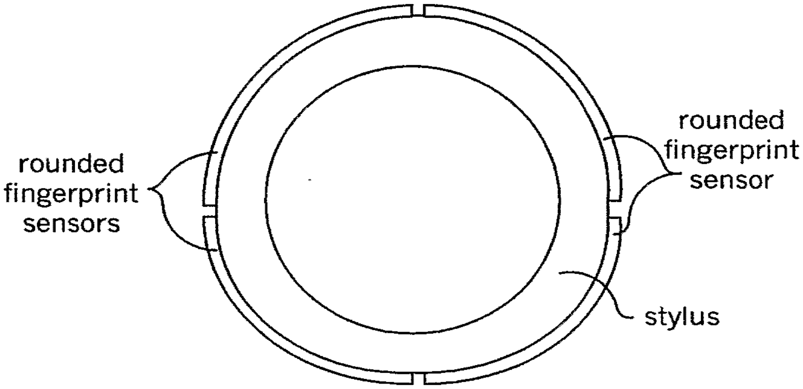


FIGURE 13B

USER RECORD NUMBER
USER NAME
USER ADDRESS
USER SECURITY CLEARANCE LEVEL
REFERENCE PRINT USER REFERENCE THUMB PRINTS - RIGHT
REFERENCE PRINT USER INDEX FINGER - RIGHT
REFERENCE PRINT PRINT OF USER HAND GEOMETRY - RIGHT
REFERENCE PRINT OF USER FACIAL GEOMETRY

FIGURE 14A
USER RECORD

SAFETY DEPOSIT BOXES
TELLER WINDOW A
TELLER WINDOW B
TELLER WINDOW C
PERSONNEL RECORDS
EMPLOYEE EMAIL
WORKING HOURS BUILDING ACCESS
OFF-HOUR BUILDING ACCESS
PARKING LOT ACCESS
BANK SAFE
CORPORATE PAPERS
PENDING LITIGATION

FIGURE 14B
SECURITY ACCESS SITES

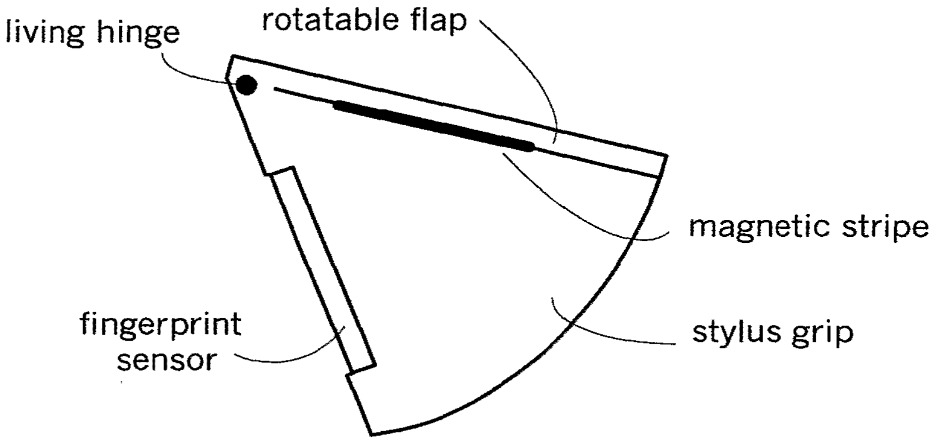


FIGURE 15A

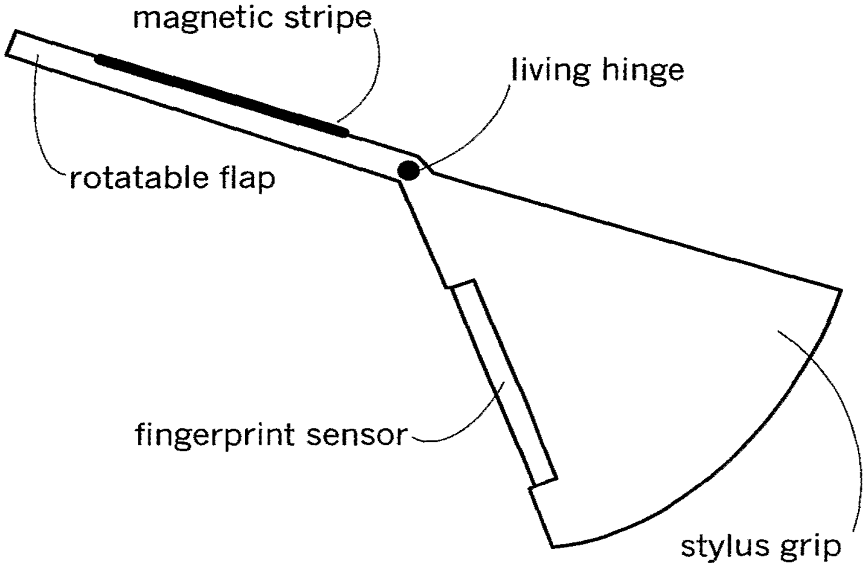


FIGURE 15B

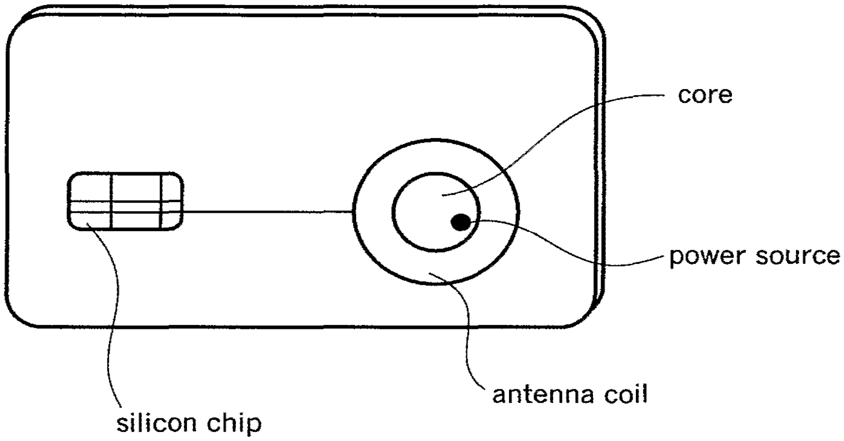


FIGURE 16A
ID CARD W/ TRANSPONDER

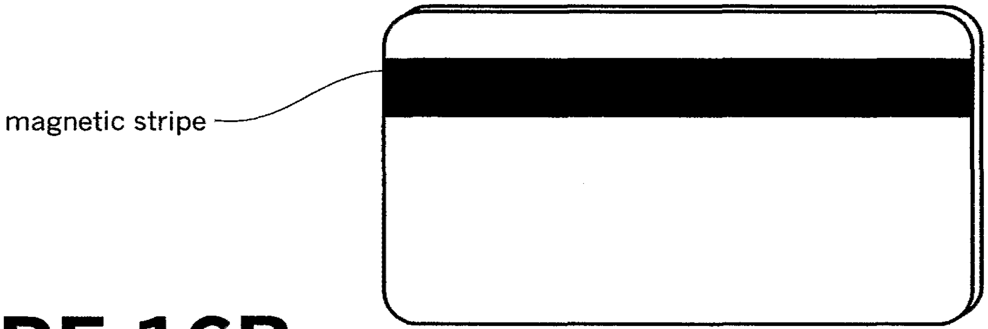


FIGURE 16B
ID CARD w/ MAGNETIC STRIPE

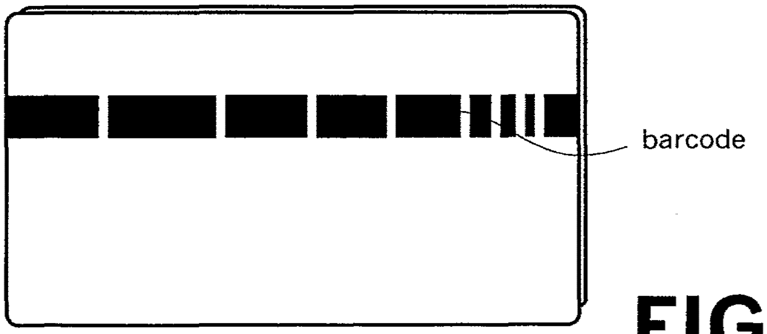


FIGURE 16C
ID CARD W/ BARCODE

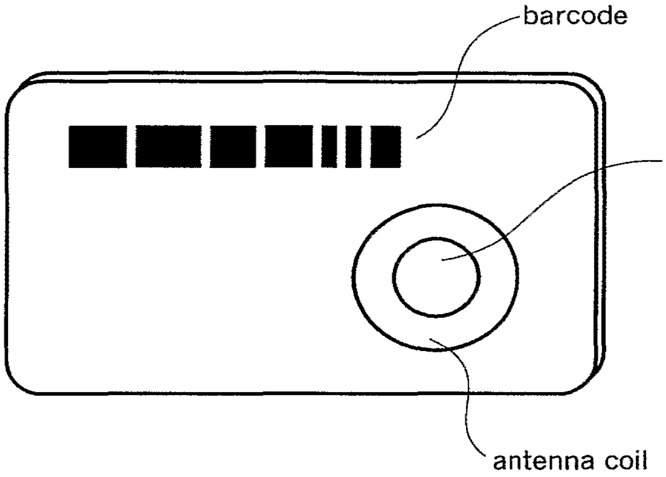


FIGURE 16D
ID CARD W/ TRANSPONDER AND BARCODE

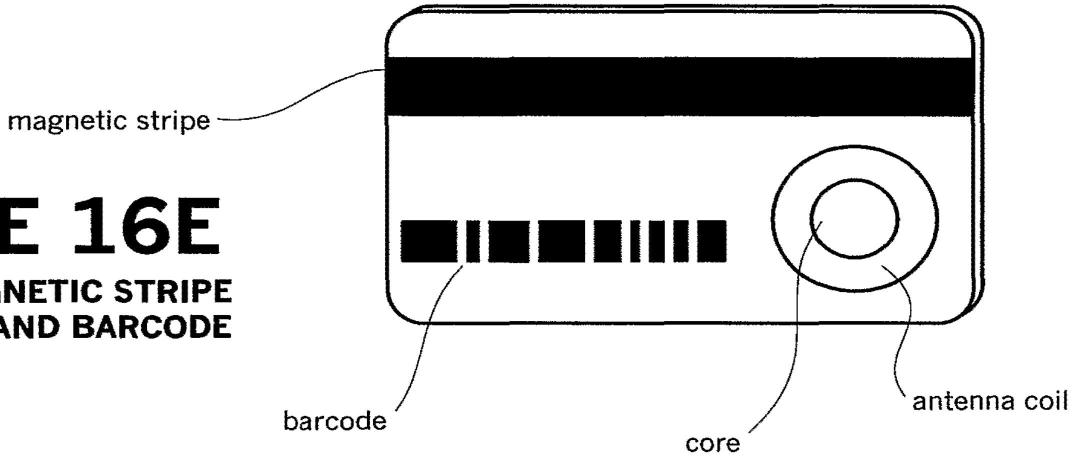


FIGURE 16E
ID CARD w/ MAGNETIC STRIPE TRANSPONDER AND BARCODE

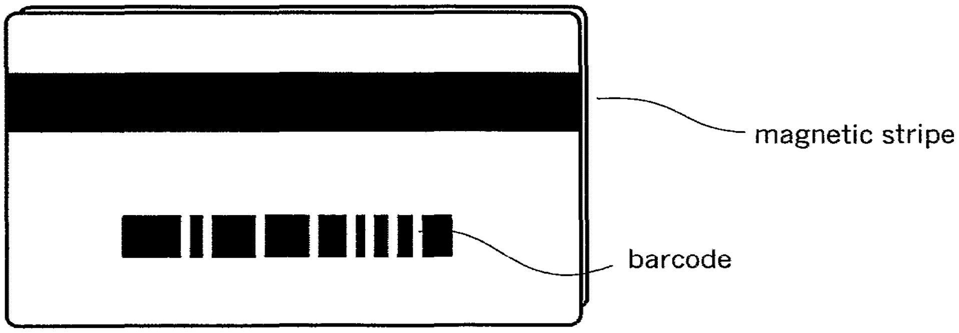


FIGURE 16F
ID CARD W/ MAGNETIC STRIPE AND BARCODE

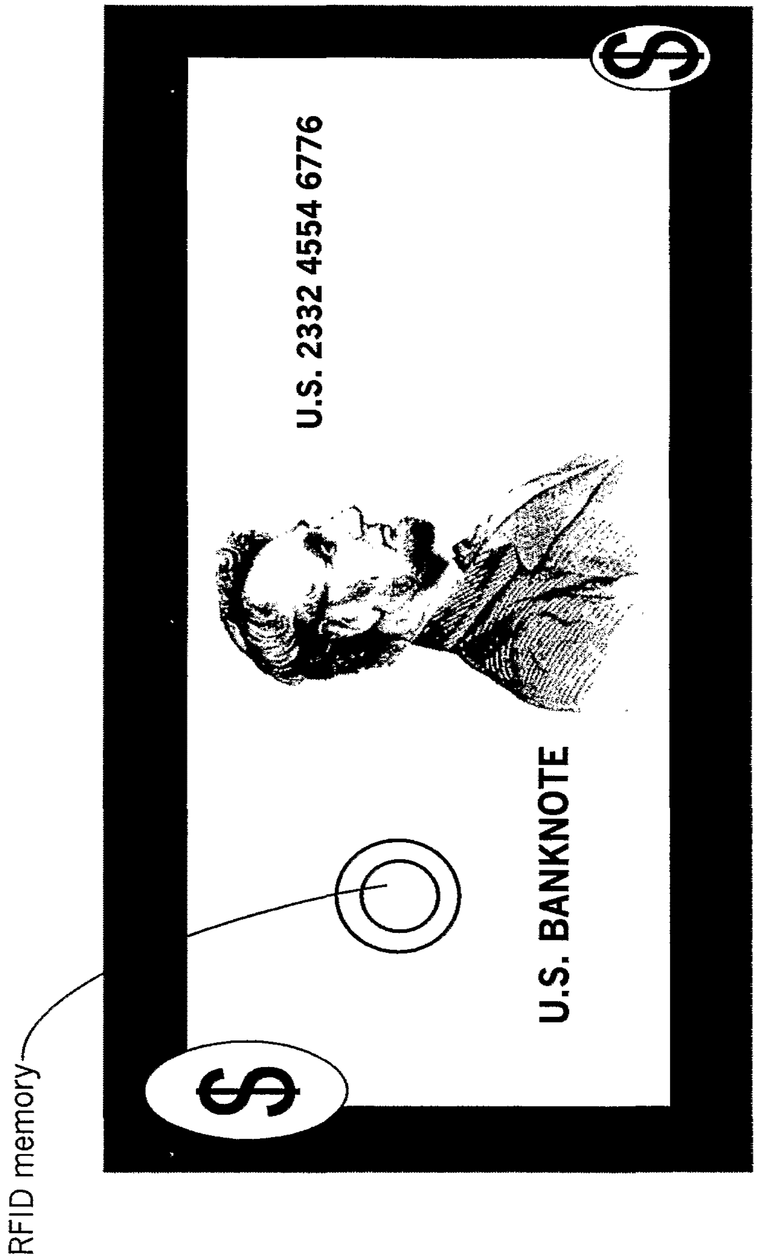


FIGURE 17
commercial paper w/ RFID element

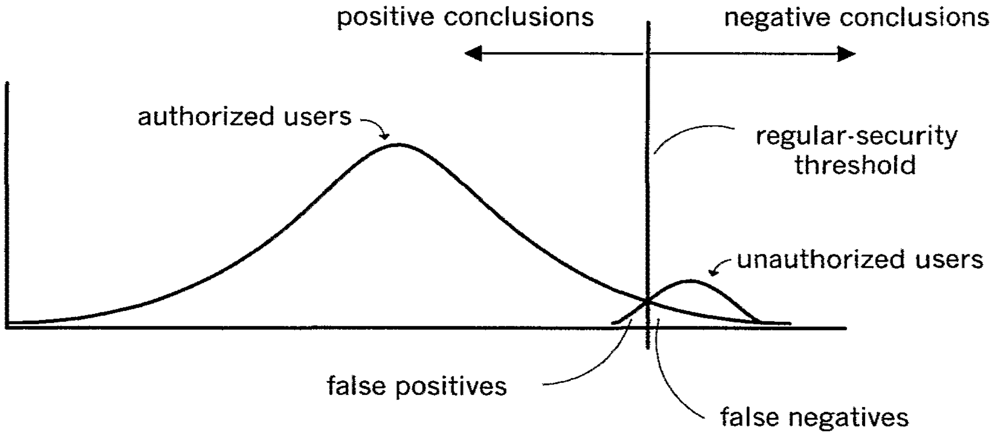


FIGURE 18A

REGULAR SECURITY

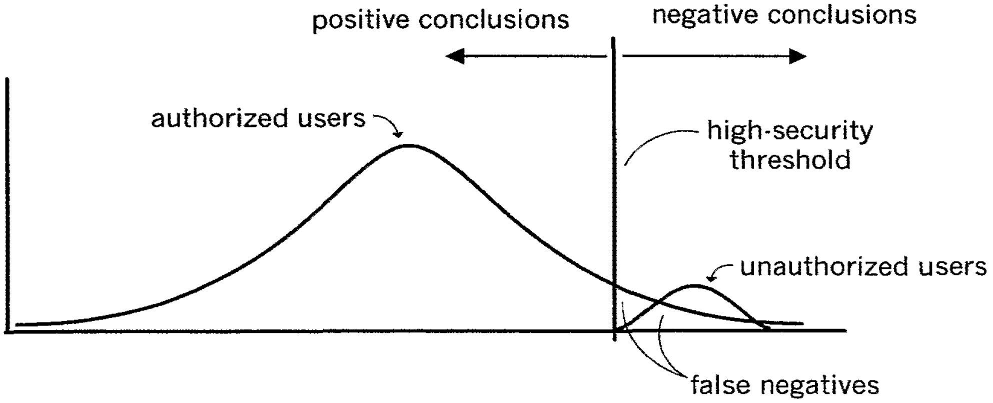


FIGURE 18B

HIGH SECURITY

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/16879

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/14
US CL : 713/202
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)
U.S. : 713/202,168,169,182-200;380/255,281,283;382/115,119,124

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5.892,824 A(BEATSON et al.) 06 April 1999 (06.04.1999), abstract, Fig.1-2, col. 5, lines 14-67 through col. 6, lines 1-64, col. 7, lines 15-39, col. 8, lines 40-52, lines 65-67 through col. 9, lines 1-45	1-10
Y	US 2002/0026419 A1 (MARITZEN et al.) 28 February 2002 (28/02/2002), absreact, pg. 3, paragraphs 39-41, 45-50, pg. 4, paragraphs 51-56, pg. 6, paragraphs 69-75.	1-10
Y	US 6,064,751 A (SMITHIES et al.) 16 May 2000 (16.05.2000), abstract, Figure 1, Fig. 3-3A Col. 7., lines 42-67 through col. 8, lines 1-6, claims 1-3.	1-10
Y	US 6,175,922 B1 (WANG) 16 January 2001 (16.01.2001), the entire document.	1-10

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 17 September 2002 (17.09.2002)	Date of mailing of the international search report 26 NOV 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C 20231 Facsimile No. (703)305-3230	Authorized officer Gail O Hayes Peggy Harrod Telephone No. (703) 305-4274

INTERNATIONAL SEARCH REPORT

PCT/US02/16879

Continuation of B. FIELDS SEARCHED Item 3:
WEST.ProQuest.Dialog. Dogpile; Search terms: access control. bimetric and (smart adj card or Identificat$4 adj card). ATM and stylus same (sens$5. Point-of- sale or POS and authenticat$4 or identificat$4 or fingureprint)

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Robert Dalton Summers
Attorney Docket Number:	12838/5 (729727US)

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Basic National Stage Fee	2631	1	155	155
Natl Stage Search Fee - Report provided	2642	1	205	205
Natl Stage Exam Fee - all other cases	2633	1	105	105
Pages:				
Claims:				
Independent claims in excess of 3	2614	3	105	315
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**780**

Electronic Acknowledgement Receipt

EFS ID:	2850361
Application Number:	12063650
International Application Number:	PCT/AU06/01136
Confirmation Number:	9949
Title of Invention:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	00757
Filer:	Robert Dalton Summers
Filer Authorized By:	
Attorney Docket Number:	12838/5 (729727US)
Receipt Date:	12-FEB-2008
Filing Date:	
Time Stamp:	18:04:37
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$780
RAM confirmation Number	2756
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional fees required under 37 CFR 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/Message Digest	Multi Part /.zip	Pages (if appl.)
1		128385app.pdf	2727318 27f147052411c1bb2ea0d0140763e51d492f85b0	yes	99

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal of New Application	1	2
Documents submitted with 371 Applications	3	39
Documents submitted with 371 Applications	40	48
Oath or Declaration filed	49	50
Information Disclosure Statement (IDS) Filed	51	52
Information Disclosure Statement (IDS) Filed	53	53
Foreign Reference	54	80
NPL Documents	81	83
NPL Documents	84	87
Preliminary Amendment	88	89
Claims	90	98
Applicant Arguments/Remarks Made in an Amendment	99	99

Warnings:

Information:

2	Foreign Reference	6861.pdf	2261957 91a3bf14e6488af5d491b41c2e5ba3d29902e228	no	62

Warnings:

Information:

3	Fee Worksheet (PTO-06)	fee-info.pdf	8543 cf36b54387579e9ea3ac7866d0c2aaa783b50816	no	2

Warnings:

Information:	
Total Files Size (in bytes):	4997818

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 12/063,650	Filing Date 08/12/2010	☒ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
□ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
□APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	02/12/2008	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X $105 =	0	OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	**0**	OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))									
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/NICHELE PETERSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/AU2006/001136

International filing date: 10 August 2006 (10.08.2006)

Document type: Certified copy of priority document

Document details: Country/Office: AU
Number: 2005904375
Filing date: 12 August 2005 (12.08.2005)

Date of receipt at the International Bureau: 22 August 2006 (22.08.2006)

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

WIPO
OMPI

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

PCT/AU2006/001136

Australian Government

Patent Office
Canberra

I, MICHELLE HENKEL, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2005904375 for a patent by SECURICOM (NSW) PTY LTD as filed on 12 August 2005.

...ALTH OF AUSTRALIA
...TENT OFFICE

WITNESS my hand this
Seventeenth day of August 2006

MHenkel

MICHELLE HENKEL
TEAM LEADER EXAMINATION
SUPPORT AND SALES

2005904375 12 Aug 2005

S&F Ref: 729727

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED:

Improving card device security using biometrics

Name and Address of Applicant:

Securicom (NSW) Pty Ltd,
an Australian company, ACN 053 874 089, of 48 Margate Street, Ramsgate,
New South Wales, 2217, Australia

Name of Inventor:

Christopher John Burke

This invention is best described in the following statement:

5805c

IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

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 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 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.

Another type of card device is the wireless "key-fob" which is a small radio transmitter that emits a radio frequency (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^{TM} 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.

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 input 801, for example by pressing their thumb against a biometric (eg 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 information 801. This is cumbersome and potentially compromises the privacy 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.

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, referred to as Biometric Card Pointer (BCP) 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.

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 defined by the ("unique") card information on the user's card as read by the card reader of the verification station. Clearly 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 someone submitting the aforementioned card requires the card user to submit both card to the card reader and a biometric signature, which is verified against the signature stored at the memory address defined by the card information.

Each use of the verification station is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature (eg thumb print or retinal scan etc.) to the biometric reader.

An authorised card user will be automatically verified by the BCP arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update etc. will simply proceed as normal. An unauthorised card user (ie a card user who misappropriated the card after the initial enrolment) will not receive authorisation, and the intended transaction will not proceed. Furthermore, the biometric signature of the unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user and prove misappropriation of the card.

The disclosed BCP arrangements require virtually no modification at all of the back-end systems or the (front-end) card. The additional administrative overheads associated with the BCP arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The BCP 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 BCP arrangements are implemented. Users of current card systems can learn to use BCP arrangements without much effort, needing only to provide a biometric signature when asked to do so at the verification station. The difference between the enrolment and verification phases are transparent to users, further reducing the effort in learning how to use the BCP arrangements.

According to a first aspect of the present invention, there is provided a method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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 BCP arrangements can be practiced;

Fig. 4 illustrates the biometric card pointer concept;

Fig. 5 is a flow chart of a process for using the biometric card pointer arrangement;

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; and

Fig. 9 shows an alternate use for the biometric card pointer arrangement.

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 disclosed BCP arrangements can be practiced. The disclosed BCP methods 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** and **9** may be implemented as software, such as a BCP application program executing within the computer system 100. In particular, the steps of the BCP processes are effected by instructions in the BCP 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 BCP software may also be divided into two separate parts, in which a first part performs the BCP methods and a second part manages a user interface between the first part and the user.

The BCP software may be stored in a computer readable medium, including the storage devices described below, for example. The BCP software is loaded into the verification station 127 from the computer readable medium, and 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 BCP 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 BCP 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 BCP 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 disclosed BCP approach the card data 604 acts 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 disclosed BCP system to determine if the card 601 is to be processed according to the disclosed BCP approach 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 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 memory 124 where their unique biometric signature is stored.

Thereafter, in later verification phases, the user couples their card 601 to the card reader 112, after which the card user is required to again present their unique biometric to the biometric reader 102. This signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112. Once verification is confirmed, the card information 605 is transferred from 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

2005904375 12 Aug 2005

disclosed BCP arrangement. 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 BCP arrangement 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 an inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Fig. 5 shows a process 200 for normal use of the BCP approach. 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 processes the card information 605 that is read from the card 601 by the card reader 112. 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 memory 124 in an earlier enrolment phase. It is also noted that the step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203. There is no need to search the database 124 to see if there is a match. Thus the disclosed BCP arrangement 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 contents 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 contents of the memory 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 contents 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 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.

2005904375 12 Aug 2005

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 signal 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**. The aforementioned step 401 can store the biometric signature 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. 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**.

2005904375 12 Aug 2005

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. 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. A separate, or overlapping, permitted card set is defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the BCP process at any given verification station 127. This has the advantage of ensuring that the local memory 124 does not overflow, and it also provides control over which users make use of which verification stations.

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 BCP 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 BCP system administrator. 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. 9 shows another application 900 to which the BCP arrangement 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 another example, the holder of the card 601 takes the card 601 and the portable verification station 127 to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card 601 is able to apply the card to the card reader 112, apply their biometric signature to the biometric reader 102, and have the verification station 127 output the corresponding card information 605. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card 601 is the authorised owner.

Industrial Applicability

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

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP 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.

Thus, for example, the BCP arrangement 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.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is fist issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room, negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP 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 disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement 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 **Fig. 5.**

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.

AUSTRALIA ONLY

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 securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

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

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

a smart card 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.

3. A method according to claim 1, wherein:

the method is performed in relation to a current verification cycle;

the steps (c), (d) and (e) are performed in relation to the current verification cycle.

4. A method according to claim 1, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

5. A method according to claim 1, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

6. A method according to claim 5, wherein the steps (db) and (eb) comprise the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

7. A method according to claim 1, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised.

8. A method according to any one of claims 5, 6 and 7 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.

9. A method according to claim 1, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

10. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

11. A verification station according to claim 10, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

12. A verification station according to claim 10, wherein the memory is incorporated in a tamper-proof manner in the verification station.

13. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. A method of securing a process substantially as described herein with reference to any one of the embodiments, as that embodiment is shown in the accompanying drawings.

15. A verification station for securing a process substantially as described herein with reference to any one of the embodiments, as that embodiment is shown in the accompanying drawings.

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 securing a process substantially as described herein with reference to any one of the embodiments, as that embodiment is shown in the accompanying drawings.

DATED this 12th Day of August 2005
SECURICOM (NSW) PTY LTD
Patent Attorneys for the Applicant
SPRUSON&FERGUSON

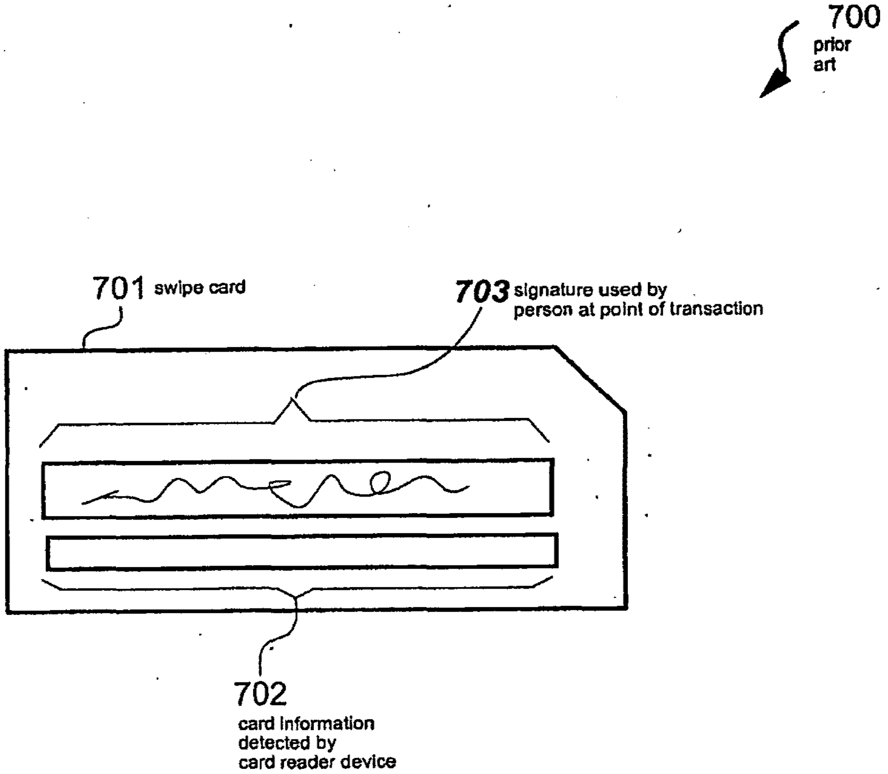
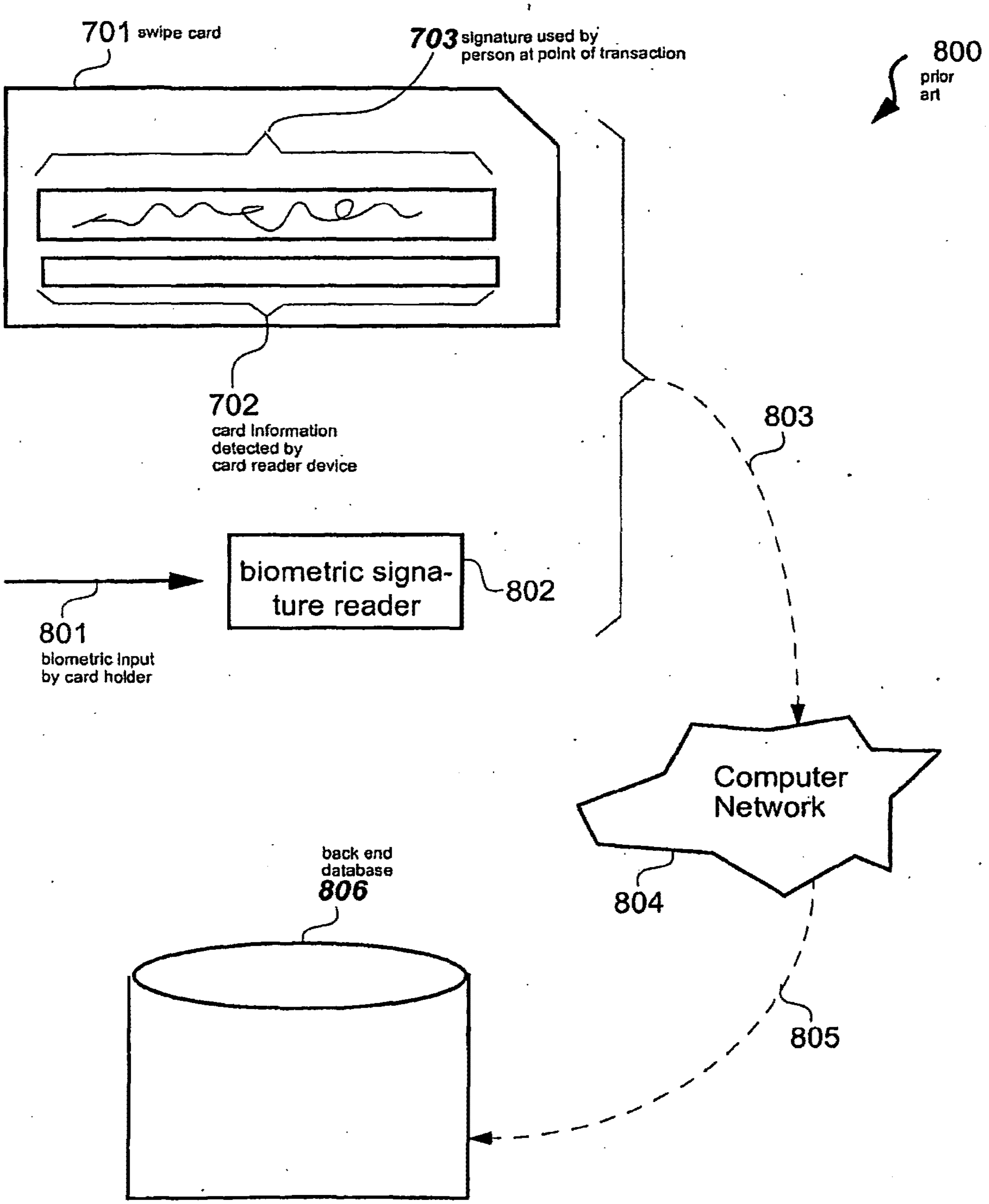


Fig. 1
prior art



701 swipe card
703 signature used by person at point of transaction
800 prior art
702 card information detected by card reader device
803
biometric signature reader
802
801 biometric input by card holder
Computer Network
804
back end database 806
805

Fig. 2
prior art

2005904375 12 Aug 2005

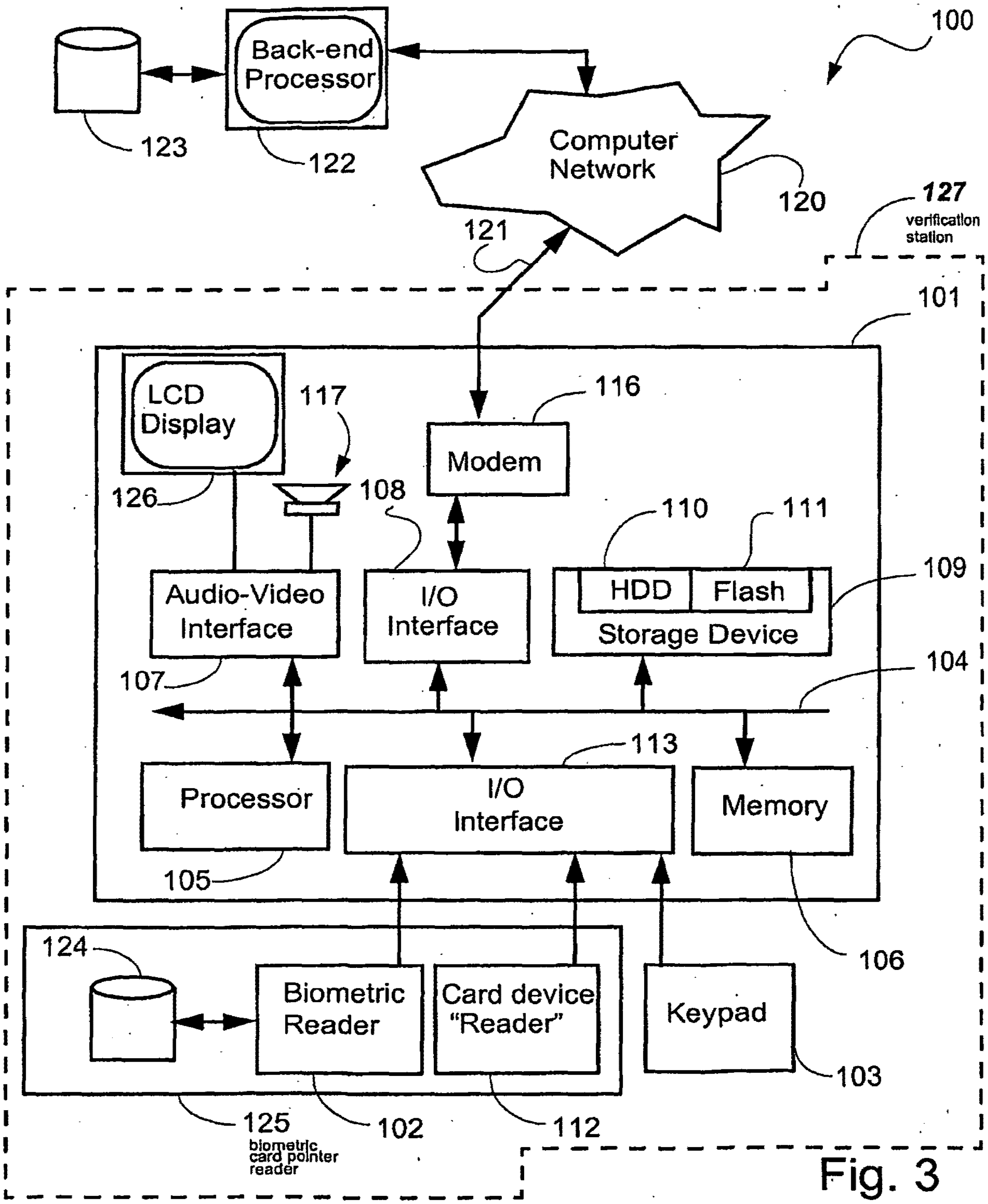


Fig. 3

2005904375 12 Aug 2005

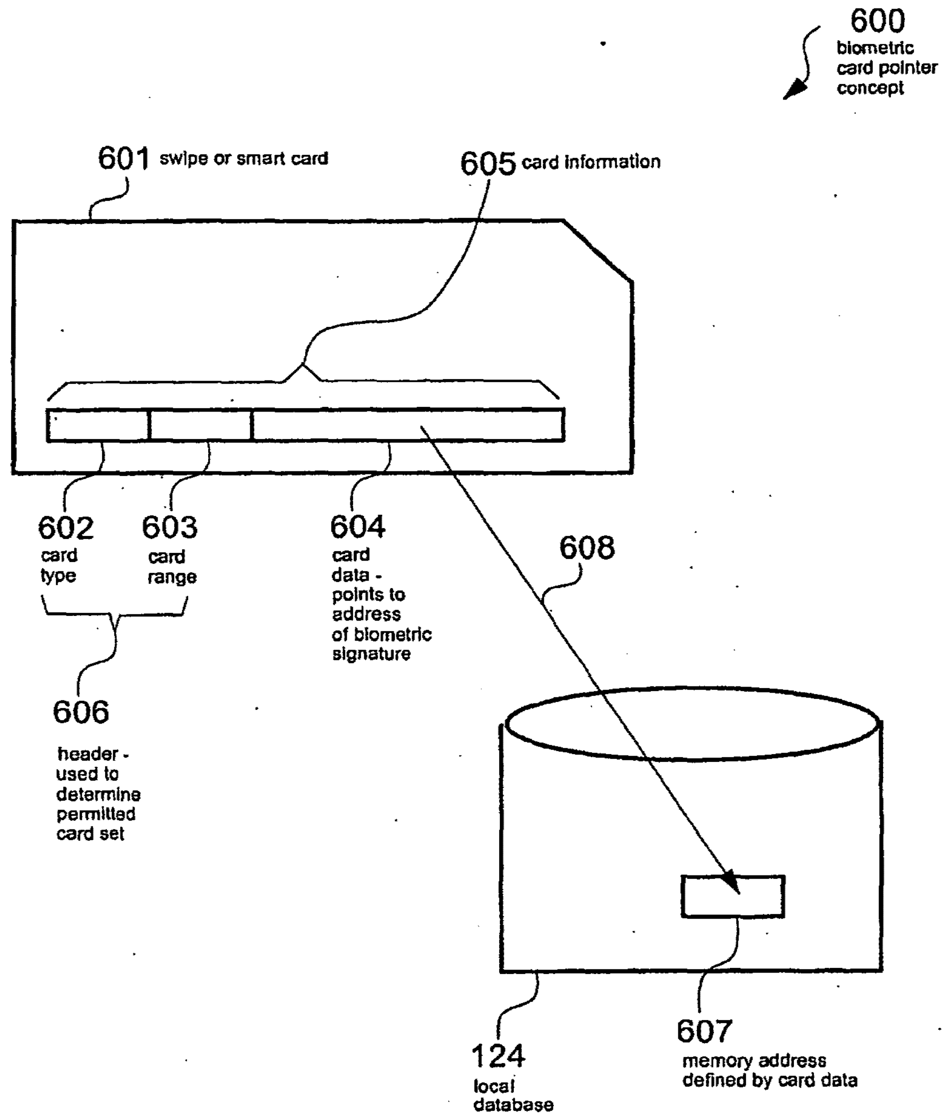


Fig. 4

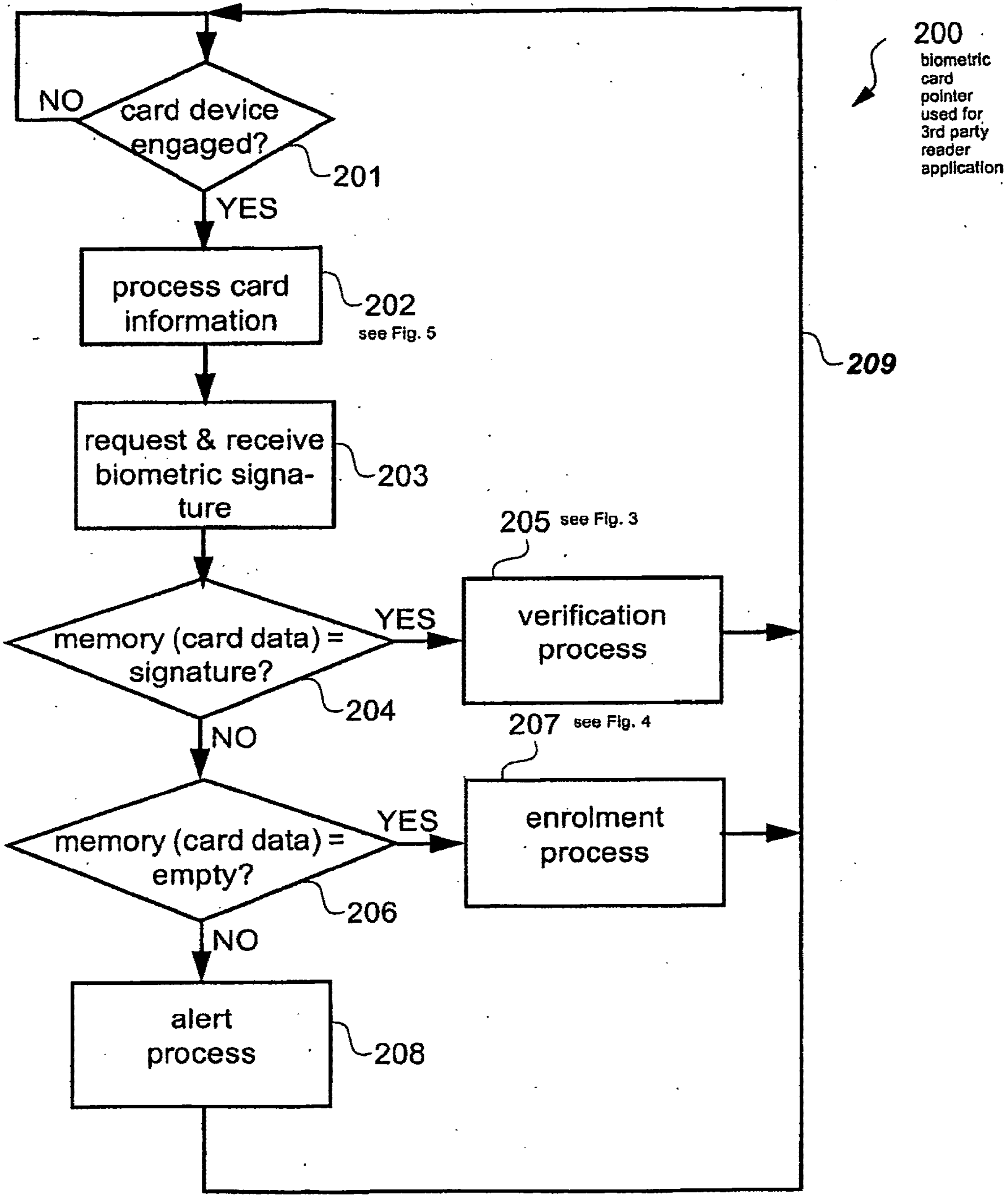

200
biometric card pointer used for 3rd party reader application
card device engaged?
NO
YES
201
process card information
202
see Fig. 5
request & receive biometric signature
203
memory (card data) = signature?
YES
NO
204
verification process
205 see Fig. 3
memory (card data) = empty?
YES
NO
206
enrolment process
207 see Fig. 4
alert process
208
209

Fig. 5

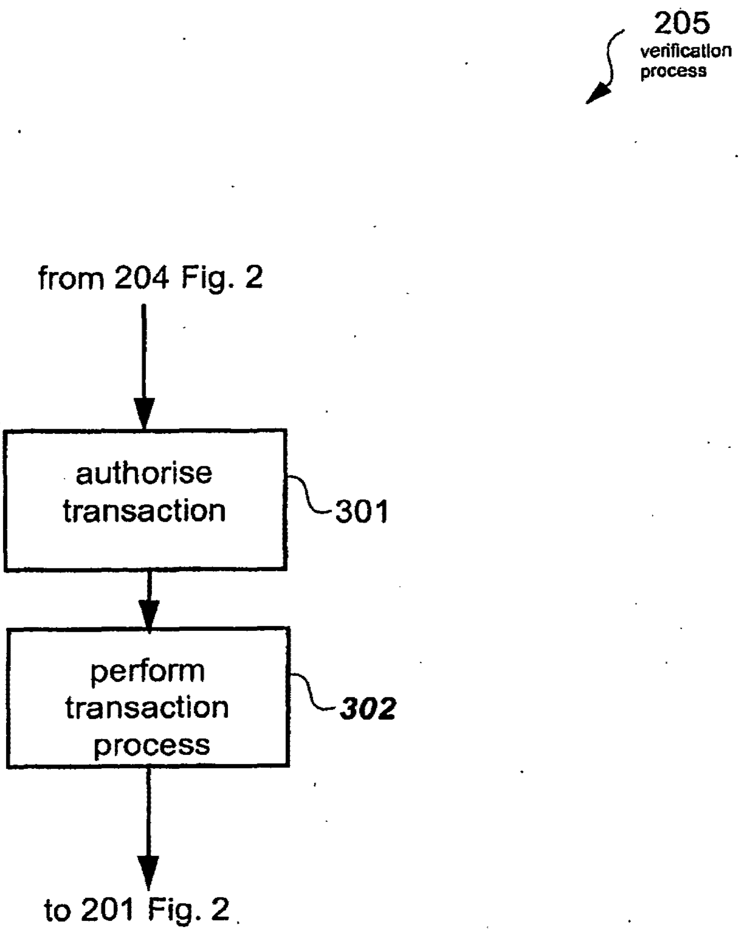

205
verification
process
from 204 Fig. 2
authorise
transaction
301
perform
transaction
process
302
to 201 Fig. 2

Fig. 6

2005904375 12 Aug 2005

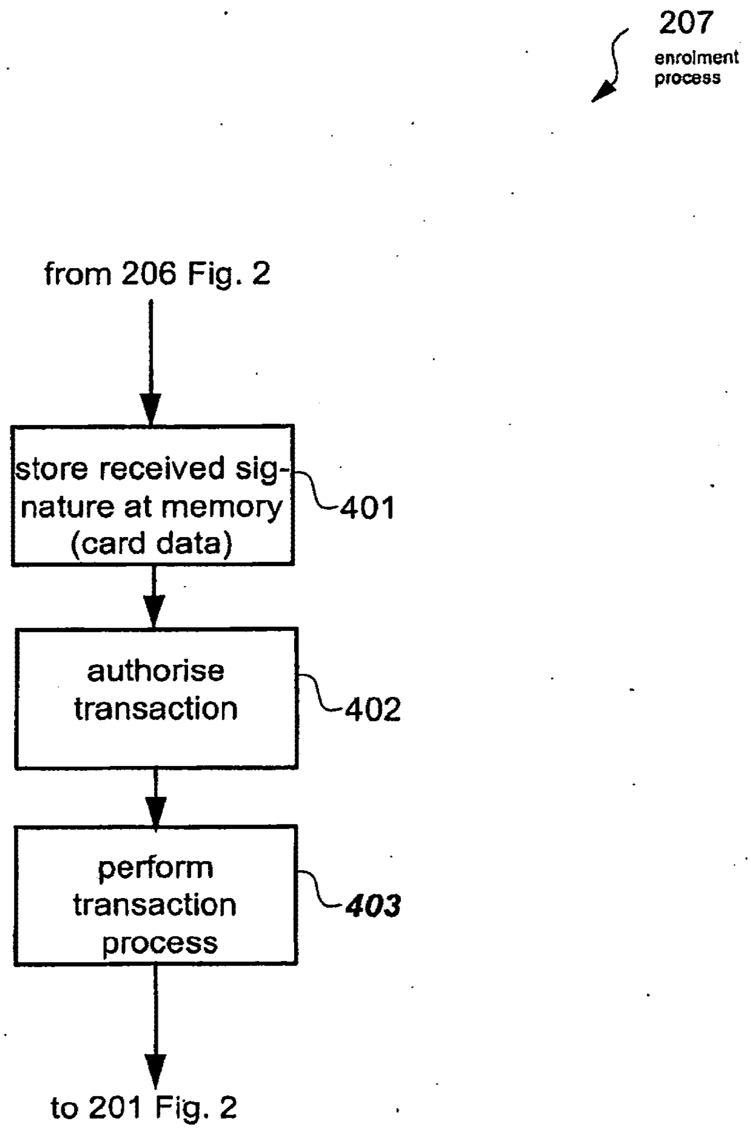


Fig. 7

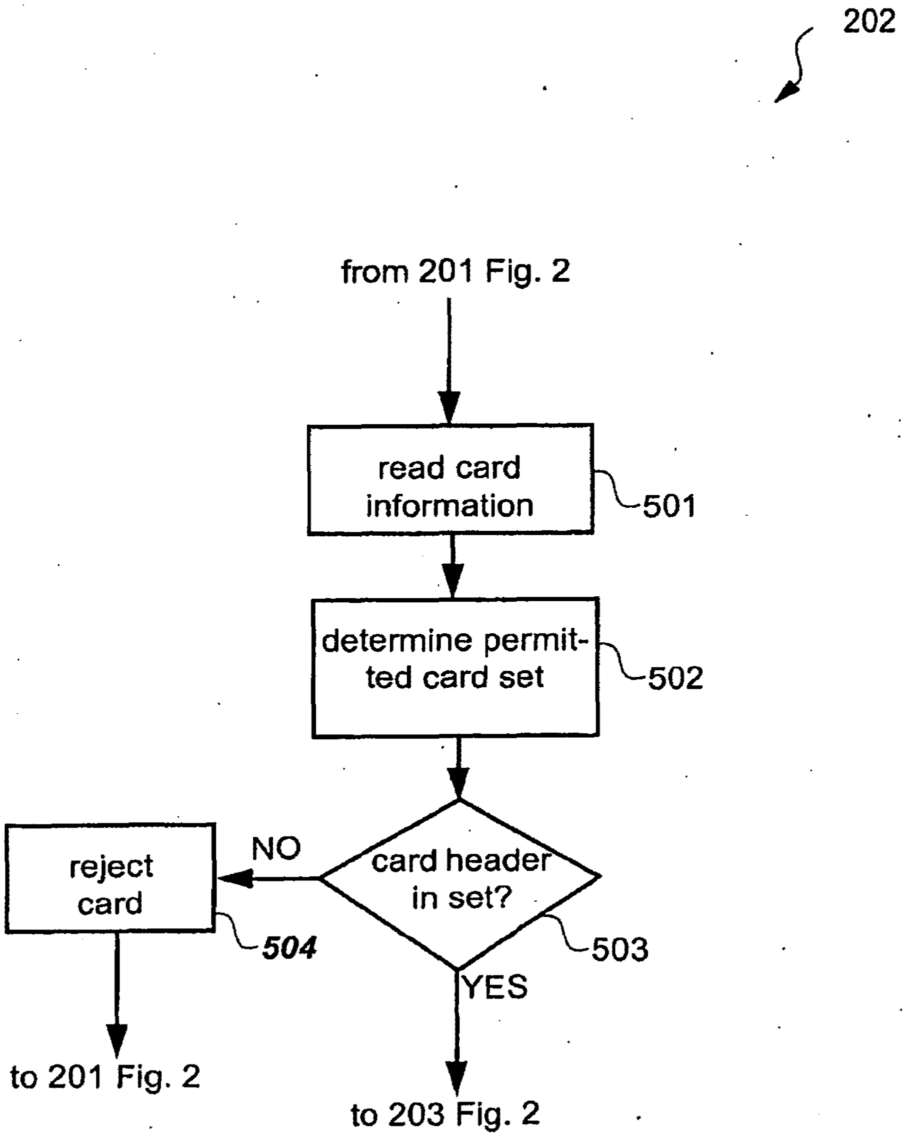

202
from 201 Fig. 2
read card information
501
determine permitted card set
502
card header in set?
503
NO
reject card
504
YES
to 201 Fig. 2
to 203 Fig. 2

Fig. 8

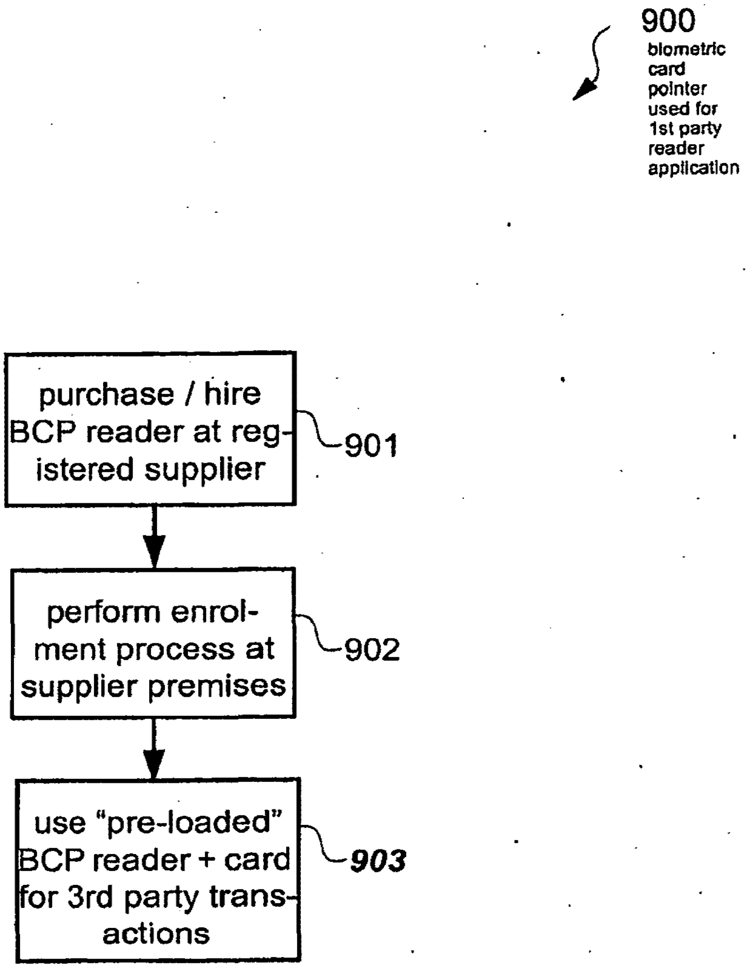

900
biometric card pointer used for 1st party reader application
purchase / hire BCP reader at registered supplier
901
perform enrolment process at supplier premises
902
use "pre-loaded" BCP reader + card for 3rd party transactions
903

Fig. 9

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/ AU2006 /001136
International Application No.

10 AUG 2006 (10.8.06)
International Filing Date

Australian Patent Office
PCT INTERNATIONAL APPLICATION
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 729727C

Box No. I TITLE OF INVENTION

Improving card device security using biometrics

Box No. II APPLICANT □ This person is also inventor.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)*

SECURICOM (NSW) PTY LTD
48 Margate Street
Ramsgate, NSW 2217
AUSTRALIA

Telephone No.

Facsimile No.

Teleprinter No.

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Australia

State *(that is. country)* of residence: Australia

This person is applicant for the purposes of: □ all designated States ☒ all designated States except the United states of America □ the United States of America only □ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (i.e. country) of residence if no State of residence is indicated below.)*

BURKE, Christopher John
48 Margate Street
Ramsgate, NSW 2217
AUSTRALIA

This person is :
□ applicant only
☒ applicant and inventor
□ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Australia

State *(that is, country)* of residence: Australia

This person is applicant for the purposes of: □ all designated States □ all designated States except the United states of America ☒ the United States of America only □ the States indicated in the Supplemental Box

□ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as : ☒ agent □ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country)*

SPRUSON & FERGUSON
GPO BOX 3898
Sydney
New South Wales 2001
AUSTRALIA

Telephone No.
+61 2 9207 0777

Facsimile No.
+61 2 9261 5486

Teleprinter No.

Agent's registration No. with the Office

□ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

See Notes to the request form

Box No. V DESIGNATIONS

The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.

However,

□ DE Germany is not designated for any kind of national protection

□ KR Republic of Korea is not designated for any kind of national protection

□ RU Russian Federation is not designated for any kind of national protection

(The check-boxes above may be used to exclude (irrevocably) the designations concerned in order to avoid the ceasing of the effect, under the national law, of an earlier national application from which priority is claimed. See the Notes to Box No V as the consequences of such national law provisions in these and certain other States.):

Box No. VI PRIORITY CLAIM

The priority of the following earlier application(s) is hereby claimed:

Filing date of earlier application *(day/month/year)*	Number of earlier application	Where earlier application is:		
		national application: country or Member of WTO	regional application:* regional Office	international application: receiving Office
Item (1) (12.8.05)▲ 12 August 2005	2005904375	Australia		

□ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

□ all items ☒ item(1) □ item(2) □ item(3) □ other, see Supplemental Box

* *Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):*

....

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(If two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):*

ISA/ AU ▲

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*

Date (day/month/year) Number Country (or regional Office)

Box No VIII DECLARATIONS

The following **declarations** are contained in Boxes Nos VIII(I) to (v) *(mark the applicable check-boxes below and indicated in the right column the number of each type of declaration):* Number of declarations

□ Box No. VIII(i) Declaration as to the identity of the inventor :

□ Box No VIII(ii) Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent :

□ Box No VIII(iii) Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application :

□ Box No VIII(iv) Declaration of inventorship (only for the purposes of the designation of the United States of America) :

□ Box No VIII(v) Declaration as to non-prejudicial disclosures or exceptions to lack of novelty :

▲ INSERTED

Sheet No. 3

Box No. IX CHECK LIST; LANGUAGE OF FILING

This international application **contains:**

(a) **in paper form,** the following number of sheets:

request (including declaration sheets)	:	3
description (excluding sequence listing and/or tables related thereto)	:	21
claims	:	7
abstract	:	1
drawings	:	7
Sub-total number of sheets	:	39
sequence listing	:	0
tables related thereto	:	0
(for both, actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (c) below)		
Total number of sheets	:	39

(b) **only in computer readable form** (Section 801(a)(i))

(i) □ sequence listing

(ii) □ tables related thereto

(c) **also in computer readable form** (Section 801(a)(ii))

(i) □ sequence listing

(ii) □ tables related thereto

Type and number of carriers (diskette, CD-ROM, CD-R or other) on which are contained the:

□ sequence listing:

□ tables related thereto:

(additional copies to be indicated under items 9(ii) and/or 10(ii), in right column)

This international application is **accompanied** by the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item):*

		Number of items
1. ☒ fee calculation sheet	:	1
2. □ original separate signed power of attorney	:	
3. □ original general power of attorney	:	
4. □ copy of general power of attorney; reference number, if any:	:	
5. □ statement explaining lack of signature	:	
6. □ priority document(s) identified in Box No. VI as item(s):	:	
7. □ translation of international application into (*language*):	:	
8. □ separate indications concerning deposited microorganism or other biological material	:	
9. □ sequence listing in computer readable form *(indicate type and number of carriers)*		
(i) □ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application)	:	
(ii) □ *(only where check-box (b)(i) or (c)(i) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter*	:	
(iii) □ together with relevant statement as to the identity of the copy or copies with the sequence listing mentioned in left column	:	
10. □ tables in computer readable form related to sequence listing *(indicate type and number of carriers*		
(i) □ copy submitted for the purposes of international search under Section 802 (b-*quarter*) only (and not as part of the international application)	:	
(ii) □ *(only where check-box (b)(ii) or (c)(ii) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Section 802 (b-*quarter*)	:	
(iii) □ together with relevant statement as to the identity of the copy or copies with the tables mentioned in left column	:	
11. □ other (*specify*):	:	

Figure of the drawings which should accompany the abstract: 4

Language of filing of the international application: English

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Paul Massey
Registered Patent Attorney
SPRUSON & FERGUSON

For receiving Office use only

1.	Date of actual receipt of the purported international application:	10 AUG 2006 (10.8.06)	
3.	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:		2. Drawings
4.	Date of timely receipt of the required corrections under PCT Article 11(2):		☒ received:
5.	International Searching Authority (if two or more are competent): ISA/	6. □ Transmittal of search copy delayed until search fee is paid	□ not received:

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

See Notes to the request form

[R:\LIBW]69133.doc:VSG

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

SPRUSON & FERGUSON
GPO Box 3998
Sydney, NSW 2001
AUSTRALIE

Date of mailing *(day/month/year)* 18 September 2006 (18.09.2006)	
Applicant's or agent's file reference 729727C	**IMPORTANT NOTIFICATION**
International application No. PCT/AU2006/001136	International filing date *(day/month/year)* 10 August 2006 (10.08.2006)
International publication date *(day/month/year)* **Not yet published**	Priority date *(day/month/year)* 12 August 2005 (12.08.2005)
Applicant SECURICOM (NSW) PTY LTD et al	

1. By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. *(If applicable)* The **letters "NR"** appearing in the right-hand column denote **a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau** under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

3. *(If applicable)***An asterisk (*)** appearing next to a date of receipt, in the right-hand column, denotes **a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b)** (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
12 August 2005 (12.08.2005)	2005904375	AU	22 August 2006 (22.08.2006)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Dorothée Mülhausen Facsimile No. +41 22 338 87 40 Telephone No. +41 22 338 96 72

(12) International Application Status Report

Received at International Bureau: 22 August 2006 (22.08.2006)

Information valid as of: Not available
Report generated on: 21.07.2010

(10) Publication number: WO2007/019605	**(43) Publication date:** 22 February 2007 (22.02.2007)	**(26) Publication language:** English (EN)
(21) Application Number: PCT/AU2006/001136	**(22) Filing Date:** 10 August 2006 (10.08.2006)	**(25) Filing language:** English (EN)
(31) Priority number(s): 2005904375 (AU)	**(31) Priority date(s):** 12 August 2005 (12.08.2005)	**(31) Priority status:** Priority document received (in compliance with PCT Rule 17.1)

(51) International Patent Classification:
G07F 7/10 (2006.01); **G07F 19/00** (2006.01); **G06K 9/00** (2006.01); **G07F 7/12** (2006.01)

(71) Applicant(s):
SECURICOM (NSW) PTY LTD [AU/AU]; 48 Margate Street Ramsgate, NSW 2217 (AU) *(for all designated states except US)*
BURKE, Christopher, John [AU/AU]; 48 Margate Street Ramsgate, NSW 2217 (AU) *(for US only)*

(72) Inventor(s):
BURKE, Christopher, John; 48 Margate Street Ramsgate, NSW 2217 (AU)

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

(54) Title (EN): IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

(54) Title (FR): AMELIORATION DE LA SECURITE D'UN DISPOSITIF A CARTE AU MOYEN DE LA BIOMETRIE

(57) Abstract:

(EN): The disclosed Biometric Card Pointer arrangements store (207) a card user's biometric signature in a local memory (124) in a verification station (127) the first time the card user uses the verification station (127) in question. The biometric signature is stored at a memory address (607) defined by the card information (605) on the user's card (601). All future uses of the particular verification station (127) by someone submitting the aforementioned card (601) requires 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 (605) thereby determining if the person submitting the card is authorised to do so.

(FR): Les dispositifs de pointeur de carte biométrique de cette invention permettent de stocker (207) une signature biométrique d'un utilisateur de carte dans une mémoire locale (124) d'un poste de vérification (127), la première fois que ledit utilisateur utilise ledit poste de vérification (127) en question. Cette signature biométrique est stockée au niveau d'une adresse de mémoire (607) définie par les informations de carte (605) sur ladite carte d'utilisateur (601). Toutes les utilisations futures du poste de vérification spécifique (127) par une personne présentant la carte susmentionnée (601) requièrent que ledit utilisateur de carte présente la carte et une signature biométrique qui est vérifiée avec à la signature stockée à l'adresse de mémoire définie par les informations de carte (605), ce qui permet de déterminer si la personne présentant la carte est autorisée à le faire.

International search report:
Received at International Bureau: 24 October 2006 (24.10.2006) [AU]

International preliminary examination report:
Chapter II demand received: 12 June 2007 (12.06.2007)

(81) Designated States:

AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW
European Patent Office (EPO) : AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR
African Intellectual Property Organization (OAPI) : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG
African Regional Intellectual Property Organization (ARIPO) : BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW
Eurasian Patent Organization (EAPO) : AM, AZ, BY, KG, KZ, MD, RU, TJ, TM

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2007 (22.02.2007)

PCT

(10) International Publication Number
WO 2007/019605 A1

(51) International Patent Classification:
G07F 7/10 (2006.01) *G06K 9/00* (2006.01)
G07F 19/00 (2006.01) *G07F 7/12* (2006.01)

(21) International Application Number: PCT/AU2006/001136

(22) International Filing Date: 10 August 2006 (10.08.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2005904375 12 August 2005 (12.08.2005) AU

(71) Applicant *(for all designated States except US)*: **SECURICOM (NSW) PTY LTD** [AU/AU]; 48 Margate Street, Ramgate, NSW 2217 (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).

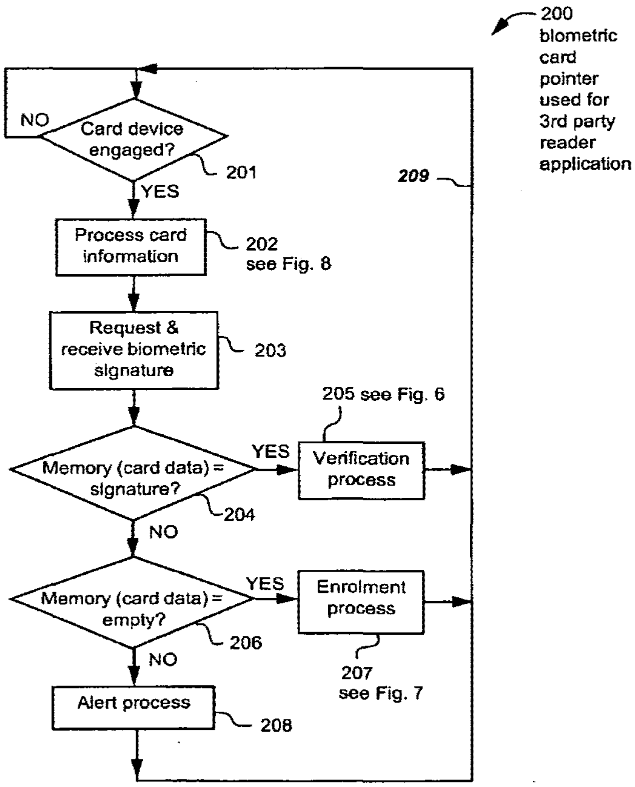
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ,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

Published:
— *with international search report*

[Continued on next page]

(54) Title: IMPROVING CARD DEVICE SECURITY USING BIOMETRICS



(57) **Abstract:** The disclosed Biometric Card Pointer arrangements store (207) a card user's biometric signature in a local memory (124) in a verification station (127) the first time the card user uses the verification station (127) in question. The biometric signature is stored at a memory address (607) defined by the card information (605) on the user's card (601). All future uses of the particular verification station (127) by someone submitting the aforementioned card (601) requires 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 (605) thereby determining if the person submitting the card is authorised to do so.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

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 secure access purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account 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 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.

Another type of card device is the wireless "key-fob" which is a small radio transmitter that emits a radio frequency (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^{TM} 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.

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 input 801, for example by pressing their thumb against a biometric (eg 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 information 801. This is cumbersome and potentially compromises the privacy 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.

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, referred to as Biometric Card Pointer (BCP) arrangements or systems, which seek to address the above problems relating to secure access and/or secure processes, 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.

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 defined by the ("unique") card information on the user's card as read by the card reader of the verification station. Clearly 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 someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, 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.

Each use of the verification station is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature (eg thumb print or retinal scan etc.) to the biometric reader.

An authorised card user will be automatically verified by the BCP arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update etc. will simply proceed as normal. An unauthorised card user (ie a card user who misappropriated the card after the initial enrolment) will not receive authorisation, and the intended transaction will not proceed. Furthermore, the biometric signature of the unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user and prove misappropriation of the card.

The disclosed BCP arrangements require little if any modification of the back-end systems or the (front-end) card. The additional administrative overheads associated with the BCP arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The BCP 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 BCP arrangements are implemented. Users of current card systems can learn to use BCP arrangements without much effort, needing only to provide a biometric signature when asked to do so at the verification station. The difference between the enrolment and verification phases are transparent to users, further reducing the effort in learning how to use the BCP arrangements.

According to a first aspect of the present invention, there is provided a method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature; and

storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to another aspect of the present invention, there is provided a method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the noted enrolment method;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

According to another aspect of the present invention, there is provided a method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to 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 of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature; and

code for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to 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 of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the noted enrolment method;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

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 BCP arrangements can be practiced;

Fig. 4 illustrates the biometric card pointer concept;

Fig. 5 is a flow chart of a process for using the biometric card pointer arrangement;

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; and

Fig. 9 shows an alternate use for the biometric card pointer arrangement.

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 disclosed BCP arrangements can be practiced. The disclosed BCP methods 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** and **9** may be implemented as software, such as a BCP application program executing within the computer system 100. In particular, the steps of the BCP processes are effected by instructions in the BCP 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 BCP software may also be divided into two separate parts, in which a first part performs the BCP methods and a second part manages a user interface between the first part and the user.

The BCP software may be stored in a computer readable medium, including the storage devices described below, for example. The BCP software is loaded into the verification station 127 from the computer readable medium, and 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 èffecting the BCP arrangements.

The verification station 127 comprises, in the described arrangement, a biometric card pointer reader 125, a keypad 103, and a computer module 101. The biometric card pointer reader is made up of a biometric reader 102, a card device reader 112 and a local database 124.

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 BCP 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 BCP 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. The card information 605 can be encoded using a magnetic strip, a bar code, or a solid state memory on the card 601. Alternately, the card device can be implemented as a wireless key fob. In one example of the disclosed BCP approach, the card data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an 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 disclosed BCP system to determine if the card 601 is to be processed according to the disclosed BCP approach or not. This is described in more detail in regard to **Fig. 8**. Alternately, any segment of the card information 605 can be used as the memory reference which points to the particular memory location in the local database 124.

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 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 memory 124 where their unique biometric signature is stored.

Thereafter, in later verification phases, the user couples their card 601 to the card reader 112, after which the card user is required to again present their unique biometric to the biometric reader 102. This signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112. Once verification is confirmed, the card information 605 is transferred from 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 disclosed BCP arrangement. 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 BCP arrangement 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 an inexpensive upgrade compared to the centralised arrangement depicted in **Fig. 2**.

Fig. 5 shows a process 200 for normal use of the BCP approach. 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 processes the card information 605 that is read from the card 601 by the card reader 112. 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 memory 124 in an earlier enrolment phase. It is also noted that the step 204 reads the contents stored at a single memory address defined by the card data 604 and checks these contents against the biometric signature received in the step 203. There is no need to search the entire database 124 to see if there is a match. Thus the disclosed BCP arrangement provides a particularly simple and fast biometric verification check thereby securing the process associated with the step 205. Once the step 205 has completed the verification process, the process 200 is directed according to an arrow 209 back to the step 201.

In an alternate arrangement, the card data 604 can be associated with a group of memory locations, rather than being the address for a specific memory location. This arrangement allows a different biometric signature to be stored in each of the group of memory locations, and in this case, the step 204 reads the contents stored in each memory location in the group defined by the card data 604, and checks the contents of each memory location in the group against the biometric signature received in the step 203. If the contents of any member of the group of memory locations matches, 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. This arrangement allows, for example, two cards having the same card data 604 to be used at the same verification station 127 after each card holder performs their own individual enrolment process.

Returning to the step 204, if the contents 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 contents of the memory 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 contents 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 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, and can capture the card in the verification station 127, thereby removing the card from the possession of the apparently unauthorised person.

The alert process 208 can send, as part of the alert message, send all or part of the card information 605 that is input to the verification station 127 in the step 201 of **Fig. 5**.

Although in the above description the step 206 tests if the memory location defined by the card data 604 is "empty", other approaches can be used. Thus when enrolment is performed, resulting in a memory location being used to store a biometric signature (eg see step 401 in **Fig. 7**), a flag can be set to indicate that the memory location in question is occupied. The term "occupied" in this context means that the memory location in question has been used in the enrolment process for a user, and that the information stored at the memory location in question has not been deleted by a BCP system administrator. If the signature stored in the database 124 at the particular memory location is deleted by a BCP system administrator (as described in regard to **Fig. 8**) then the flag can be reset to indicate that the memory location in question is no longer occupied.

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 signal 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 (which may be viewed as a process of obtaining verified access to a protected resource), whatever that may be. Thus, for example, if the process 200 of **Fig. 5** relates withdrawal of cash from an Automatic Teller Machine (ATM) operated by one of a number of service providers, 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**. The aforementioned step 401 can store the biometric signature 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. 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. 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. A separate, or overlapping, permitted card set is defined for each verification station 127. This ensures that a limited population of cards such as 601 undergo the BCP process at any given verification station 127. This has the advantage of ensuring that the local memory 124 does not overflow, and it also provides control over which users make use of which verification stations.

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 set of permitted cards 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 BCP 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 BCP system administrator. 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. 9 shows another application 900 to which the BCP arrangement 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 another example, the holder of the card 601 takes the card 601 and the portable verification station 127 to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card 601 is able to apply the card to the card reader 112, apply their biometric signature to the biometric reader 102, and have the verification station 127 output the corresponding card information 605. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card 601 is the authorised owner.

Industrial Applicability

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

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP 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.

Thus, for example, the BCP arrangement 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.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is fist issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room; negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP 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 disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement 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 **Fig. 5.**

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.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature; and

storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

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

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

a smart card 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.

5. A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised.

9. A method according to any one of claims 6, 7 and 8 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.

10. A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader receiving the biometric signature; and

means for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

12. A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

13. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature; and

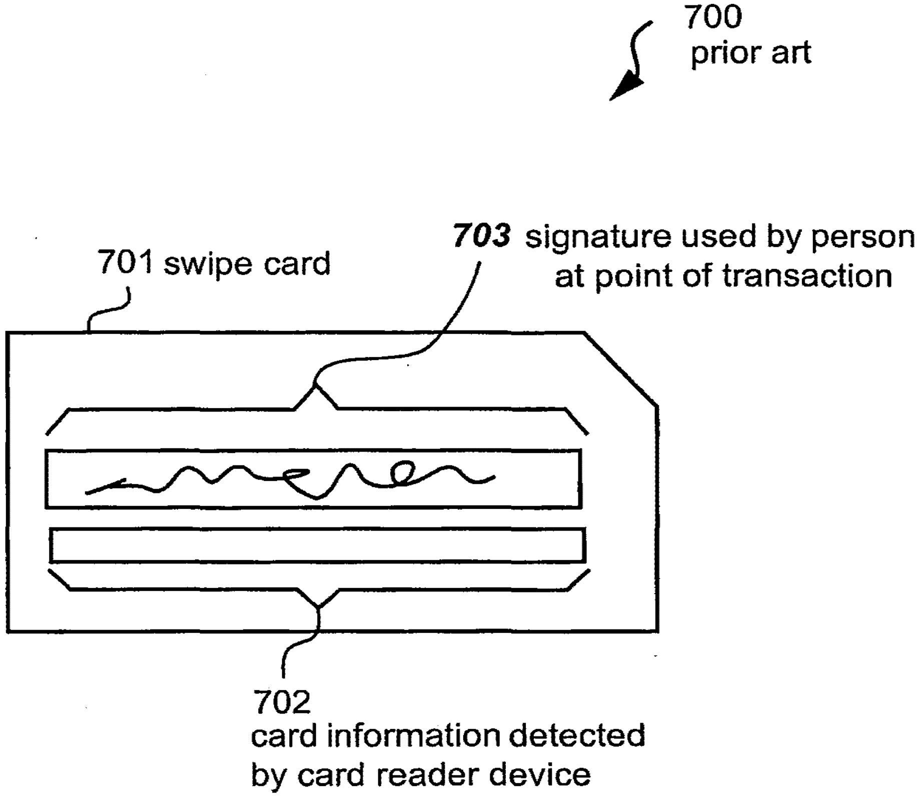
code for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

18. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.



700
prior art
701 swipe card
703 signature used by person at point of transaction
702
card information detected by card reader device

Fig. 1
prior art

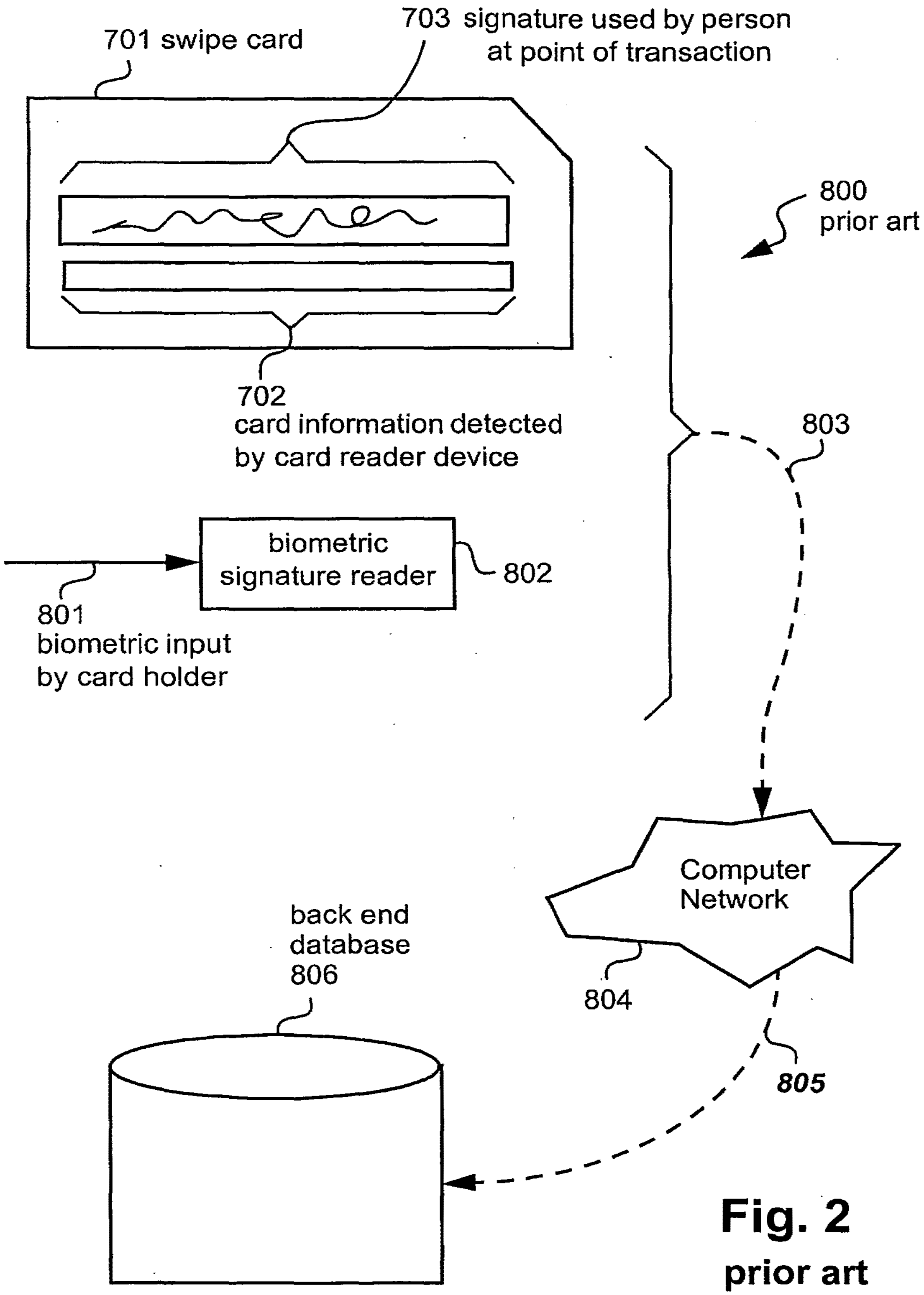

701 swipe card
703 signature used by person at point of transaction
800 prior art
702 card information detected by card reader device
803
biometric signature reader
802
801 biometric input by card holder
Computer Network
back end database 806
804
805

Fig. 2
prior art

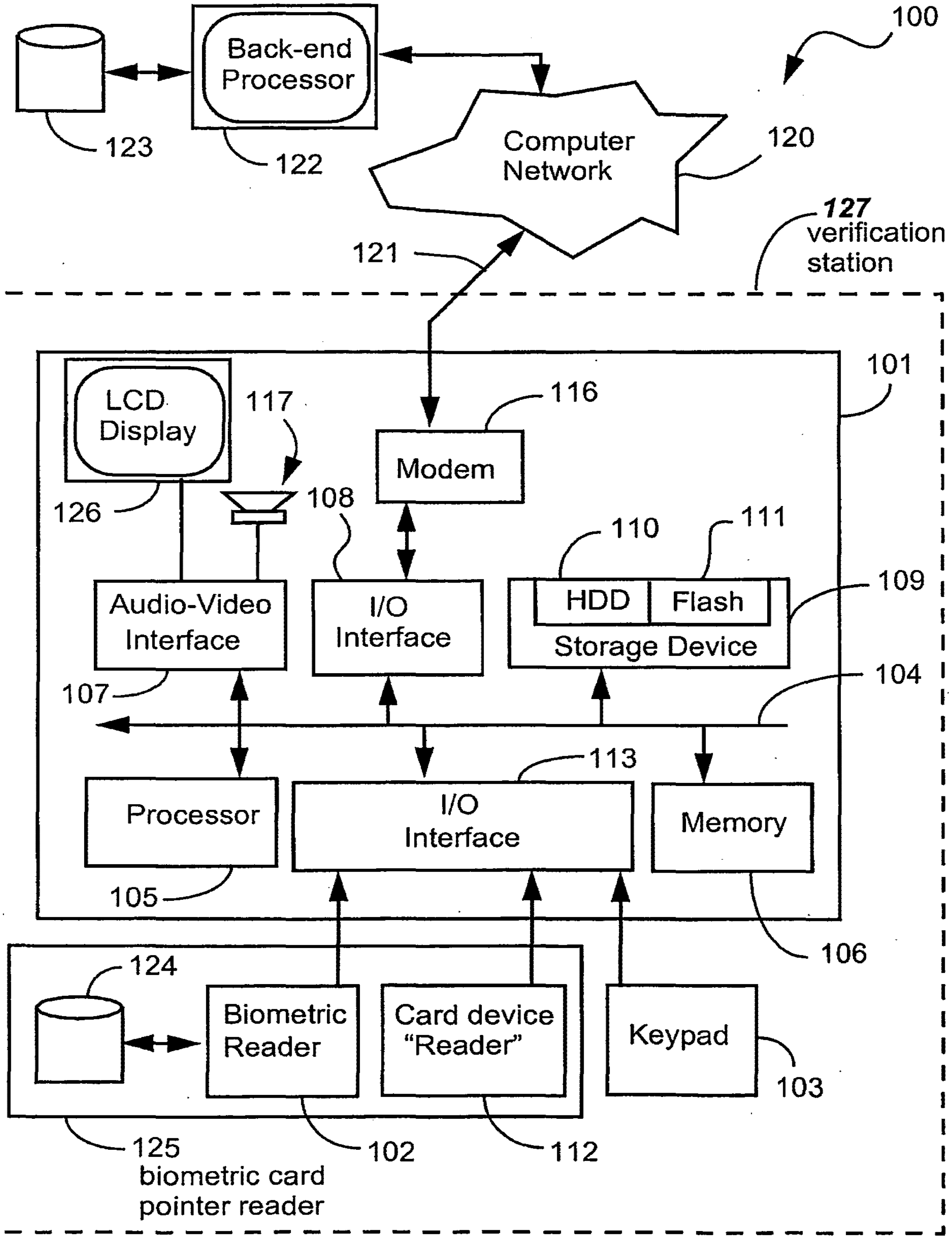

Back-end
Processor
123
122
100
Computer
Network
120
127
verification
station
121
101
LCD
Display
117
116
Modem
126
108
110
111
109
HDD
Flash
Audio-Video
Interface
I/O
Interface
Storage Device
104
107
113
Processor
I/O
Interface
Memory
105
106
124
Biometric
Reader
Card device
"Reader"
Keypad
103
125
biometric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

Fig. 3

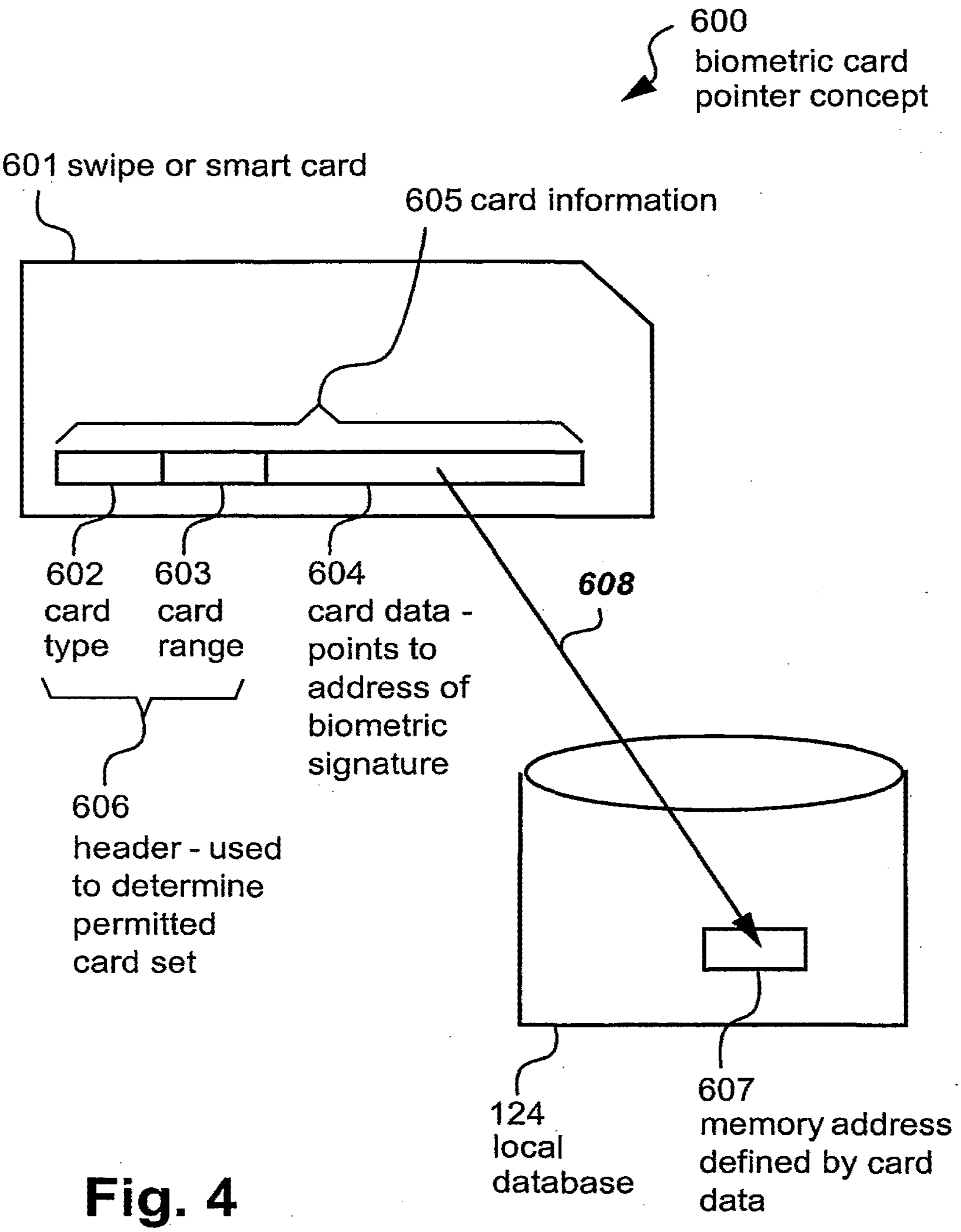

600
biometric card
pointer concept
601 swipe or smart card
605 card information
602
card
type
603
card
range
604
card data -
points to
address of
biometric
signature
608
606
header - used
to determine
permitted
card set
124
local
database
607
memory address
defined by card
data

Fig. 4

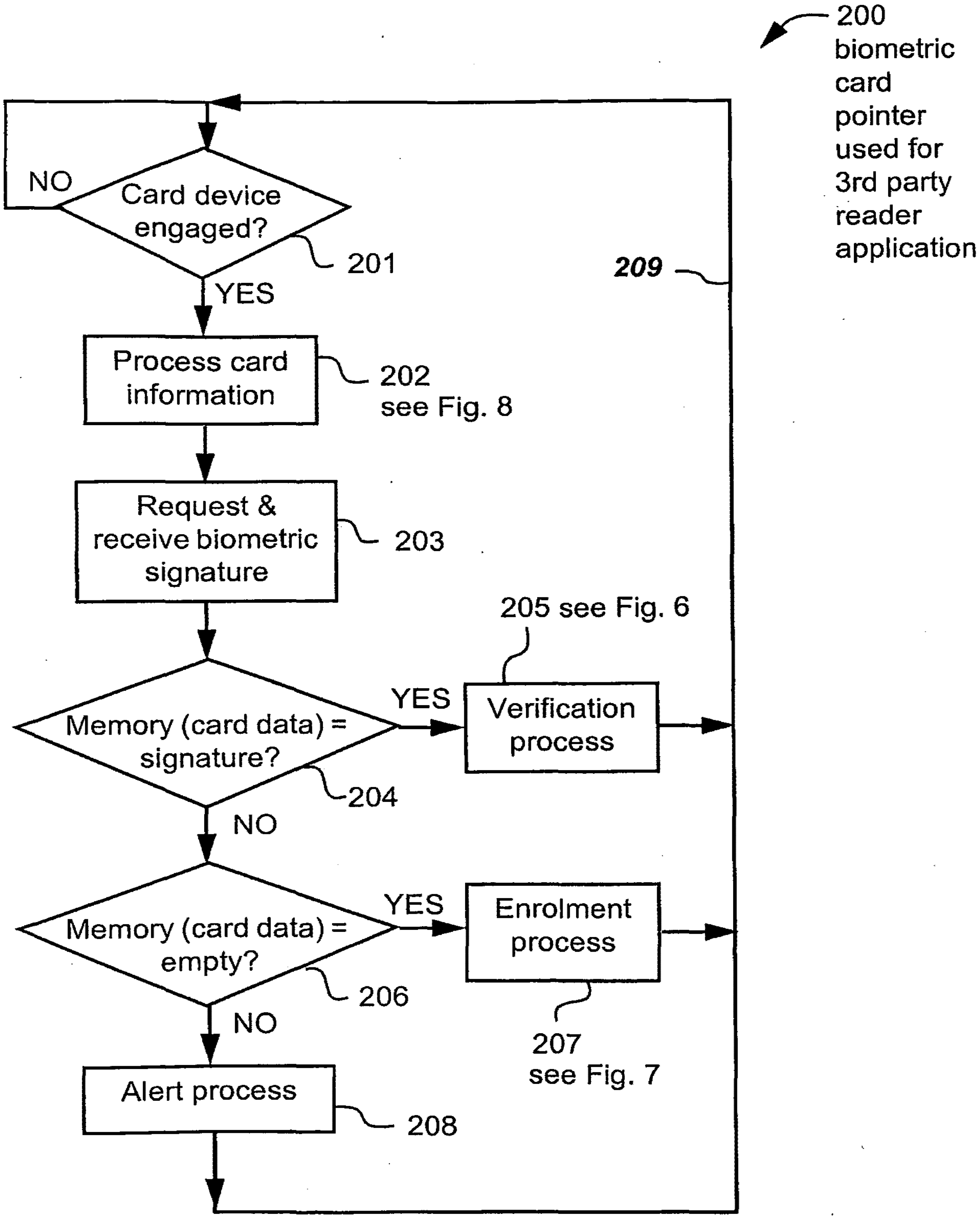
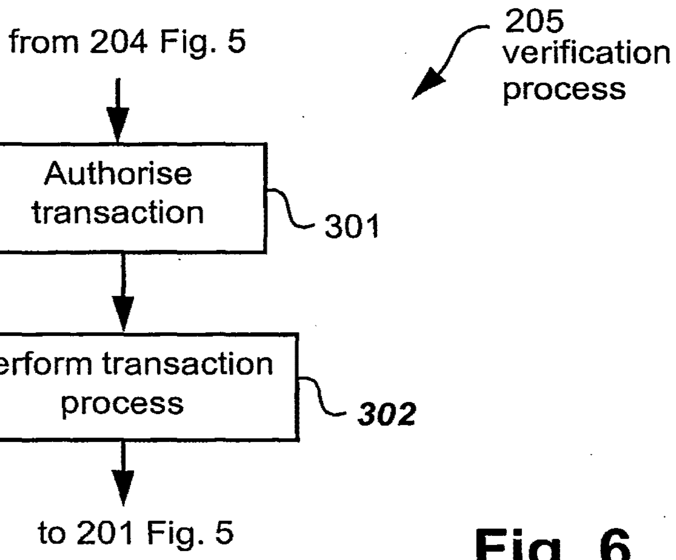
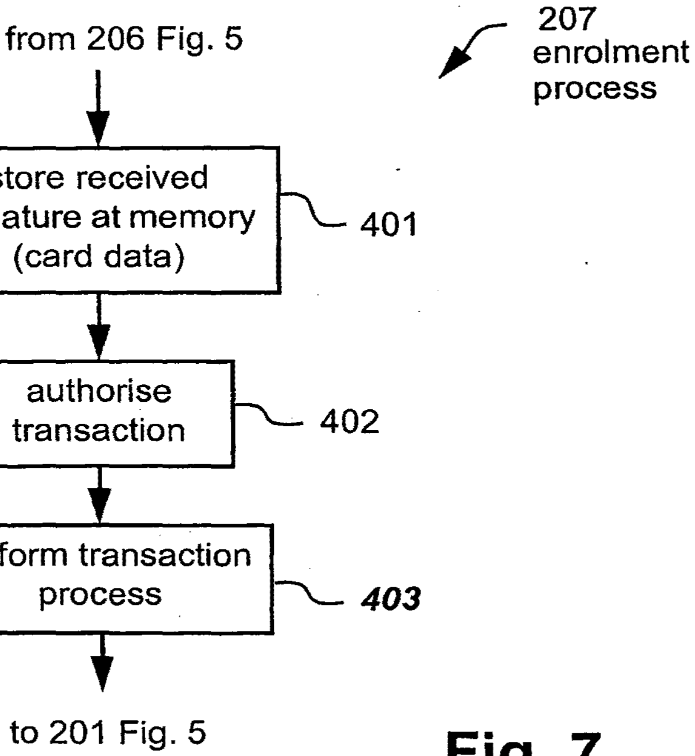

200
biometric
card
pointer
used for
3rd party
reader
application
Card device engaged?
NO
YES
201
209
Process card information
202
see Fig. 8
Request & receive biometric signature
203
205 see Fig. 6
Memory (card data) = signature?
YES
Verification process
204
NO
Memory (card data) = empty?
YES
Enrolment process
206
NO
207
see Fig. 7
Alert process
208

Fig. 5



from 204 Fig. 5
205 verification process
Authorise transaction
301
Perform transaction process
302
to 201 Fig. 5

Fig. 6



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

Fig. 7

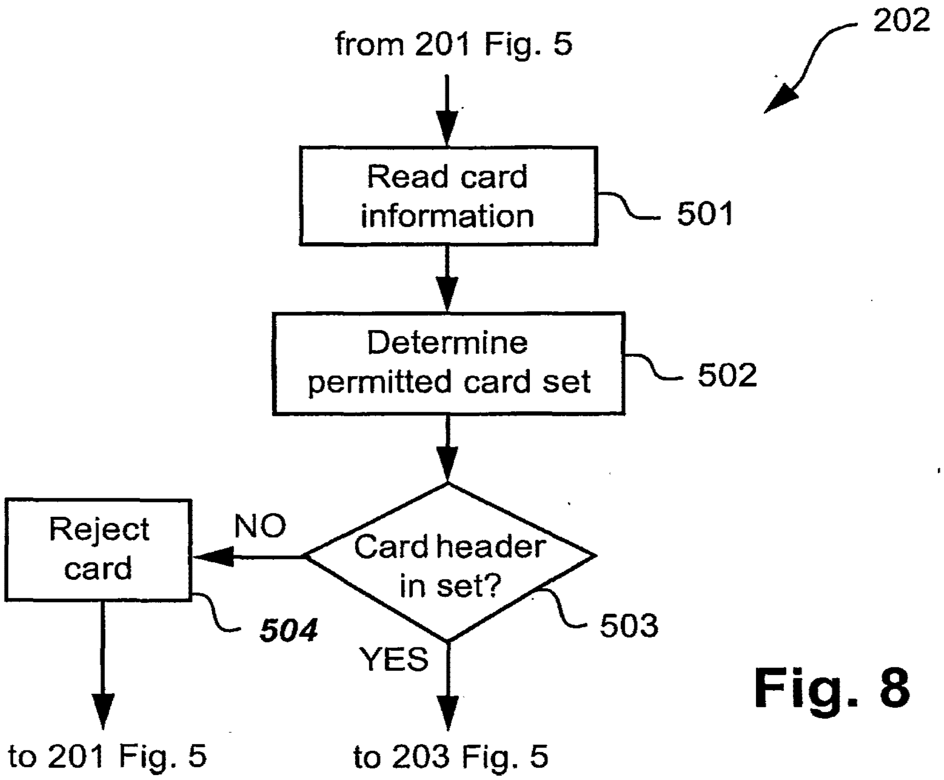

202
from 201 Fig. 5
Read card information
501
Determine permitted card set
502
Card header in set?
503
NO
Reject card
504
YES
to 201 Fig. 5
to 203 Fig. 5

Fig. 8

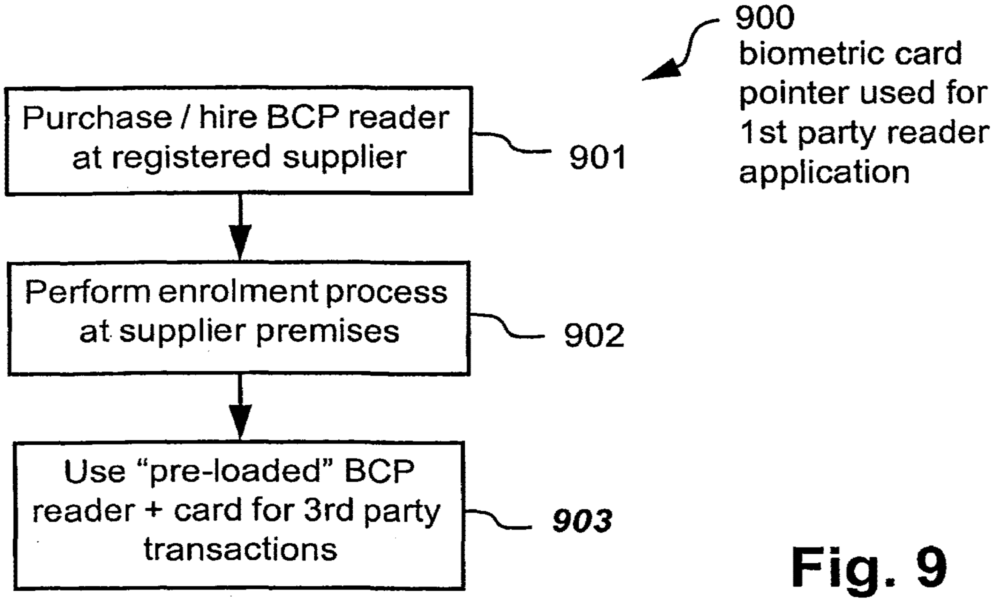

900
biometric card pointer used for 1st party reader application
Purchase / hire BCP reader at registered supplier
901
Perform enrolment process at supplier premises
902
Use "pre-loaded" BCP reader + card for 3rd party transactions
903

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2006/001136

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G07F 7/10 (2006.01) *G07F 19/00* (2006.01)
G06K 9/00 (2006.01) *G07F 7/12* (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)
DWPI, USPTO, Espace, PCT Gazette Search with IPC marks and keywords including atm/credit/debit/smart/id card/passport, atm machine, local database/DB/memory/storage/cache, biometric signature/fingerprint/iris scan, verification/authentication/authorisation/security/protection

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5457747 A (DREXLER et al.) 10 October 1995 Abstract, figures 1 and 3, column 3 line 51 to column 4 line 35, column 4 line 61 to column 5 line 18	1-2,11-12,17-18
X	CA 2412403 A1 (TAYLOR) 20 May 2003 Abstract, figure 2, page 6 lines 3-10 and 12-17, page 7 lines 4-11	1-2,11-12,17-18
X	WO 2003/036861 A1 (BLACK) 1 May 2003 Whole document, but see especially the abstract, page 4 paragraph 3, page 5 paragraphs 1 and 4, page 8, pages 15-16, all figures	1-2,11-12,17-18

☒ Further documents are listed in the continuation of Box C ☒ 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 17 October 2006	Date of mailing of the international search report 20 OCT 2006
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. (02) 6285 3929	Authorized officer **J.W. THOMSON** Telephone No : (02) 6283 2214

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2006/001136

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 6796492 B1 (GATTO) 28 September 2004 Whole document, especially column 12 lines 1-51	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2006/001136

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

Patent Document Cited in Search Report		Patent Family Member					
US	5457747	US	5412727	US	5559885		
CA	2412403	CA	2363372	EP	1315118	US	2003120933
WO	03036861	AU	18801/02	AU	41808/99	AU	63544/00
		CA	2327580	CA	2448707	CN	1307709
		CN	1526218	CN	1763685	EP	1084479
		EP	1391075	EP	1393493	EP	1422669
		EP	1422670	MX	PA03010837	US	6307956
		US	6539101	US	6925565	US	6970583
		US	7047419	US	7082213	US	2001055411
		US	2002025062	US	2002081005	US	2002178369
		US	2005169504	US	2005180618	US	2005261972
		US	2006005042	US	2006023922	WO	0122351
		WO	0205478	WO	9952060	ZA	200308701
US	6796492	AU	55448/96	CA	2218233	EP	0832465
		US	5546523	US	6149055	US	2003209599
		US	2005173519	WO	9632687		

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

END OF ANNEX

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)*	20 OCT 2006
Applicant's or agent's file reference 729727C	**FOR FURTHER ACTION** See paragraph 2 below

International application No. **PCT/AU2006/001136**	International filing date *(day/month/year)* 10 August 2006	Priority date *(day/month/year)* 12 August 2005

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

G07F 7/10 (2006.01) ***G07F 19/00*** (2006.01) ***G06K 9/00*** (2006.01) ***G07F 7/12*** (2006.01)

Applicant
SECURICOM (NSW) PTY LTD et al

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

☒	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
☒	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 IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Date of completion of this opinion 17 October 2006	Authorized Officer **J.W. THOMSON** Telephone No. (02) 6283 2214

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/AU2006/001136

Box No. I **Basis of this opinion**

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

☒ 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. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, 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.

3. □ 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.

4. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/AU2006/001136

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	**3-10, 13-16**	**YES**
	Claims	**1-2, 11-12, 17-18**	**NO**
Inventive step (IS)	Claims	**3-10, 13-16**	**YES**
	Claims	**1-2, 11-12, 17-18**	**NO**
Industrial applicability (IA)	Claims	**1-18**	**YES**
	Claims		**NO**

2. Citations and explanations:

The following documents identified in the International Search Report have been used for the purposes of this report:

D1: US 5457747 A (DREXLER et al.) 10 October 1995

D2: CA 2412403 A1 (TAYLOR) 20 May 2003

D3: WO 2003/036861 A1 (BLACK) 1 May 2003

D4: US 6796492 B1 (GATTO) 28 September 2004

NOVELTY (N):

1. The invention defined in claims 1-2, 11-12 and 17-18 is not novel when compared to the prior art documents D1, D2 and D3 which disclose all of the essential features of the invention claimed:

   D1 discloses a system for detecting and deterring fraudulent use of wallet-sized cards used in an electronic verification terminal (see abstract), including receiving and storing biometric data (see column 3 line 51 to column 4 line 35) in a memory location defined by the card if it is not already occupied (see figure 3). On subsequent presentations of the card the biometric information stored in memory is compared to biometric information acquired from the card possessor to verify their identity (see figure 3, as well as column 4 line 61 to column 5 line 18).

   D2 discloses a method for verifying a person's identity using signatures or other biometrics (see page 6 lines 3-10), including recording a reference signature and storing it in memory on a portable, readable card, such as the magnetic strip on a credit card (see page 6 lines 12-17) and comparing the reference signature to the signature provided by the card bearer (see page 7 lines 4-11, as well as figure 2).

   D3 discloses an identity authentication system used at a point-of-sale (POS) terminal. The customer registers by providing a signature and biometric data (e.g. a fingerprint), the biometric data is stored in a wireless device with memory, and thereafter the biometric data of the user is compared to that stored in the wireless device (see whole document).

(Continued in supplemental box)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of: V

INVENTIVE STEP (IS):

2. Claims 1-2, 11-12 and 17-18 also lack an inventive step over the prior art for reasons as stated for novelty.

Note: Although document D4 cannot be used as a citation for novelty or inventive step purposes, it is still considered highly relevant. It discloses an ATM system and method including a fingerprint identification unit (i.e. a biometric reader) and local memory for storing user information. When a user tries to use the ATM, the local memory of the terminal is searched for a positive match. If no match is found (i.e. if the user hasn't used the terminal before or is an unauthorised user) a search of the central database can be performed. The system disclosed by document D4 differs from the claimed application as it does not allow a user to register with the ATM locally if the match is not found, but discloses all of the remaining features of the invention claimed in claims 1-18 (see in particular column 12 lines 1-51 of the cited document).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/AU2006/001136

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claims **1-15** and **17-18** are not fully supported by the description. The specification makes it clear that the biometric information is to be stored in **local** memory incorporated into the verification station (i.e. teaches away from storing the data in a central repository), but the claims omit this feature. It is claimed that the biometric signature is stored in memory, without limiting it to local memory.

In addition, claims **1-2**, **11** and **17-18** are also not fully supported by the description as they do not disclose the step of comparing the biometric signature provided on subsequent uses of the card **at a particular verification station** with the biometric signature already stored in memory (i.e. verifying user's identity) which is essential to the working of the invention. Note that, although claims 2 and 18 talk about "subsequently presenting card information and a biometric signature", they do not explicitly state that they are provided to the same verification station.

PATENT COOPERATION TREATY
PCT
INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 729727C	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/AU2006/001136	International filing date *(day/month/year)* 10 August 2006	Priority date *(day/month/year)* 12 August 2005

International Patent Classification (IPC) or national classification and IPC

G07F 7/10 (2006.01) ***G07F 7/12*** (2006.01)
G06K 9/00 (2006.01) ***G07F 19/00*** (2006.01)

Applicant

SECURICOM (NSW) PTY LTD et al

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

a. ☒ *(sent to the applicant and to the International Bureau)* a total of 8 sheets, as follows:

☒ sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. 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

Date of submission of the demand 12 June 2007	Date of completion of this report 19 November 2007
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer **MLADEN MITIC** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. (02) 6283 3193

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No. **PCT/AU2006/001136**

Box No. I **Basis of the report**

1. With regard to the **language**, this report is based on:

☒ 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))

☐ publication of the international application (under Rule 12.4(a))

☐ international preliminary examination (Rules 55.2(a) and/or 55.3(a))

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originallv filed" and are not annexed to this report)*:

☐ the international application as originally filed/furnished

☒ the description:

pages **1-21** as originally filed/furnished
pages* received by this Authority on with the letter of
pages* received by this Authority on with the letter of

☒ the claims:

pages as originally filed/furnished
pages* as amended (together with any statement) under Article 19
pages* **22-29** received by this Authority on **12 June 2007** with the letter of 12 June 2007
pages* received by this Authority on with the letter of

☒ the drawings:

pages **1-7** as originally filed/furnished
pages* received by this Authority on with the letter of
pages* received by this Authority on with the letter of

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing *(specify)*:
☐ any table(s) related to the sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing *(specify)*:
☐ any table(s) related to the sequence listing *(specify)*:

5. ☐ This report has been established taking into account **the rectification of an obvious mistake** authorized by or notified to the Authority under Rule 91 (Rule 70.2(e)).

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims **1-18**	**YES**
	Claims **NONE**	**NO**
Inventive step (IS)	Claims **1-18**	**YES**
	Claims **NONE**	**NO**
Industrial applicability (IA)	Claims **1-18**	**YES**
	Claims **NONE**	**NO**

2. Citations and explanations (Rule 70.7)

The following documents identified in the International Search Report have been used for the purposes of this report:

D1: US 5457747 A (DREXLER et al.) 10 October 1995

D2: CA 2412403 A1 (TAYLOR) 20 May 2003

D3: WO 2003/036861 A1 (BLACK) 1 May 2003

D4: US 6796492 B1 (GATTO) 28 September 2004

NOVELTY (N) AND INVENTIVE STEP (IS):

Claims **1-18** meet the criteria set forth in PCT Article 33(2) for novelty and 33(3) for inventive step. The prior art published before the priority date does not disclose or obviously suggest to a person skilled in the art storing the biometric signature in a local memory external to the card.

International application No.	PCT/AU2006/001136

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claims **3-10** and **13-15** are not fully supported by the description. The specification makes it clear that the biometric information is to be stored in **local** memory incorporated into the verification station (i.e. teaches away from storing the data in a central repository), but the claims omit this feature. It is claimed that the biometric signature is stored in memory location defined by the provided card information, without limiting it to local memory.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

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

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

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

a smart card 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.

5. A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised.

9. A method according to any one of claims 6, 7 and 8 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.

10. A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader receiving the biometric signature;

means for defining, dependent upon the received card information, a memory location in a local memory external to the card;

means for determining if the defined memory location is unoccupied; and

means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

12. A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

13. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in 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 securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature;

code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

code for determining if the defined memory location is unoccupied; and

code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

18. A computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
12/063,650	Christopher John Burke	12838/5 (729727US)

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

INTERNATIONAL APPLICATION NO.	
PCT/AU06/01136	
I.A. FILING DATE	PRIORITY DATE
08/10/2006	08/12/2005

CONFIRMATION NO. 9949
371 FORMALITIES LETTER

OC000000042810156

Date Mailed: 07/30/2010

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as an Elected Office (37 CFR 1.495):

- Indication of Small Entity Status
- Priority Document
- Copy of the International Application filed on 02/12/2008
- Copy of the International Search Report filed on 02/12/2008
- Copy of IPE Report filed on 02/12/2008
- Copy of Annexes to the IPER filed on 02/12/2008
- Preliminary Amendments filed on 02/12/2008
- Information Disclosure Statements filed on 02/12/2008
- Oath or Declaration filed on 02/12/2008
- Small Entity Statement filed on 02/12/2008
- Request for Immediate Examination filed on 02/12/2008
- U.S. Basic National Fees filed on 02/12/2008
- Assignment filed on 08/21/2008
- Priority Documents filed on 02/12/2008

The applicant needs to satisfy supplemental fees problems indicated below.

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
    - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.492(h) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fees required for this application is $**65** for a Small Entity:

- $**65** Surcharge.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

PATRICIA A BOOKER

Telephone: (703) 756-1409

Patricia Booker

PATENT APPLICATION FEE DETERMINATION RECORD Effective December 8, 2004	Application or Docket Number Q063650

CLAIMS AS FILED - PART I

SMALL ENTITY TYPE ☑ OR OTHER THAN SMALL ENTITY

	(Column 1)	(Column 2)	RATE	FEE		RATE	FEE
U.S. NATIONAL STAGE FEES							
BASIC FEE			BASIC FEE	155	OR	BASIC FEE	
EXAMINATION FEE			EXAM. FEE	205		EXAM FEE	
SEARCH FEE			SEARCH FEE	105		SEARCH FEE	
FEE FOR EXTRA SPEC PGS	minus 100 =	/ 50 =	X $ 125 =			X $ 250 =	
TOTAL CHARGEABLE CLAIMS	20 minus 20 =	.	X $ 25 =		OR	X $ 50 =	
INDEPENDENT CLAIMS	6 minus 3 =	3	X $ 100 =	315	OR	X $ 200 =	
MULTIPLE DEPENDENT CLAIM PRESENT		□	+ $ 180 =		OR	+ $ 360 =	
			TOTAL	780	OR	TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

SMALL ENTITY OR OTHER THAN SMALL ENTITY

AMENDMENT A		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL FEE
	Total	*	Minus	**	=	X $ 25 =		OR	X $ 50 =	
	Independent	*	Minus	***	=	X $ 100 =		OR	X $ 200 =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□	+ $ 180 =		OR	+ $ 360 =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT FEE	

AMENDMENT B		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE	ADDI-TIONAL FEE		RATE	ADDI-TIONAL FEE
	Total	*	Minus	**	=	X $ 25 =		OR	X $ 50 =	
	Independent	*	Minus	***	=	X $ 100 =		OR	X $ 200 =	
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□	+ $ 180 =		OR	+ $ 360 =	
						TOTAL ADDIT. FEE		OR	TOTAL ADDIT FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than '20', enter "20"
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than '3', enter "3"
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1

Patricia Booker

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

(FOR USE WITH FORM PTO-875)

SERIAL NO. 12063650

FILING DATE

APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT			AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.		IND.	DEP.	IND.	DEP.	IND.	DEP.
1	1		1				51						
2		1		1			52						
3	1		1				53						
4		1		1			54						
5		1		1			55						
6		1		1			56						
7		1		1			57						
8		1		1			58						
9		3		1			59						
10		1		1			60						
11	1		1				61						
12		1		1			62						
13	1		1				63						
14		1		1			64						
15		1		1			65						
16	1		1				66						
17	1		1				67						
18		1		1			68						
19				1			69						
20				1			70						
21							71						
22							72						
23							73						
24							74						
25							75						
26							76						
27							77						
28							78						
29							79						
30							80						
31							81						
32							82						
33							83						
34							84						
35							85						
36							86						
37							87						
38							88						
39							89						
40							90						
41							91						
42							92						
43							93						
44							94						
45							95						
46							96						
47							97						
48							98						
49							99						
50							100						
TOTAL IND.	6	↓	6	↓		↓	TOTAL IND.		↓		↓		↓
TOTAL DEP.	14	←	14	←		←	TOTAL DEP.		←		←		←
TOTAL CLAIMS	20	▨	20	▨		▨	TOTAL CLAIMS		▨		▨		▨

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on August 12, 2010.

Robert D. Summers, Jr., Reg. No. 57,844

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: 12/063,650

371 Filing Date: August 10, 2008

For: IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Not Yet Assigned

Group Art Unit: Not Yet Assigned

Confirmation No.: 9949

RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

Mail Stop Missing Parts
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with the Notification of Missing Requirements Under 35 U.S.C. 371 in the United States Designated/Elected Office (DO/EO/US) dated **July 30, 2010**, enclosed herewith for filing are the following documents for the above-referenced patent application:

☒ Fully executed Declaration for Patent Application

☒ Power of Attorney and Correspondence Address Indication Form

□ Fully executed Combined Declaration and Power of Attorney

□ Petition for Ext. of Time (37 CFR § 1.136(a)) to File Missing Parts

☒ Other: Statement Under 37 CFR 3.73(b) (including copy of Assignment recorded on August 21, 2008 at Reel 021424/Frame 0961.

Applicant is: ☒ small entity (per 37 CFR 1.27) □ other than small entity

Fees Associated with Payment:

☐ Filing Fee: $_____

☒ Declaration Surcharge: $65.00

☐ Addtl. Claim Fees: $_____ for _____ additional claims

☐ Search Fee: $_____

☐ Examination Fee: $_____

☐ App. Size Fee: $_____ (for each additional 50 sheets that exceeds 100 sheets, including specification and drawings)

Payment Method:

☐ Check in the amount of $_____ is enclosed to cover the fees listed above.

☐ Payment by credit card in the amount of $_____ to cover the fees listed above.

Form PTO-2038 is enclosed for this purpose.

☒ The Commissioner is hereby authorized to charge $65.00 to cover the Declaration surcharge listed above to Deposit Account No. 23-1925.

☒ The Commissioner is hereby authorized to charge any deficiencies in fees or credit overpayment to Deposit Account No. 23-1925.

Respectfully submitted,

Dated: August 12, 2010

Robert D. Summers, Reg. No. 57,844
Attorney for Applicant

BRINKS HOFER GILSON & LIONE
PO BOX 10395
CHICAGO, IL 60610
(312) 321-4200

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION
(37 C.F.R. §1.63)

As a below named inventor, I hereby declare:

My residence, mailing address, and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor or an original, first and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled:

IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

the specification of which (check one)

☐ is attached hereto.

☒ was filed on February 12, 2008 as United States Application No. 12/063,650 .

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge my duty to disclose to the United States Patent and Trademark Office all information that I know to be material to patentability as defined in 37 C.F.R. §1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or (f), or §365(b) of any foreign application(s) for patent or inventor's or plant breeder's rights certificate(s), or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's or plant breeder's rights certificate(s) or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application:			Priority Not Claimed
2005904375 (Number)	Australia (Country)	08/12/2005 (Filing Date, MM/DD/YYYY)	☐
(Number)	(Country)	(Filing Date, MM/DD/YYYY)	☐

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: pending, or abandoned)

I hereby claim the benefit under 35 U.S.C. §120 of any United States applications(s), or §365(c) of any PCT International Application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

PCT/AU2006/001136 (Application Serial No.)	08/10/2006 (Filing Date, MM/DD/YYYY)	Pending (Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)
(Application Serial No.)	(Filing Date, MM/DD/YYYY)	(Status: patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole inventor
BURKE, Christopher John

Sole inventor's signature
X

Date X
31 JULY 2008

Residence (City, State/Foreign Country)
Ramsgate, New South Wales, 2217 Australia

Citizenship
Australia

Mailing Address
48 Margate Street, Ramsgate, New South Wales, 2217 Australia

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY and CORRESPONDENCE ADDRESS INDICATION FORM	**Application Number**	12/063 650
	Filing Date	12 February 2008
	First Named Inventor	Christopher John Burke
	Title	**Improving card device security using biometrics**
	Art Unit	
	Examiner Name	
	Attorney Docket Number	12838/5

I hereby revoke all previous powers of attorney given in the above-identified application.

I hereby appoint Brinks Hofer Gilson & Lione

☒ Practitioners associated with Customer Number

OR

☐ Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agents(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please recognize or change the correspondence address for the above-identified application to:

☐ The address associated with the above-mentioned Customer Number
OR
☐ The address associated with Customer Number
OR

☐ Firm *or* Individual Name					
Address					
City		State		ZIP	
Country					
Telephone		Fax			

I am the:

☐ Applicant/Inventor.

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Securicom (NSW) Pty Ltd

Signature	X	Date	X 31 JULY 2008 Day Month Year
Name	X CHRIS BURKE	Telephone	
Title	X MANAGING DIRECTOR		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more that one signature is required, see below *.

☒ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application for to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

S&F Ref: 729727US

(1336472_1):NIS

PTO/SB/96 (09-04)
Approved for the use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Securicom (NSW) Pty Ltd

Application No. / Patent No.: 12/063 650 Filed/Issue Date: 12 February 2008

Entitled: Improving card device security using biometrics

Securicom (NSW) Pty Ltd an, an Australian company, ACN 053 874 089

(Name of Assignee) (Assignee, eg, corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. □ an assignee of less than the entire right, title, and interest.
The extent (by, percentage) of its ownership interest is _______%

in the patent application/patent identified above by virtue of either:

A. ☒ an assignment from Inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel ______________, Frame ________, or for which a copy thereof is attached.

OR

B. □ A chain of title from the Inventor(s), of the patent application/patent identified above, to the current assignee As shown below:

1. From: ______ To: ____
The document was recorded in the United States Patent and Trademark Office at
Reel __________, Frame ______________, or for which a copy thereof is attached.

2. From: ______ To: ____
The document was recorded in the United States Patent and Trademark Office at
Reel __________, Frame ______________, or for which a copy thereof is attached.

3. From: ______________________________ To: ____
The document was recorded in the United States Patent and Trademark Office at
Reel __________, Frame ______________, or for which a copy thereof is attached.

□ Additional documents in the chain of title are listed on a supplemental sheet.

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.
[NOTE: A separate copy (ie., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO.
See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Securicom (NSW) Pty Ltd

X
Signature

X 31 JULY 2008
Date (Day Month Year)

X CHRIS BURKE
Printed or typed Name

0412440117
Telephone Number

X MANAGING DIRECTOR
Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application for to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

S&F REF: 729727US

UNITED STATES PATENT AND TRADEMARK OFFICE

UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND
DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

AUGUST 22, 2008 *500627471A*

PTAS

ROBERT D. SUMMERS, JR.
POST OFFICE BOX 10395
CHICAGO, IL 60610

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 571-272-3350. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT SERVICES BRANCH, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 08/21/2008 REEL/FRAME: 021424/0961
NUMBER OF PAGES: 2

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).
DOCKET NUMBER: 12838/5 (729727US)

ASSIGNOR:
BURKE, CHRISTOPHER JOHN DOC DATE: 07/31/2008

ASSIGNEE:
SECURICOM (NSW) PTY LTD
48 MARGATE STREET
RAMSGATE, NEW SOUTH WALES 2217
AUSTRALIA

SERIAL NUMBER: 12063650 FILING DATE:
PATENT NUMBER: ISSUE DATE:
TITLE: IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

021424/0961 PAGE 2

ASSIGNMENT SERVICES BRANCH
PUBLIC RECORDS DIVISION

PATENT ASSIGNMENT

Electronic Version v1.1
Stylesheet Version v1.1

08/21/2008
500627471

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
Christopher John Burke	07/31/2008

RECEIVING PARTY DATA

Name:	Securicom (NSW) Pty Ltd
Street Address:	48 Margate Street
City:	Ramsgate, New South Wales 2217
State/Country:	AUSTRALIA

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	12063650

CORRESPONDENCE DATA

Fax Number: (312)321-4299

Correspondence will be sent via US Mail when the fax attempt is unsuccessful.

Phone:	312-321-4200
Email:	rsummers@usebrinks.com
Correspondent Name:	Robert D. Summers, Jr.
Address Line 1:	Post Office Box 10395
Address Line 4:	chicago, ILLINOIS 60610

ATTORNEY DOCKET NUMBER:	12838/5 (729727US)
NAME OF SUBMITTER:	Robert D. Summers, Jr.

Total Attachments: 1
source=128385assn#page1.tif

US sole
(After Application Filed)

ASSIGNMENT OF PATENT RIGHTS FOR THE UNITED STATES

FOR VALUE RECEIVED, I Christopher John Burke, an Australian citizen

residing at 48 Margate Street, Ramsgate, New South Wales 2217, Australia

hereby sell, assign, transfer and convey unto: Securicom (NSW) Pty Ltd

incorporation details: an Australian company, ACN 053 874 089

having a place of business at: of 48 Margate Street, Ramsgate, New South Wales 2217, Australia

its successors, assigns and legal representatives (hereinafter called the "Assignee"), the entire right, title and interest, for the United States, in and to certain inventions relating to

Improving card device security using biometrics

and described in an application for Letter Patent of the United States filed by us on 12 February 2008

and which has been accorded Application No. 12//063 650

and in and to said application, and all divisions, renewals and continuations thereof, and all Letters Patent of the United States which may be granted, thereon, and all reissues and extensions thereof; and I hereby authorize and request the Commissioner of Patents and Trademarks of the United States to issue all Letters Patent upon said inventions to the Assignee or to such nominees as it may designate.

AND I authorize and empower the said Assignee or nominees to invoke and claim for any application for patent or other form of protection for said inventions, the benefit of the right of priority provided by the International Convention for the Protection of Industrial Property, as amended, or by any convention which may henceforth be substituted for it, and to invoke and claim such right of priority without further written or oral authorization from me.

AND I hereby consent that a copy of this assignment shall be deemed a full legal and formal equivalent of any assignment, consent to file or like document which may be required in the United States for any purpose and more particularly in proof of the right of said Assignee or nominees to claim the aforesaid benefit of the right of priority provided by the International Convention for the Protection of Industrial Property as amended, or by any convention which may henceforth be substituted for it.

AND I hereby covenant that we have the full right to convey the entire right, title and interest herein assigned and that I have not executed and will not execute any agreement in conflict herewith.

AND I hereby covenant and agree that we will communicate to said Assignee or nominees all facts known to me pertaining to said inventions, and testify in all legal proceedings, sign all lawful papers, execute all divisional, continuing and reissue applications, make all rightful oaths and declarations and in general perform all lawful acts necessary or proper to aid said Assignee or nominees in obtaining, maintaining and enforcing all lawful patent protection for said inventions in the United States.

By: X
Christopher John Burke

Date: X 31 JULY 2008
Day Month Year

X
Signature of Witness
Name: X CHRISTINE BURKE

S&F Ref: 729727US

(1336219_1):NIS

Electronic Patent Application Fee Transmittal

Application Number:	12063650
Filing Date:	
Title of Invention:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Robert Dalton Summers/Lori Peterson
Attorney Docket Number:	12838/5 (729727US)

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Oath/decl > 30 mo. from priority date	2617	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**65**

Electronic Acknowledgement Receipt	
EFS ID:	8205762
Application Number:	12063650
International Application Number:	
Confirmation Number:	9949
Title of Invention:	IMPROVING CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	00757
Filer:	Robert Dalton Summers/Magdalena Pieczonka
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/5 (729727US)
Receipt Date:	12-AUG-2010
Filing Date:	
Time Stamp:	14:36:16
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$65
RAM confirmation Number	704
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		128385rmr.PDF	504875 6c7270573d46791b016d4c112019ccb47a5edaa5	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Miscellaneous Incoming Letter	1	1
Applicant Response to Pre-Exam Formalities Notice	2	3
Oath or Declaration filed	4	5
Power of Attorney	6	6
Assignee showing of ownership per 37 CFR 3.73(b).	7	11

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (PTO-875)	fee-info.pdf	30471 c41c7022df4c79ad66c2f5b35feb8d1182bfa863	no	2

Warnings:

Information:

Total Files Size (in bytes):	535346

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on August 12, 2010.

Robert D. Summers, Jr., Reg. No. 57,844

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: 12/063,650

371 Filing Date: August 10, 2008

For: IMPROVING CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Not Yet Assigned

Group Art Unit: Not Yet Assigned

Confirmation No.: 9949

Mail Stop Missing Parts
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

Sir:

Attached are:

☒ Transmittal Letter; Response To Notification Of Missing Requirements Under 35 U.S.C. 371; Declaration; Power of Attorney and Correspondence Address Indication Form; Statement Under 37 CFR 3.73(b) (including copy of Assignment recorded on August 21, 2008 at Reel 021424/Frame 0961.

Fee calculation:

□ No additional fee is required.

□ Small Entity.

□ An extension fee in an amount of $____ for a ___-month extension of time under 37 C.F.R. § 1.136(a).

□ A petition or processing fee in an amount of $____ under 37 C.F.R. § 1.17(e).

□ An additional filing fee has been calculated as shown below:

						Small Entity			Not a Small Entity	
	Claims Remaining		Highest No.	Present			Add'l Fee	or		Add'l Fee
Total		Minus				x $26=			x $52=	
Indep.		Minus				x 110=			x 220	
First Presentation of Multiple Dep. Claim						+$195=			+$390=	
						Total	$		Total	$

Fee payment:

□ A check in the amount of $_____ is enclosed.

☒ Please charge Deposit Account No. 23-1925 in the amount of $65.00 for the Declaration surcharge.

□ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

August 12, 2010
Date

Robert D. Summers, Jr. (Reg. No. 57,844)

BRINKS
HOFER
GILSON
&LIONE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/063,650	08/12/2010		845	12838/5	20	6

CONFIRMATION NO. 9949

FILING RECEIPT

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

OC000000043083383

Date Mailed: 08/18/2010

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Christopher John Burke, New South Wales, AUSTRALIA;

Power of Attorney: The patent practitioners associated with Customer Number 757

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/AU06/01136 08/10/2006

Foreign Applications

AUSTRALIA 2005904375 08/12/2005

If Required, Foreign Filing License Granted: 08/17/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/063,650**

Projected Publication Date: 11/25/2010

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

CARD DEVICE SECURITY USING BIOMETRICS

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
12/063,650	Christopher John Burke	12838/5

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

INTERNATIONAL APPLICATION NO.	
PCT/AU06/01136	
I.A. FILING DATE	PRIORITY DATE
08/10/2006	08/12/2005

CONFIRMATION NO. 9949
371 ACCEPTANCE LETTER

OC000000043083384

Date Mailed: 08/18/2010

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

08/12/2010	08/12/2010
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Indication of Small Entity Status
- Copy of the International Application filed on 02/12/2008
- Copy of the International Search Report filed on 02/12/2008
- Copy of IPE Report filed on 02/12/2008
- Copy of Annexes to the IPER filed on 02/12/2008
- Preliminary Amendments filed on 02/12/2008
- Information Disclosure Statements filed on 02/12/2008
- Oath or Declaration filed on 08/12/2010
- Small Entity Statement filed on 02/12/2008
- Request for Immediate Examination filed on 02/12/2008
- U.S. Basic National Fees filed on 02/12/2008
- Assignment filed on 08/21/2008
- Priority Documents filed on 02/12/2008
- Power of Attorney filed on 08/12/2010

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

PATRICIA A BOOKER

Telephone: (703) 756-1409

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/063,650	08/12/2010	Christopher John Burke	12838/5

CONFIRMATION NO. 9949

PUBLICATION NOTICE

OC000000044678396

757
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

Title:CARD DEVICE SECURITY USING BIOMETRICS

Publication No.US-2010-0296708-A1
Publication Date:11/25/2010

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

757 7590 02/26/2013
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
JOHNS, ANDREW W	
ART UNIT	PAPER NUMBER
2665	
MAIL DATE	DELIVERY MODE
02/26/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 12/063,650	**Applicant(s)** BURKE	
	Examiner Andrew W. Johns	**Art Unit** 2665	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2008*.

2a)□ This action is **FINAL**.   2b)☒ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☒ Claim(s) *1-15,19 and 20* is/are allowed.

7)☒ Claim(s) *16-18* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)□ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *21 July 2010* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *2/12/08*.

3) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 U.S.C. § 101

1. 35 U.S.C. § 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 16-18 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

Claims 16-18 are variously directed towards a computer program product that includes a computer readable medium variously having computer programs recorded thereon. The broadest reasonable interpretation of a claim drawn to such a computer readable medium typically covers both forms of non-transitory tangible media and transitory propagating signals, *per se*, in view of the ordinary and customary meaning of computer readable media. See the OG Notice of 23 February 2010, entitled "Subject Matter Eligibility of Computer Readable Media", 1351 OG 212. When the broadest reasonable interpretation of a claim covers a signal, *per se*, the claim must be rejected under 35 U.S.C. § 101 as covering patent ineligible subject matter. See *In re Nuijten*, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007). Therefore, claims 16-18 broadly encompass a propagating signal, *per se*, so that they broadly encompass subject matter that is ineligible for patent protection under 35 U.S.C. § 101.

It is suggested that amending these claims so that they clearly and unambiguously exclude such propagating signals from the full scope of the claimed subject matter would resolve this matter. In particular, amending these claims to recite a "non-transitory computer readable medium", as suggested in the OG Notice, would properly limit the claimed invention to eligible subject matter by clearly and unambiguously excluding propagating signals, which are by their very nature transitory, from the fully scope of the claims.

Allowable Subject Matter

3. Claims 1-15 and 19-20 are allowed.

4. The following is a statement of reasons for the indication of allowable subject matter: None of the prior art teaches or suggests defining a memory location in a local memory external to a card in dependence on information received from the card and when that memory location is determined to be unoccupied, storing a received biometric signature therein, as variously required by claims 1 and 11. Further, none of the prior art teaches or suggests that a verification station determines if card information provided to a verification station has previously been provided to that verification station, as required, in part, by claims 3 and 13.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew Johns whose telephone number is (571) 272-7391. The examiner in normally available Monday through Friday, typically between 6:15 am and 2:45 pm Eastern Time. The examiner may also be contacted by e-mail using the address: andrew.johns@uspto.gov. (Applicant is reminded of the Office policy regarding e-mail communications. See M.P.E.P. § 502.03)

If attempts to reach the examiner are unsuccessful, the examiner's supervisor, Bhavesh Mehta, can be reached at (571) 272-7453. The fax phone number for this art unit is (571) 273-8300. In order to ensure prompt delivery to the examiner, all unofficial communications should be clearly labeled as "Draft" or "Unofficial."

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center Receptionist whose telephone number is (571) 272-2600.

A. Johns
21 February 2013

/Andrew W. Johns/
Primary Examiner, Art Unit 2665

Search Notes	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
382	115, 119, 155, 159	2/21/2013	/AWJ/
356	71	2/21/2013	/AWJ/
350	5.2, 5.52, 5.53, 5.8, 5.81, 5.82, 5.83	2/21/2013	/AWJ/
235	380, 382	2/21/2013	/AWJ/

SEARCH NOTES

Search Notes	Date	Examiner

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

✓	**Rejected**	**-**	**Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		**DATE**								
Final	Original	02/21/2013								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	✓								
	17	✓								
	18	✓								
	19	=								
	20	=								

FORM PTO-1449	SERIAL NO. Not Yet Assigned	CASE NO. **12838/5**
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT	FILING DATE Herewith	GROUP ART UNIT Not Yet Assigned
	APPLICANT: **BURKE, Christopher John**	

REFERENCE DESIGNATION **U.S. PATENT DOCUMENTS**

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
/AWJ/	A1	6,796,492 B1	09/28/2004	Gatto	235/379	9/10/02
/AWJ/	A2	5,457,747 A	10/10/1995	Drexler et al.	380/24	

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES OR NO
/AWJ/	A3	CA 2 412 403 A1	05/20/2003	Canada	G06K 9/62	n/a
/AWJ/	A4	WO 03/036861 A1	05/01/2003	PCT	H04L 9/14	n/a

EXAMINER INITIAL		**OTHER ART – NON PATENT LITERATURE DOCUMENTS** (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.
/AWJ/	A5	International Search Report dated October 20, 2006.
/AWJ/	A6	International Preliminary Report on Patentability dated November 19, 2007.

EXAMINER /Andrew W. Johns/	DATE CONSIDERED 02/20/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on May 23, 2013.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: CHRISTOPHER J. BURKE
Appln. No.: 12/063,650
Filed: February 12, 2008
For: CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/0005

Examiner: JOHNS, Andrew W.
Art Unit: 2665
Confirmation No. 9949

AMENDMENT AND RESPONSE TO OFFICE ACTION

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA22313-1450

Dear Sir:

Assignee has timely filed the following response to the Non-final Office Action mailed February 26, 2013 ("Office Action"). Assignee respectfully requests reconsideration and allowance of the present claims in view of the following remarks and amendments.

Amendments to the Claims begin on page 2 of this response.

Remarks and Arguments begin on page 12 of this response.

Amendments to the Claims:

The listing of Claims will replace all prior versions and listings of the Claims in the application:

Listing of Claims:

1. (Original) A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. (Original) A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim 1;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. (Original) A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

4. (Original) A method according to claim 3, wherein the card device is one of:

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

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

a smart card 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.

5. (Original) A method according to claim 3, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. (Original) A method according to claim 3, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. (Original) A method according to claim 6, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. (Previously Presented) A method according to claim 3, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised authorized.

9. (Previously Presented) A method according to any one of claims claim 6, 7 and 8 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.

10. (Original) A method according to claim 3, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

11. (Previously Presented) A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader for receiving the biometric signature;

means for defining, dependent upon the received card information, a memory location in a local memory external to the card;

means for determining if the defined memory location is unoccupied; and

means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

12. (Original) A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim 11; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

13. (Currently Amended) A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for [[;]]:

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for [[;]]:

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

14. (Original) A verification station according to claim 13, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

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

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

15. (Original) A verification station according to claim 13, wherein the memory is incorporated in a tamper-proof manner in the verification station.

16. (Currently Amended) A non-transitory ~~computer program product including a~~ computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for [[;]] :

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for [[;]]:

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

17. (Currently Amended) A non-transitory ~~computer program product including a~~ computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature;

code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

code for determining if the defined memory location is unoccupied; and

code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

18. (Currently Amended) A non-transitory ~~computer program product including a~~ computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim 17;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

19. (Previously Presented) A method according to claim 7, 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.

20. (Previously Presented) A method according to claim 8, 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..

REMARKS

Claims 1-20 are currently pending. Claims 13, 16, 17 and 18 were amended. The amendments do not include new matter. Support for the amendments may be found in Application, at least at ¶¶ 0083-0094, 101, and 0102 and Figs 3 and 4. Assignee respectfully requests reconsideration of pending claims 1-20, and allowance of the Application in view of the above claim amendments and the following remarks.

Detailed Remarks

I. Rejections Under 35 U.S.C. § 101

The Office Action, at pages 2-3, rejected claims 16-18 under 35 U.S.C. § 101 as directed to non-statutory subject matter. Assignee respectfully traverses these rejections.

Claims 16, 17 and 18, as amended, positively recite a non-transitory computer readable medium, as provided under 35 U.S.C. § 101 in order to qualify as a statutory process. Thus, for at least these reasons, Assignee respectfully requests the rejections be withdrawn directed to claims 16-18.

II. Allowable Subject Matter

Claims 1-15 and 19-20

The Office Action, at page 3, conceded that claims 1-15 and 19-20 recite allowable subject matter for at least the following reasons: i) "None of the prior art teaches or suggests defining a memory location in a local memory external to a card in dependence on information received from the card and when that memory location is determined to be unoccupied, storing a received biometric signature therein, as variously required by claims 1 and 11;" and ii) "none of the prior art teaches or suggests that a verification station determines if card information provided to a verification station has previously been provided to that verification station, as required, in part, by claims 3 and 13."

Claims 16, 17 and 18

Claim 16, as amended, recites a program comprising "code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station." These features of claim 16 are at least consistent with the features recited by claims 3 and 11, conceded by the Examiner as allowable subject matter. Thus, for at least the reasons given regarding claims 3 and 11, claim 16 recites allowable subject matter.

Claim 17, amended, recites a program comprising "code for determining if the defined memory location is unoccupied; and code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location." These features of claim 17 are at least consistent with the features recited by claims 1 and 11, conceded by the Examiner as allowable subject matter. Thus, for at least the reasons given regarding claims 1 and 11, claim 17 and claim 18, which depends from claim 17, recite allowable subject matter.

* * * *

Conclusion

In view of the above remarks and amendments, Assignee respectfully submits that this Application is in condition for allowance and such action is earnestly requested. If for any reason the Application is not allowable, the Examiner is requested to contact the Assignee's undersigned attorney.

Respectfully submitted,

/Robert D. Summers, Jr./
Robert D. Summers Jr.
Registration No. 57,844
Attorney for Assignee

BRINKS HOFER GILSON& LIONE
CUSTOMER NO. 00757
Telephone: (312) 321-4200
Facsimile: (312) 321-4299

Electronic Acknowledgement Receipt

EFS ID:	15857358
Application Number:	12063650
International Application Number:	
Confirmation Number:	9949
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers
Filer Authorized By:	
Attorney Docket Number:	12838/5
Receipt Date:	23-MAY-2013
Filing Date:	12-AUG-2010
Time Stamp:	18:54:04
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	128385tl.pdf	42024 8fdaa85386d501950878fdb974e4025312c0aae7	no	1

Warnings:

Information:

2		128385rsp.pdf	381042 352ed48d3c873d62636900ff07cd333ce26bb189	yes	13

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	11
Applicant Arguments/Remarks Made in an Amendment	12	13

Warnings:

Information:

Total Files Size (in bytes):	423066

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on May 23, 2013.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: 12/063,650

371 Filing Date: August 10, 2008

For: CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Johns, Andrew W.

Group Art Unit: 2665

Confirmation No.: 9949

Mail Stop Amendment
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

Attached are:

☒ Transmittal Letter; Amendment and Response to Office Action.

Fee calculation:

☒ No additional fee is required.

☒ Small Entity.

☐ An extension fee in an amount of $____ for a ___-month extension of time under 37 C.F.R. § 1.136(a).

☐ A petition or processing fee in an amount of $____ under 37 C.F.R. § 1.17(e).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

☐ A check in the amount of $_____ is enclosed.

☐ Please charge Deposit Account No. 23-1925 in the amount of $_____ for the filing fees.

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

May 23, 2013
Date

/Robert D. Summers, Jr./
Robert D. Summers, Jr. (Reg. No. 57,844)

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 12/063,650	Filing Date 08/12/2010	□ To be Mailed

ENTITY: □ LARGE ☒ SMALL □ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	**165**
□ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
□ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
□ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
□ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	**165**

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	**05/23/2013**	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x $40 =	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	x $210 =	0
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	□ Application Size Fee (37 CFR 1.16(s))						
	□ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/GLORIA TRAMMELL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

757 7590 06/10/2013

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
JOHNS, ANDREW W	
ART UNIT	PAPER NUMBER
2665	

DATE MAILED: 06/10/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

TITLE OF INVENTION: CARD DEVICE SECURITY USING BIOMETRICS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/10/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail
Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

757 7590 06/10/2013
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

TITLE OF INVENTION: CARD DEVICE SECURITY USING BIOMETRICS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/10/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
JOHNS, ANDREW W	2665	382-119000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________
2____________________
3____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee
□ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies __________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number __________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
□ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
□ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

757 7590 06/10/2013
BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
JOHNS, ANDREW W	
ART UNIT	**PAPER NUMBER**
2665	

DATE MAILED: 06/10/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 503 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 503 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 12/063,650	**Applicant(s)** BURKE	
	Examiner Andrew W. Johns	**Art Unit** 2665	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed 23 May 2013*.

   □ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.

2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-20*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☒ All b) □ Some *c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. ______ .
   3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

   Interim copies:

   a) □ All b) □ Some c) □ None of the: Interim copies of the priority documents have been received.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. □ Examiner's Amendment/Comment
6. □ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/Andrew W Johns/
Primary Examiner, Art Unit 2665

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12063650	BURKE
	Examiner	**Art Unit**
	ANDREW W JOHNS	2665

CPC

Symbol				Type	Version
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			
		/			

CPC Combination Sets

Symbol				Type	Set	Ranking	Version
		/					
		/					

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
382	119

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
340	5.82				

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
G	0	6	K	9 / 00 (2006.01.01)					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	05/31/2013 (Date)	O.G. Print Claim(s): 1 O.G. Print Figure: 5

U.S. Patent and Trademark Office

Part of Paper No. 20130531

Issue Classification	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	05/31/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

Issue Classification	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	19	17												
2	2	20	18												
3	3	8	19												
4	4	11	20												
5	5														
6	6														
7	7														
10	8														
9	9														
12	10														
13	11														
14	12														
15	13														
16	14														
17	15														
18	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	05/31/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	235	(biometric near4 enroll$5).clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:24
L2	14026	(memory near4 location).clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:24
L3	120	2 near8 card.clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:24
L4	1	1 same 3	US-PGPUB; UPAD	OR	ON	2013/05/31 13:24
L5	300	2 near6 (open or available or unoccupied).clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:27
L6	1	1 same 5	US-PGPUB; UPAD	OR	ON	2013/05/31 13:27
L7	1	1 and 5	US-PGPUB; UPAD	OR	ON	2013/05/31 13:28
L8	658	(verification near4 (station or terminal)).clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:28
L9	543	(card near6 previous$4).clm.	US-PGPUB; UPAD	OR	ON	2013/05/31 13:28
L10	2	8 same 9	US-PGPUB; UPAD	OR	ON	2013/05/31 13:28

5/31/2013 1:29:28 PM
C:\Users\ajohns\Documents\EAST\Workspaces\Applications\12\000\12063650.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9949

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/063,650	08/12/2010 **RULE**	382	2665	12838/5

APPLICANTS
Christopher John Burke, New South Wales, AUSTRALIA;

** **CONTINUING DATA** *************************
This application is a 371 of PCT/AU06/01136 08/10/2006

** **FOREIGN APPLICATIONS** *************************
AUSTRALIA 2005904375 08/12/2005

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** ** ** SMALL ENTITY **
08/17/2010

			STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	☑ Yes □ No	□ Met after Allowance	AUSTRALIA	7	20	6
35 USC 119(a-d) conditions met	☑ Yes □ No					
Verified and Acknowledged	/ANDREW W JOHNS/ Examiner's Signature	Initials				

ADDRESS

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610
UNITED STATES

TITLE

CARD DEVICE SECURITY USING BIOMETRICS

FILING FEE RECEIVED 845	FEES: Authority has been given in Paper No.____________ to charge/credit DEPOSIT ACCOUNT No.____________ for following:	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time) □ 1.18 Fees (Issue) □ Other ________________ □ Credit

Search Notes	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
382	115, 119, 155, 159	2/21/2013	/AWJ/
356	71	2/21/2013	/AWJ/
340	5.2, 5.52, 5.53, 5.8, 5.81, 5.82, 5.83	2/21/2013	/AWJ/
235	380, 382	2/21/2013	/AWJ/
Above updated		5/31/2013	/AWJ/

SEARCH NOTES

Search Notes	Date	Examiner

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Interference text search in PGPUB and UPAD files in EAST	(search history attached)	5/31/2013	/AWJ/

Index of Claims	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	02/21/2013	05/31/2013							
1	1	=	=							
2	2	=	=							
3	3	=	=							
4	4	=	=							
5	5	=	=							
6	6	=	=							
7	7	=	=							
10	8	=	=							
9	9	=	=							
12	10	=	=							
13	11	=	=							
14	12	=	=							
15	13	=	=							
16	14	=	=							
17	15	=	=							
18	16	✓	=							
19	17	✓	=							
20	18	✓	=							
8	19	=	=							
11	20	=	=							

FIRST SUPPLEMENTAL FORM PTO-1449	SERIAL NO. **12/063,650**	CASE NO. **12838/5**
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT	FILING DATE **August 12, 2010**	GROUP ART UNIT **2665**
	APPLICANT: **BURKE, Christopher John**	

REFERENCE DESIGNATION **U.S. PATENT DOCUMENTS**

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
	B1	2004/0041690 A1	03/04/2004	Yamagishi		
	B2	6,665,601 B1	12/16/2003	Nielsen		

FOREIGN PATENT DOCUMENT

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES OR NO
	B3	WO 2004/100053 A1	11/18/2004	WIPO		n/a

EXAMINER INITIAL		OTHER ART – NON PATENT LITERATURE DOCUMENT (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.
	B4	Supplementary European Search Report dated August 29, 2011 for EPO Application No. EP 06760981.8.

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2004 (18.11.2004)

PCT

(10) International Publication Number
WO 2004/100053 A1

(51) International Patent Classification[7]: G06K 9/00, G06F 21/00, G07C 9/00

(21) International Application Number: PCT/US2004/013788

(22) International Filing Date: 3 May 2004 (03.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/467,168 1 May 2003 (01.05.2003) US

(71) Applicant (*for all designated States except US*): **U.S. BIOMETRICS CORPORATION** [US/US]; 2948 Artesian, Unit #112, Naperville, IL 60565 (US).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): **DELGROSSO, David** [US/US]; 68 Redstart Road, Naperville, IL 60565 (US). **ORR, Fraser** [GB/GB]; 64 Redstart Road, Naperville, IL 60565 (US).

(74) Agent: **MORNEAULT, Monique, A.**; Wallenstein Wagner & Rockey, Ltd., 311 South Wacker Drive - 5300, Chicago, IL 60606 (US).

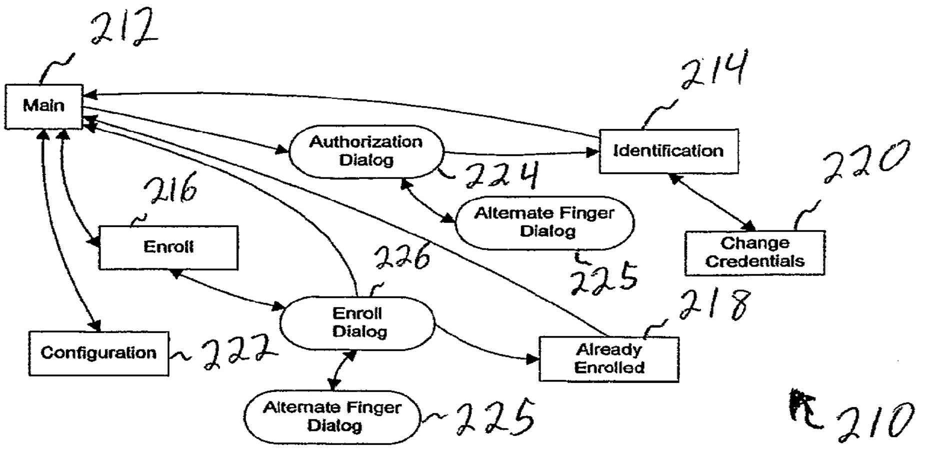
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PREVENTING IDENTITY FRAUD



(57) **Abstract:** A system and method for verifying the identity of an individual for check cashing and other financial purposes is disclosed. A client, such as a bank or other financial institution, obtains a biometric identifier from a customer and can either try to match it in a local database or send it to a central database to be matched. Either database can be filtered according to a tag or location of the institution to speed up the matching process. The central database transmits information associated with the matched individual to determine whether or not to complete the transaction.

WO 2004/100053 A1

SYSTEM AND METHOD FOR PREVENTING IDENTITY FRAUD

DESCRIPTION

Related Applications

This application claims the benefit of U.S. Provisional Patent Application No. 60/467,168, filed on May 1, 2003, and incorporated herein by reference.

Technical Field

The present invention generally relates to an identification system for preventing fraud and more particularly, to an identification system using biometric data for verifying users and preventing fraudulent check cashing.

Background of the Invention

Identity fraud has become increasingly common in today's society. As more people advance into the electronic age, it has become easier to digitally manipulate common forms of identification. It is no longer safe to merely require a social security number and a driver's license or other picture identification to verify an individual's true identity. As computers, scanners, and printers improve in quality, so do fraudulent forms of identification. Fraudulent identification has become increasingly sophisticated, with even trained professionals, in some cases, unable to tell the difference between a fake and a real form of identification. Average customer service employees generally have even less training in distinguishing between real identification and fakes.

One area particularly susceptible to fraudulent identification is banking and check cashing systems. Check cashing can be performed for individuals (the payee) that do not have bank accounts if the payor's account is with the bank so the checking information can be verified. In these situations, the bank typically requires some form of photo identification such as a driver's license to verify the individual's identity as well as to record the individual's driver's license number if there is ever a problem with the check. Bank tellers are given brief training for distinguishing between real and fake identification, but they are not generally professionals at such matters. For a reasonable amount of money, an individual can purchase image editing software and a printer capable of creating realistic drivers' licenses and social security cards. These forms of fraudulent identification can be used to mislead tellers and other customer service representatives at banks or other financial institutions.

Additionally, other check cashing institutions cash checks for individuals even though neither the payor nor the payee have an account with the institution. Even though the check is typically verified according to the account number, there is no way to guarantee the check is not stolen or fake. Not only could the check be stolen, but also the individual cashing the check could be using fraudulent identification.

Apart from check cashing, an individual may try to use fraudulent identification to open credit accounts. As with banks, to apply for credit accounts, an individual typically needs a photo form of identification and in some cases, an additional form of identification such as a social security card. As previously noted, both photo identification and social security cards can be easily manipulated using digital editing software and a printer.

Overall, the problems with fraudulent identification originate from the fact that current forms of identification are too prone to manipulation because of advancing technology. To combat evolving digital imaging technology, new security measures are being employed with photo identification such as holograms. While improvements to photo identification may prove helpful, more needs to be done to prevent identity theft and fraudulent identification.

One method to prevent identity theft and fraudulent identification is to use biometric information to identify individuals. Biometric information, such as fingerprints, is a nearly infallible means of personal identification that is not easily falsified. Fingerprints do not change with time and are unique to each individual. However, there remains a need for an efficient system and method for identifying individuals to prevent identity fraud related to banking and credit transactions that is capable of identifying individuals at any location.

Summary of the Invention

The present invention relates to a method and a system that can be implemented , at least in part, as a computer program to verify the identity of an individual and monitor activity related to check cashing and credit reporting services.

The present invention helps prevent identity fraud by using biometric identifiers to verify the identity of individuals. The biometric identifier is captured at a remote location and can then be compared to either a local database or sent to a central server for comparison to biometric identifiers contained in a central database. If a match is found in the local database, the client (bank or other user of the system) sends a message to the central server to obtain the information regarding the identified individual. The central server first verifies the local match, but if a match is not found on the local database, or if the local database is not used, the central server tries to match the biometric identifier to verify an individual. If there is a successful match, the central server transmits information contained in data fields to the client regarding the matched individual. One advantage of the present invention is this system contains a large database, not restricted to a local region.

Another advantage of the present invention is that it is capable of being highly efficient when searching either a local or a central database to match a biometric identifier. The local database is smaller and thus faster to search than the central database. But, both of these databases are capable of being searched according to a tag or location. For example, a biometric identifier stored in a database can be tagged by the individual's last name, phone number, date of birth, etc. so that the entire database need not be searched according to the biometric identifier. This improves efficiency by filtering the database into a smaller database to be searched for a matching biometric identifier. Searching according to biometric identifiers is much slower than searching according to a tag or location. The faster tag searching eliminates identifiers not needing to be searched to determine a match, thus decreasing the total search time. Therefore, another advantage of the present invention is the efficiency associated with searching the databases for a matching biometric identifier.

Other advantages and aspects of the present invention will become apparent upon reading the following detailed description and the accompanying drawings.

Brief Description of the Drawing

In the accompanying drawings forming part of the specification, and in which like numerals are employed to designate like parts throughout the same:

FIGURE 1 is a simplified block diagram of an embodiment of a system in accordance with the present invention for identifying an individual to prevent check cashing fraud;

FIGURE 2 is an embodiment of a map of screens that can be provided to a user (e.g., bank teller) of the system of FIGURE 1;

FIGURE 3 provides an illustration of an identification page or screen in accordance with the present invention;

FIGURE 4 is a map of an embodiment of a finger scanning process in accordance with the present invention;

FIGURE 5 provides an illustration of an Office of Foreign Assets Control (OFAC) screen or page in accordance with the present invention;

FIGURE 6 is an embodiment of a map of screen that can be provided to a user (e.g., back management, staff, and the like) of the system of FIGURE 1;

FIGURE 7 provides an illustration of a customer list page or screen in accordance with the present invention;

FIGURE 8 provides an illustration of a mark transaction dialog in accordance with the present invention; and,

FIGURE 9 is provides an illustration of an edit customer notes dialog in accordance with the present invention.

Detailed Description

While this invention is susceptible of embodiments in many different forms, there is shown in the drawings and will herein be described in detail, preferred embodiments of the invention with the understanding the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the broad aspect of the invention to the embodiments illustrated.

Definitions of terms

Throughout the specification, the following terminology will be used:

1. Bank – Refers to one type of entity that can use the present invention. However, this invention is useful for many other organizations such as financial institutions, credit bureaus, credit card companies, and retail outlets that cash negotiable instruments, such as checks. Accordingly, these other organizations are included in the term bank for the purpose of this specification.
2. Customer – Refers to a person who wishes to cash a check or otherwise use the present invention to verify his or her identity.
3. Teller – Refers to a representative of the bank who can operate an embodiment of the present invention for assisting a customer in that customer's transaction. This term is also applicable to any other representative that uses an embodiment of the invention to verify a customer's identity.
4. Bank Network Controller – Refers to the person or persons who may be responsible for the operation of an embodiment of the present invention in any particular bank or other organization using the present invention.
5. Biometric identifier – Refers to a unique feature of a customer, such as voice print, palm print, finger print, facial recognition pattern, retinal recognition and so forth.

6. Biometric reader – Refers to any device for collecting biometric identifier data.

Overview of the system

The present invention can be implemented by any form of applicable technology, including but not limited to the following computer and circuitry types: electrical, digital, analog, optical, magnetic, mechanical, or any combination thereof. In addition, the system chosen to implement the invention can be general purpose, embedded, portable, networked, client/server, web server, database server, wireless or any combination thereof. In addition, user input can be obtained through various means including but not limited to keyboard, computer mouse, punch cards and speech recognition. Biometric input can be obtained through various means including, but not limited to fingerprint scanners, retinal scanners, voice scanners, video cameras, microphones, or any other scanners. Output devices include, but are not limited to cathode ray tube, light emitting diode, liquid crystal display, vacuum, fluorescent or plasma displays, speech synthesis, printers and plotters.

Referring to FIGURE 1, an embodiment in accordance with the present invention is shown. Three independent banks are represented as 1, 3, and 5. Bank 1 has multiple branches 7a, 7b associated with it. Any number of different branches and banks can use the present invention. Additionally, any number of teller stations can be located within each branch. For example, branch 7a has three teller stations 2a-c. Each bank 1, 3, 5 can have a data management client 13, 15, 17 respectively. The data management client can be used by an authorized representative of the bank to add data about individuals or transactions. Each teller station 2a-c is connected by an internal network to an external network and a central server (data center), although multiple central servers 20a-20c can be used to improve efficiency.

Each central server 20a-c has a copy of the central database 21a-c. The copies of the central database are identical. Each central database 21a-c contains biometric identifiers and associated identities with data fields about the individual corresponding to the identity of that individual.

An individual desiring to cash a check inputs at least one biometric identifier at a teller station such as teller 2a at branch 7a of bank 1. The biometric identifier is transmitted through the network to a central server 20a for analysis. The central server 20a searches its copy of the central database 21a for a matching biometric identifier. This can be accomplished using a single computer 23a or divided between many computers for improved efficiency. If the identifier is similar to multiple biometric files, the system will request and match an additional identifier to verify the identity. Once a match has been made, the corresponding identity and data fields are transmitted back to the teller station 2a for approval to finalize the check cashing transaction.

Bank Tellers

Each bank teller station has a computer running client computer software that implements an embodiment in accordance with the present invention. This client software provides a graphical user interface (GUI) both to capture information from the customer, which is sent to the central servers, and to display information returned from the central servers. The computer which runs the client software also has a biometric reader attached to it, usually through a universal serial bus (USB) port, though other connectivity modalities can be available depending on the particulars of the capture device. Optionally, the client software can also have a check scanner attached that reads the magnetic numbers at the bottom of a check. The present invention can also include a software development kit. There is a plethora of biometric reader devices manufactured by various corporations and it would be cumbersome to develop software for each reader. The software development kit incorporates many other reader software development kits into one so the system software can be developed independent of the devices.

During a transaction, the client software captures information about the customer, including a biometric identifier, and optionally captures information about the check itself. This information is sent to the central servers. The particular central server that the teller station uses is dynamically reconfigurable from the central servers. This allows the flexibility to effectively balance the load on the biometric identifier matching engines.

Transmission Protocol

When the data is sent from the client software to the central servers, it is sent using a protocol. The data is packaged up according to this protocol, and encrypted using a public key cryptographic system. This protocol can be replaced with a different encryption protocol if desired. In public key cryptography, a pair of keys, which are mathematically related, is generated. One of these keys, the public key, can be used to encrypt a message, but not decrypt it, whereas the other, the private key, can be used to decrypt the message, but not encrypt it. The public key is not secret since it cannot be used to decrypt the message.

In this system, each teller station has its own public and a private key. The public key for each teller station is known to the central server, and that key is used to encrypt each message sent from the central server to the teller station. When it is received, the teller can use its private key to decrypt the message.

Additionally, for each teller station, the central server has a public and a private key. That is to say, the central server has many public/private key pairs, one for each teller station. Whenever a teller station wishes to send a message to the central server, it encrypts it with the specific central server public key allocated to that teller station. When the central server receives the message, it is decrypted by the corresponding private key. This multiple use of asymmetric public key cryptography greatly increases the security of the system by making key distribution secure. Additionally, even if one encryption key was broken, the system is not compromised because only one client key was decrypted, leaving the remaining system secure.

The communication protocol provides for the following functions:

1. Identify this person – Requests the person whose biometric identifier is provided in the protocol be identified, and information about that person be returned. This protocol goes from client to server.

2. Enroll this person – Requests the person who's biometric identifier is included in the protocol be enrolled in the system. This protocol travels from client to server.

3. Request received – This informs the client that the central server has received the request and is beginning to process it. This protocol goes from server to client.

4. Request reroute – This corresponds to the request received protocol, but it informs the client that subsequent requests should be sent to a different central server and also includes the IP address of the new central server in the protocol. This protocol goes from server to client.

5. Identification result – Returns the result of an identification request containing all the information that the specific bank is privy to. This protocol goes from server to client.

6. Enroll successful – Returns an indication that the enrollment was successful. This protocol goes from server to client.

7. Duplicate enrollment – Returns a result very similar to Identification result, except it is returned in response to an enrollment request (Enroll this person), but the enrollment failed due to duplication. This protocol is sent from server to client.

8. Adjust data – This protocol is sent from a data manager station at a bank to adjust some fields in the central database concerning a particular individual. This protocol is sent from the data management client to the server.

9. Adjustment result – Returns an indication of the success or failure of an Adjust data request. This protocol is sent from the server to the data management client.

10. Download new client GUI – A process whereby the data management software downloads GUI details to the front-end software. This is a process to allow the bank managers to change how the teller screen looks and automatically download that new look and feel. This protocol is sent from the server to the client.

11. Send me a local database image file – A process whereby the local machine can download a local database for biometric data searching. By doing some of the searching locally it greatly reduces the load on the central servers. The central server determines which biometric data to put in the database. The local database is a set of biometric data, and an associated customer identifier. This protocol is sent from the client to the server.

12. Local Database Message – This message is in response to "Send me a local database image file." It contains the requested local database of biometric data for searching. The client machine should cache the local database in a local encrypted file until the server indicates that a new local database is required. This protocol goes from the server to the client.

13. Person identified – This indicates the local database has successfully identified the individual in question and requests that the central server fill in the remaining data fields for that person such as name, address, transaction log, etc. The server responds with a standard identification result message. However, the identification message result can be preceded by "Update local database." This protocol goes from the client to the server.

14. Update local database – This message is sent when a "Person identified" message indicates that the local database is significantly out of date. It contains a list of instructions to add, remove or change biometric data in the local database. It can also contain a single flag indicating that the database is too far out of date and that a new local database should be requested. This message goes from the server to the client.

15. Request local database encryption key – The local database is stored on the local disk in an encrypted fashion. This protocol requests the encryption key, which is stored only on the central servers. This protocol goes from client to server.

16. Local database encryption key reply – This message is in response to the previous message and contains a reply containing the local database encryption key. This message goes from server to client.

Central Server (Data Center)

The central servers are responsible for processing requests from the clients. Each central server has the following responsibilities and functions:

1. Biometric matching – A set of computers is used to match a biometric profile sent from the client to one of the stored biometric files in the database.

2. Database operations – A database performs a number of different functions, such as finding data about a customer when the customer's fingerprint is matched; enrolling data about a customer when the customer's biometric identifier is not matched during an enrollment; performing transaction detail based analysis of a transaction, such as looking for bad checks, stolen check stock, and terminated employees; modifying a person's record in accordance with the user request or from the data management client software; determining information a bank is entitled to view; managing the downloading of new GUI front ends to the tellers; determining the central server associated with each teller station; and logging information.

3. Legacy check verification – Banks maintain records of checks that are fraudulent. These checks can be scanned into the system and the information can be used to mark existing individuals and new enrollments that have previously committed check fraud at other banking institutions.

4. Logging operations – This function is closely related to database functions. However, it is considered separately since it has a fundamentally different character. This process logs every transaction request and response. It is designed so that any transaction can be accurately redisplayed, including all the detail transmitted to the teller. Additionally, this process is responsible for storing graphical images of every biometric file sent through the system. The log can also be printed.

5. Validation of drivers' license numbers – This function verifies each individual's driver's license number.

6. Validation of social security numbers – This function verifies each individual's social security number.

7. Compliance with OFAC regulations – This function assists in ensuring that the individual is not a Special Designated foreign national.

Data Management Client

The data management client enables the managers of each bank to input information about bad checks and other commentary on individuals and transactions. It allows the following actions:

1. Annotate an individual who enrolled at the bank – Permits a manager to categorize an individual with a comment and a seriousness comment, levels one through ten. Depending on the severity of the comment level, the comment will be displayed more and more aggressively to the teller when this person is accessed.

2. Annotate an individual transaction performed at this bank – This allows the manager to annotate a particular transaction even if the individual was not enrolled at the bank. This might arise should someone enrolled elsewhere cash a bad check at a different bank.

3. Delete an individual enrolled at the bank – This is a process which allows an individual to be deleted from the system should he or she be enrolled at that bank.

4. Viewing transaction logs – Allows the system to view transaction logs in a variety of ways, including by branch, by teller, by company, by account and by person. It also allows filtering by company and amount.

5. Configure a bank's sharing parameters and various other configuration details – Each bank can designate which fields it shares out of its portion of the database. Preferably, this must be done in cooperation with the central server. The user of the data management software can use it to make requests to the central server, however, the final installation is preferably done at the central server headquarters after discussion with appropriate authorities at the bank.

6. Add or delete extra fields collected on each user and transaction – The user of the data management software can use it to make requests to the central server, but the final installation is preferably done at the central server headquarters after discussion with appropriate authorities at the bank.

7. Set up a new GUI front end for the bank – The user of the data management software can use it to make requests to the central server, however, the final installation will preferably be done at the central server headquarters after discussion with appropriate authorities at the bank.

Personal And Transaction Database

Each individual bank has the ability to configure its portion of the database in a manner consistent with its particular policies. The database makes two areas available to the banks: personal data, which contains information about an individual with a particular biometric identifier; and, transaction data, which contains information about the transactions an individual has performed. Each area contains a number of fields of data about the person or transaction. For example, personal data contains the name in one field, the address in a different field and so forth. Each bank can choose which fields it wants to share and which it wants to keep private. Additionally, each bank can also add custom fields of its own to either set of data. For example, a specific bank can want to collect a customer's height, and eye color as an additional identification criteria. This bank can legitimately add that field, and either share it with other banks or not share it.

When a bank opts to share a particular field, it makes that bank's data on that field available to all others who are also sharing the same field. Thus, sharing the field also gives one access to that data from other banks. If one does not share a field, one cannot view other bank's information in that field. Additionally, a bank can choose not to include a particular field in its database. In such case, that field is left blank. However, it is preferred that both areas have some fields that are mandatory and must be included and shared. Examples of these fields are listed below in Table 1.

In one embodiment, the required fields that preferably must be shared for each individual are: name (title, first, middle initial, last, suffix), address, date of birth, gender, social security number and driver's license number or alternative identification. The required fields that preferably must be shared for each transaction include the last name, the first name and the amount of the transaction.

Name	Address
Biometric data	Enrolling Bank
Date of enrollment	Driver's license number
Comments	Payee
Payor	Account number

Check number	Date of transaction
Transaction number	RTN number
Check stock number	Teller system field code

Table 1. Possible mandatory fields.

BIOMETRIC DATABASE

Image Files Verses Biometric Codes

The following description discloses an embodiment of the present invention using fingerprints to identify individuals. Other forms of biometric data can also be similarly used.

Generally speaking, it is impractical to compare the specific images of two fingerprints to determine similarity or identity. There are several reasons this is true, but the principle reason is that such a comparison would be extraordinarily slow. Consequently, before a comparison is made, a feature extraction algorithm is run on the fingerprints to identify crucial points of comparison. Specifically, fingerprint algorithms find certain points of ridge bifurcation and end points, and use their positions and the angles of the ridge as a biometric code describing the fingerprint. Each individual fingerprint has a set of these so-called "minutiae points," and all fingerprint comparisons take place by comparing these sets of biometric code in particular ways. Such codes allow the fingerprint algorithms to more easily compensate for the major problems in comparing images, namely the translation, and rotation of the two images, in addition to the elasticity of the skin in the finger causing other types of distortion.

Finally, biometric codes can largely ignore spots, scars and other blemishes. These biocodes can be readily generated from a fingerprint image. However, the reverse process, converting a biocode into a fingerprint image, is not possible. It is necessary therefore, if it is desired to reproduce the exact fingerprint, to store both the biocode and the fingerprint image. Biocodes are typically a few hundred bytes in length, a size which can readily be stored in a database. However, images/files are several dozens of kilobytes, which preferably must be stored in separate files. It should be noted that the above principles similarly apply to other types of biometric identifiers, including facial recognition, retinal recognition and voice scan.

Image File Storage

Each fingerprint image is stored in a separate file. An image of every fingerprint read by the system is stored, including enrollments and authorizations. This enables the system to recreate any transaction in detail. Each fingerprint image is stored under a file name with a numeric code corresponding to its 64-bit identifier in the database. The fingerprints are stored in a “tree-like” data structure in the file system where the file path to the picture corresponds to the file name. Each file is stored in standard jpeg format.

Database History And Purging

To reduce the amount of searching required on fingerprint records, the records are regularly purged. All personal records free of negative comments that have not been accessed in the previous year are removed, along with all attached transaction records. This process is performed overnight while the database load is very low.

BIOMETRIC SEARCHING TECHNOLOGIES

Exhaustive Searching

Whenever searching a database of biometric identifiers, two results are possible, either the identifier is found, or it is not found. Both these results are useful under different circumstances. For example, when trying to identify an individual based on a fingerprint, it is obviously necessary to find a matching fingerprint in the database. However, it is also useful to know that there is no match. For example, when enrolling a new user, it is useful to know that the individual’s fingerprint is not enrolled anywhere else in the database to guarantee unique enrollment. Consequently, the present invention has two important processes: searching for a match, and determining that there is no match. The most straightforward way to perform both of these processes is by exhaustively comparing every fingerprint in the database with the scanned fingerprint. But this can be very expensive. One goal of the present invention is to reduce exhaustive searching as much as possible. This is accomplished by organizing the order in which the fingerprints are searched in such a way that the system is more likely to encounter a matching fingerprint first. The following description outlines approaches to accomplish this goal.

Parallel Searching

Whenever a biometric identifier is received into a central server and slated for identification by exhaustive search, it is submitted to several searching computers at once. The complete database of biometric identifiers is divided up equally among the searching machines. The size of the database searched by each machine depends on the performance of that machine.

When an exhaustive search is made, the same biometric identifier is submitted to all the searching machines simultaneously, and they all search their databases in parallel. When one search engine matches it signals that a match is found, searching on all other machines for that biometric identifier stop.

Depending on load considerations and on the number of transactions per second, computing resources can be allocated appropriately. The database splits into fractions, called f1-fn. When the number of transactions is low, each fraction sits on one searching computer. However, should the number of transactions justify, fractions can be placed on several computers at once. This means that not only can the system allow one biometric identifier to be searched for on multiple machines at once, but one can also have multiple fingerprints searched on multiple machines simultaneously.

Geographic Fractional Searching

Geographical fractional searching is useful for eliminating excessive use of the central server based on the observation that most likely a biometric identifier is going to be used near the place where it is enrolled. This is a straightforward observation because people generally tend to stay in the same location for long periods of time. Consequently, if the fingerprints in the database are sorted by the zip code where individuals get registered, then the system can search according to the zip code where the fingerprint is obtained, thus, the system is more likely to find a match quickly.

However, a zip code is generally too exact a value, since individuals regularly travel outside their zip code area, but still remain nearby. Consequently, a faster search based on the surrounding zip codes can be performed. One embodiment sorts identifiers according to the first three digits of the zip code where the identifier was enrolled. What this means is that when searching for a biometric identifier, the system first looks at all the biometric identifiers enrolled in nearby zip codes as the location where the biometric identifier was obtained, to find a match. This heuristic works well in both types of search. If the system is searching to match a biometric identifier, it will most likely find a match early on. However, if the system is performing a search to determine that there is no match, it will most likely hit on the erroneous match early in the searching process. This expedient reduces the cost of searching a database of fingerprints.

Tagged Searching

In tagged searching, an additional tag can be used to further reduce the number of biometric identifiers to be searched. But tagged searching is only useful for finding a matching biometric identifier; it is not useful for determining there is no match. A tag can be something easily entered into the system, such as an encoded last name, a birth date or a phone number.

When using a last name as a tag, it has been found that a fuzzy matching system such as Soundex or Metaphone provides an ideal tag. It has been determined through experimentation that such an encoding can reduce the number of biometric identifiers searched. On average, such searching requires one five hundredth of the number required otherwise, with a relatively flat peak behavior on extremely common last names.

The process involves tagging every biometric identifier with a code indicating the Metaphone encoded last name of that biometric identifier's owner, and comparing the tag against the last name before the biometric identifier comparison is made. It is much less expensive, in terms of performance, to compare the encoded last name than to compare the biometric identifier itself. It is estimated to be ten thousand times quicker, depending on the specifics of the implementation. Consequently, this is a valuable tool to reduce the cost of searching.

Tagged searching is also useful for quickly identifying duplicates when an individual is attempting to enroll in the system. When searching for a duplicate enrollment, the system performs a preliminary search to find any duplicates based on a tag because this method is much faster. If no duplicate is found, the system continues to perform an exhaustive search for the biometric identifier to determine if a duplicate exists.

However, this process of tagged searching has two major problems. First, it requires extra data entry, requiring the teller to enter the last name of the person along with his or her biometric identifier. Second, it only works if the last name supplied is the same as the one in the database. Should a false name be given, that biometric identifier will not be matched. In general, this can be acceptable if one is trying to identify the person, since a failed identification match requires an enrollment. The enrollment process finds the already enrolled biometric identifier because the system performs an exhaustive search to verify that the biometric identifier does not already exist in the system.

Localized Searching For Load Distribution

A third heuristic of the present invention to reduce the load on the biometric identifier database is to do some of the searching on the local computers. In particular, the system can download a part of the biometric identifier database onto the teller station computer. The teller station computer then searches this part of the database for a matching biometric identifier. If the search matches an identifier, then the client sends a protocol message to the central server to obtain the details of the matched person. Otherwise the client asks the central server to perform a full search. If the teller station matches an identifier, the central server will still match the identifier contained in its database to the suggested match to verify the individual and protect the security of the system. This process allows the system to offload some of the processing of biometric identifiers onto the client's machines, which greatly reduces the amount of processing the central server performs.

The protocol for this is straightforward. On initialization, the teller machine sends a message to the central server requesting the local database. The central server algorithms decide which are the best biometric identifiers to send. The easiest algorithm is to send the biometric identifiers matching and surrounding the teller station's zip code. This data is stored in an encrypted file on the teller machine and also held in the machine's memory. When a search is commenced, the teller station performs the search, and when a match is found, the client machine sends the result of that match to the central server. Again, the central server compares the proposed match with the identifier contained in its database to verify the individual. If a match is not found, then a standard search is performed using the central server rather than the local machine.

When a local search is performed, the local machine also sends a date and time code back to the central server. This date and time code reflects the last time the local database was updated. If the local database is older than a predetermined date, the central server sends a protocol message containing information that the local machine can use to update its local database. This information is applied to the memory search image, and then saved in encrypted format into a file on the local machine's hard drive. This information consists of adding new fingerprints, deleting old ones and changing existing ones. The encryption key for the local file is stored at the central server, not on the local machine. The encryption key is provided over an encrypted channel when the teller station requests it and it is never saved anywhere on the local machine. This prevents the proprietary database information from becoming exposed if a hacker were to gain access to the local machine.

When the client software is first installed, it requests a local database from the central server according to its home zip code for use in localized searching. The client software first performs a test to determine if the local machine is capable of performing local client searching. A database is transferred to the local machine and is stored as a cached file on the local hard drive. Subsequently, whenever the client software is run, it determines the encryption key of the local cached database by requesting the local database encryption key from the central server. This key is used to decrypt the cached file in the machine's memory. Whenever an identification is requested by the software, it first searches for the biometric identifier in its local database. If it is found, then a request for the information, the biometric identifier and corresponding identification number, are passed to the central server. The central server verifies the biometric identifier matches the identity proposed by the client. Additionally, this message contains the date and time that the local biometric identifier database was last updated.

The server looks at the date the biometric identifier database was last updated, and if necessary, sends a list of changes the local database must preferably make. Alternatively, the server can send a message indicating that too many changes have taken place and a new local database should be downloaded. Next, the server verifies the proposed identity from the client with the biometric identifier contained in the database. Finally, the server sends a standard identification message giving the client software a full set of information about the customer. If the local machine cannot identify the customer from its database, the local machine sends a standard identification request to the central server, as if the local database had never been consulted.

Automatic Load Balancing

The central servers constantly monitor their loads and response time, and identify central servers and computer systems that are overloaded. Using a dynamic balancing algorithm, the system reallocates some of the tellers to different central servers to compensate for this problem.

Enrollment Propagation

In a multiple central server environment, it is desired to keep all central servers up to date with new enrollments. To do so, the central server receiving the enrollment request sends a message to each central server indicating an enrollment of that fingerprint is taking place. Whenever one of the other central servers receives such a message, it is stored on a list of pending enrollments. Whenever a central server performs an enrollment, it first matches against the pending enrollment list. If a match is found, the enrollment is delayed until the original enrollment is complete. When the original enrollment is complete, the central server stores the information in the database, passes the new biometric identifier and corresponding personal information to the other central server to store in their memory databases of biometric identifiers. Finally, the biometric identifier is removed from the pending enrollment list. Subsequently, the delayed enrollment will be allowed, and the duplicate will be found and dealt with in the normal manner.

Biometric Identifiers Obtained in the Enrollment Process

Preferably, when an individual seeks to enroll in the system, at least two biometric identifiers are obtained. One acts as a primary identifier and the other as a secondary or backup identifier. For example, in an embodiment of the present invention utilizing fingerprints, two fingerprints would be obtained. The reason for this is because there is a limit to the degree that two fingerprints can be distinguished when they are very similar. When the individual attempts to enroll, the system performs a search to verify that the individual is not already enrolled. If the central server finds a match or very similar fingerprints, the system automatically notes that those individuals must preferably also provide an additional fingerprint to verify his correct identity for each transaction because they are potentially duplicates.

At enrollment, the present invention also automatically requests identifiers according to a predetermined priority. For example, in an embodiment utilizing fingerprints as identifiers, the system automatically requests certain fingerprints from the individual. If the individual is missing any of the requested fingers, the system proceeds down the list of priority identifiers. The list of priority for the primary identifier follows in order (fingers): right index, left index, right middle, left middle, right ring, left ring, right pinkie, left pinkie, and finally left thumb. The list of priority for the secondary identifier follows in order (fingers): right thumb, left index, right middle, left middle, right ring, left ring, right pinkie, left pinkie, and finally left thumb. If the first available finger on the secondary list is already being used as a substitute for the primary identifier, then the next on the list will be used as a substitute for the secondary identifier.

Overview Of the Search Process

In an embodiment, an overview of the steps in the searching process is as follows:

1. A biometric identifier is searched in the local database (optionally).
2. If a match is found, the central server verifies the proposed match from the local database with the identifier contained in the central database.
3. If a match is not found, the biometric identifier is sent to the central server.
4. If the biometric identifier is tagged, it is initially searched according to the tag.
5. If the biometric identifier is not tagged, it is searched according to Zip code geographical fractioning.
6. If geographical fractioning fails then the biometric identifier is searched for exhaustively.

Once the biometric identifier is identified, the database is used to decorate this biometric identifier with all data relating to that person, and also all recent transaction data performed by the person viewable by the bank. Any of the above steps except step 6 can safely be removed without affecting the outcome of the search, though obviously impacting the performance of the central servers.

Biometric Identifier Identification Tasks

1. Enrollment – This is a process whereby a person who is not associated with the database can enroll his or her biometric identifier in the database for future check cashing processes. Preferably, every person using the system must first enroll in the system.

2. Fraud Check – This is a process whereby a person can identify himself or herself using a biometric identifier to verify that he or she has used the system without fraud. Banks can use this information as a basis to decide whether or not to cash a check.

3. Off line enrollment – This process is similar to regular enrollment, but it is performed outside of the bank at the human resource departments of the companies whose employees wish to cash checks.

Information Displayed

The software displays a person's identity such as his or her name, address, and a number of other fields specified by the bank. The system can optionally display a photograph of the person. The system also displays any messages attached to this person including any messages attached to transactions they performed. This allows the system managers to alert the teller of problem customers. The system manager can also display alert messages such as pop up windows that list specific urgent issues with particular customers. The system also lists any recent transactions this person has had with the system, allowing the teller to see when a person is cashing several checks at several different banks, a situation that usually indicates a fraud in progress.

Check Verification Tasks

Stock Number – The database keeps a list of stolen check stock numbers. Every check is compared to the list of stolen check stock numbers.

Check Number – The database keeps a list of stolen check numbers. Every check is compared to the list of stolen check numbers for the specific account the check is drawn against.

Stop Limit – The database can set a limit on the size of checks that can be cashed on a particular account.

Ex-employee alert – The database alerts the teller when someone who has been fired from a company is trying to cash a payroll check after his or her termination. Facilities are provided to allow the cashing of the final paycheck.

Sharing and updates

Sharing information – One of the features of the present invention is the ability of banks to share their fraud information with other banks. This is largely configurable, allowing each bank to decide on a field by field basis which information to share. A bank can receive information from any data field that it shares with the other banks.

Reconfiguration of the data stored – In addition to certain standard fields, the banks can, at their discretion, collect other types of data from the teller station. For example, a bank might wish to collect an individual's height and/or weight at the time of enrollment.

Downloading of front ends – To facilitate the use of the present invention, the bank can redesign the GUI screens that the teller views. The present invention processes these files and automatically download them to the teller stations.

Analysis and Reporting

Additional unique aspects of the present invention include analysis and reporting functions. Individual banks are allowed to manipulate and interact with their data through a network connection that allows them to generate a number of different reports. For example, each bank or branch can request non-customer transaction reporting. This information can include the number of non-customer transactions, the monetary value of non-customer transactions, and the number of fraudulent non-customer transactions at a bank's various branches. Another aspect of the analysis and reporting functions allows a bank to determine the identity of non-customer individuals that cash checks at their locations and track the types of transactions conducted. This information can be utilized for fraud protection and to market different products to customers and non-customers. The analysis and reporting functions can also be utilized to develop trends for customers, bank branches, and tellers. For example, a trend analysis can be run for each teller to determine if any tellers might possibly be involved with fraudulent transactions. Another example allows a bank to inquire about the volume of transactions during various timeframes to add additional tellers to assist customers. Additional analyses can be performed to meet the specific needs of each bank or branch.

Example 1

Enrolled Customer Wants to Cash a Check

An enrolled user enters a bank, and tries to cash a check. An embodiment of the present invention proceeds through the following steps. The individual's name, right index finger and right thumb, if required, are collected by the teller and entered into the client software. Optionally, the check is also scanned using a check scanner, or the check data is entered by hand. This information is packaged up, encrypted and sent to a designated central server. The information is received by the central server, is unpackaged, and decrypted. The central server uses various algorithms to identify the person with the given fingerprint. Having identified the person, his or her information is looked up in a database, including personal information, and check transaction information. This information is packaged up, encrypted and returned to the same teller station. The information is decrypted and displayed on the screen for the teller. The information is also logged by the central server.

Example 2

An Unenrolled Customer Wants to Cash a Check

In this scenario, a person wishes to cash a check, however, they are not currently enrolled in the system. The person approaches the teller, the teller questions the individual and determines that they are not enrolled. Then the teller clicks the enroll button on their software. The enroll process is used to capture various basic pieces of information, such as name, address and so forth. The enroll process captures several copies of the individual's right index fingerprint or next available primary substitute. Next, the process captures several copies of the individual's right thumbprint or next available secondary substitute. The biometric and personal information is packaged up, encrypted and sent to a designated central server. The information is received at the central server, unpackaged, and decrypted. The central server uses various algorithms to search, comprehensively, for a matching primary fingerprint in the database. If a similar primary fingerprint is found, the secondary fingerprint of each identity is compared to verify if they are duplicates or just similar. The purpose of this search is to eliminate dual enrollments. If no match is found, the data is entered into the database and the new fingerprint is distributed to the various central servers. A confirmation is packaged, encrypted and returned to the teller station. Additionally, the event is noted in the log. If a fingerprint match is found during the search, a message indicating a duplicate enrollment is packaged, encrypted and returned to the teller station. Additionally, the event is noted in the log. The teller station receives the message, unpacks it, decrypts it and displays the information on the screen. All logged information can be printed at any time.

The present invention can be used for increased security for check cashing transactions at banks as well as at many other financial institutions such as credit bureaus. The present invention uses a central server and central database to ensure that an enrolled individual can cash checks or perform other transactions at any bank connected to the central server. The present invention is not limited to branches of an individual bank, but can be used by any and all banks connected to the system. Whatever data fields a particular bank shares can be accessible to that bank about individuals that were not enrolled at that bank. This sharing of information makes the present invention extremely useful for preventing check cashing fraud because an individual's banking history can be available to other banks. The individual's history with other banks can provide insight to his or her propensity to commit fraudulent transactions.

Not only is the present invention useful to many separate banks, but it also operates efficiently. Optional tagging can be used to increase the speed at which biometric identifiers are matched in the system. Additionally, local databases not only improve that speed of biometric identifier matching, but also reduce the load on the central servers.

Turning to FIGURE 2, a map of screens is provided wherein each screen can be provided on a visual display associated with one or more users of the system (i.e., bank tellers). The screens 210 include a main screen or page 212, an identification screen or page 214, an enroll screen or page 216, an already enrolled screen or page 218, a change credentials screen or page 220, and a configuration screen or page 224.

In an embodiment, the main page 212 is the entry point for the system and is displayed when the program first starts. From this page the teller can reach all other functions. Inputs on this page can include a name input box for entering a customer's name (e.g., first, last, middle initial, and suffix) and a dollar amount for the check being presented by the customer to the teller.

The main page 212 can also include command icons or buttons (not shown) wherein, by selecting an icon, commands are executed such as OFAC, Identify, Enroll, and Exit. The OFAC command causes the system to perform an OFAC check on the customer's name as entered in the main page. In an embodiment, the OFAC check is an exact match comparison against a U.S. Treasury OFAC list. If a match is found, the OFAC match dialog box is show, if no match is found, a message saying so is shown.

The Identify command on the main page 212 causes a request that a person be identified, and a check associated with that person be cashed. As a result, an authorization dialog box 224 is displayed to collect a fingerprint. Using the fingerprint and the last name of the person, the system attempts to identify the person. Should the name and fingerprint match one enrolled in the system database, the identification page 214 for that person is displayed. If the person is not identified, then the user (e.g. bank teller) is informed of this and offered two choices: 1) either click OK or Cancel to terminate the operation, wherein the input fields are cleared and the main page 212 is displayed again; or 2) attempt to enroll this person in the database, wherein the enroll page 216 is displayed with the name from the name input box is pre-filled into that page's form.

In an embodiment, the failure to identify the person using the Identify command does not mean that the person is not enrolled; instead, it simply means that they are not enrolled under the last name given in the name input box. Should a person be enrolled under a false name, they would not be correctly identified at this stage. However, should they subsequently try to enroll, their possible mendacity will be discovered, since the enroll process checks all fingerprints in the database, regardless of which name is used.

The Enroll command on the main page 212 results in the enroll page 216 being displayed. Further, the Exit command causes the software to exit.

Turning to the identification page 214, this screen shows information about a person such as enrollment information and recent transactions. If the customer is submitting a check for cashing, the information about this check is also displayed. The identification page 214 allows the user to indicate the disposition of that check comprising the choices of: accepted, rejected or abandoned. Preferably, a user may not use the file exit command from this page, or close the identification page in any other way, since that would leave a transaction without a disposition.

In an embodiment, any transactions performed by the identified person that satisfied the following criteria are shown on the identification screen 214: 1) all transactions performed in a defined time range such as the past 30 days; 2) all transactions that have been marked in the back office; 3) all rejected and abandoned transactions; 4) all duplicate enrolls (including re-enrolls); and, 5) all enrolls.

Turning to FIGURE 3, preferably all transactions that have been marked in the back office, all rejects, and all duplicate enrolls (excluding re-enrolls) are displayed first in a transaction list 310 provided on the identification page 214, wherein the most recent transaction is displayed at the top of the list. Additionally, all transactions of that nature are further highlighted by having a background color such as, for example, light gray.

After that, all other transactions are shown on the list 310 with the most recent first. The last entry in the list is preferably the initial enrollment of the person. Each transaction lists the date on which it took place, the time, the bank's name and the name of the location, the amount of the check, the disposition of the check, and, if desired, any additional notes.

Enrollment transaction summaries are shown as successful enrollments, duplicate enrollments, and re-enrollments. A successful enrollment transaction summary provides the date and time of the enrollments, along with the full name under which the person enrolled. A duplicate enrollment transaction summary provides the date of the duplicate enrollment, the full name under which the person used when attempting a duplicate enrollment, and the words "DUPLICATE ENROLL" highlighted in red. A re-enrollment is defined as an attempt to re-enroll in the system using the same name or social security number. This is considered a re-enrollment since it is unlikely that the person is attempting fraud, rather they are simply trying to re-enroll and had forgotten that they were enrolled. These types of transactions preferably do not appear at the start of the list 310 and are not highlighted since they are not considered important indications of fraud. A re-enrollment transaction summary provides the date and full name under which the person used when attempting a duplicate enroll.

The identification page 214 also shows the name and address of the person trying to cash the check, and the details known about the check. As stated previously, the bank can enter notes about a person using the back office software as described in detail further herein. Preferably, notes are not shared among banks. In an embodiment, there are three types of notes: 1) regular notes that appear in the area below the person's name; 2) pop up notes that appear below the person's name, but also are displayed in a pop up box when the page is first displayed, and also when the show alerts button or icon is selected; and, 3) cancelable pop up notes, that are displayed the same as regular pop up notes, however, they also have a cancel button or icon on the pop up box. When the cancel button is selected, and a confirmation is accepted from the teller, then that note is permanently cancelled for that user (i.e., teller).

In an embodiment, the identification page 214 can be reached without submitting a check by performing an identify from the main page 212 with the check amount filed left blank. If this occurs, a number of differences appear in the visual display of the identification page 214. In particular, the check information is left blank, the three buttons or icons for accepting, rejecting and abandoning the check disappear, and a new OK button appears in the middle of the area where the accept, reject and abandon buttons are shown on a regular identification screen or page 214 shown in FIGURE 3.

The command icons or buttons available on the identification page 214 include: Show Alerts; Change; Accept; Reject; Abandon; OK; and Close. The Show Alerts command causes the pop up box that was originally displayed when the identification page appeared to be redisplayed. The Change command causes the change credentials page 220 to be displayed with the fields filled-in for this person. After the OK icon or button is selected, the same identification page 214 is redisplayed, allowing the teller to mark the disposition of the check. If the teller selected the Change command to make changes, and then, after returning to the identification page selected the Change command again, a warning is first displayed, telling the user that the changes they made in the previous invocation of the Change command will not be shown in the change screen and must be re-entered if they proceed. This gives the user (i.e., the teller) the choice to abandon going to the change credentials page, or proceeding anyway.

The Accept command causes the transaction to be marked as an accepted (i.e., cashed) check. After marking the transaction, the main page 212 is redisplayed. This command is not available if the identification page 214 was entered without a check to be cashed.

The Reject command causes the reject dialog to be displayed, and the result is used to mark the check with the selected rejection reason. After marking the transaction the main page 212 is redisplayed. Preferably, this command is not available if the identification page 214 was entered without a check to be cashed.

The Abandon command provides a shortcut to marking the transaction as an abandoned transaction. After selecting this icon or button, the transaction is marked as abandoned, and the main page 214 is redisplayed.

The OK icon or button preferably only appears if the identification page 214 was entered without a check to be cashed. When the button is selected, the system displays the main page 212. Further, the close button or icon allows the user to close the application if the identification page 214 was entered without a check to cash.

As indicated previously, the enroll page or screen 216 enables a user such as a teller to enroll a customer into the system. The inputs provided on this page include: name, social security number, gender, address, date of birth, drivers license, additional information, and an optional notes filed. In an embodiment, entry of the social security number is not mandatory.

The commands that are available for execution from the enroll page 216 include Next and Cancel. The Cancel command results in the main page 212 being displayed. Further, the Next command causes an enroll dialog 226 to be displayed. If the enroll dialog 226 is cancelled, then the user is returned to the enroll page 216. However, if OK is selected, and the fingerprints are acceptable after being entered as explained in detail further herein, then the person is enrolled in the database. If the enrollment it is a re-enroll (i.e., a duplicate enrollment wherein the name or the social security number is the same), then a message box stating such is displayed. Selecting OK on the message box results in the system displaying the main page 212. . If the enrollment is detected as a duplicate enroll, and the name and social security number are different, the already enrolled page 218 is displayed. In either case, a transaction is stored in the database. If the enrollment is successful, a dialog saying so is displayed, and on selecting OK, the main page 212 is displayed.

The already enrolled page or screen 218 provides a warning to a user (i.e., teller) that a person is attempting to enroll a second time in the system. The inputs available on the page 218 are the same as provided in the enroll page. However, they are pre-filled with the values supplied by the enrollee at their first enrollment. Additionally, the fields cannot be edited.

The change credentials page or screen 220 allows a user such as a teller to change a customer's information. The inputs available on this screen include the same set of fields as provided on the enroll page 216. However, the fields on the change credentials screen are pre-filled with the values supplied by the enrollee at their enrollment, or the last value from the last credentials change. Additionally, the notes field may be omitted from this page.

The commands available from the change credentials page include: OK and Cancel. The OK command results in the changes being made to the database. The Cancel command results in the system reverting back to the original transaction list without committing the changes to the server.

The configuration page or screen 222 allows a user to view the configuration of the software. The inputs available on this screen include: Teller ID; Delay Sending Images; and, Message File. The commands available on this screen include: Test; Update; and, Close.

The Teller ID is a standard numeric file that contains the teller identification. If this field is zero, it indicates that the bank does not distinguish between teller stations.

The Delay Sending Images input is a check box that, when checked, causes the software to omit fingerprint image files from transmission to the server. Instead, they are cached in the directory indicated on the configuration page. In an embodiment, a separate program runs the scheduler to upload these files at a later time when more network banding width is available and when a customer is not waiting for a response. The Message File input is a file name text box to access the message file as described in greater further herein.

The test command is an icon or button that, when selected, results in a testing of communication with the configuration server. The results of the test are provided in a message box that indicates whether communication was successful or not.

The Update command causes the software to re-read its configuration from a central website or server. The fields on this page update to reflect the new configuration. Further, the Close command closes the configuration page 222 and returns the user to the main page 212.

The authorization dialog 224 is a dialog that collects a single fingerprint to identify the person. In an embodiment, the dialog will time out if it is left unattended for a time period of, preferably, five minutes. The input to the authorization dialog 224 is the fingerprint read from an external piece of hardware, which can be plugged into a port such as a USB port or other input port. The commands to the authorization dialog 224 include: Start Scanning; Alternative Finger; and, Cancel.

The Start Scanning command causes the reader to start scanning the fingerprint. If the fingerprint is a poor quality image, a dialog indicates so and allows the user to either try again, or cancel, which closes the dialog.

The Alternative Finger command causes the alternative finger dialog 225 to be displayed as described in detail further herein. When the authorization dialog 224 returns, it indicates to the user (i.e., teller) what finger they should scan. Further, the Cancel command closes the authorization dialog 224.

The alternative finger dialog 225 allows a teller to specify which fingers the customer has, should they be missing a right index and right thumb. The teller specifies the situation in the dialog, and then the dialog follows a protocol to decide which finger(s) will be used as a substitute. The input for the alternative finger dialog 225 includes a radio button for each of ten fingers wherein the teller indicates if the finger is intact, damaged, or missing.

The command available from the alternative finger dialog 225 consists of an OK command wherein, by clicking or selecting this command, the dialog goes away and adjusts the calling dialog to specify the correct alternative finger. For the primary (first finger), the calling dialog selects the first of, right index, left index, right middle, left middle, right ring, left ring, right pinkie, and left pinkie. For the second finger, the calling dialog requests the right thumb first, then the first of the preceding list that is not used as a primary identifier, and as a last resort the left thumb is used. In an embodiment, if a person has less than two fingers, then they cannot use the system.

As indicated previously, the enroll dialog 226 allows a user to enroll in the system. The dialog 226 collects three copies of two different fingers and produces an average of each set of three images to obtain a print. The inputs to the enroll dialog 226 are fingerprints read from an external piece of hardware connected to an input port. The commands to the enroll dialog 226 include: Start Scanning; Alternative Finger, and Cancel. The Start Scanning command causes the process of collecting prints to be started. A diagram of the scan process is provided in FIGURE 4. The Alternative Finger command causes the alternative finger dialog 225 to be displayed. When it returns it indicates to the user what finger they should scan. Further, the Cancel command closes the dialog.

As shown in FIGURE 5, the OFAC match dialog displays data from the U.S. Department of the Treasury's OFAC list. The commands on this page include a Close and Override button. In an embodiment, the Close and Override button, along with an override message appear two seconds after the dialog is first displayed. This is to deliberately delay closing the dialog to force the teller to properly consider its disposition. In a further embodiment, if an OFAC match dialog is displayed from the main page OFAC button, then the override button and the override message are not displayed.

The Override command indicates to the calling enroll process that the teller wished to override the automatic OFAC check and continue with the enrollment anyway. It is desired that this process be avoidable since the OFAC check can produce false matches by the nature of the fact that more than one person can have the same name. Further, the Close command closed the OFAC match dialog box.

In an embodiment, the system includes a menu bar. The commands of the menu bar include: Go To Main; Go To Enroll Page; Go To Configuration Screen; Update; About; and, Exit. The Go To Main Page cause the display to revert to the main page 212 whenever this is possible within the application. That is to say, on every screen except preferably the identification screen 214 and the change credentials page 220 because, within these screens, it is desired that the teller indicate the disposition of the check.

The Go To Enroll command results in the user being brought to the enroll page 216 whenever this is possible with the application. That it to say, every screen except preferably the identification screen 214 and the change credentials page 220.

The Go to Configuration Screen command causes the user to go to the configuration screen 222. Preferably, this menu item is only available from the main page 212.

The Update command causes the software to check for a software update at the vendor's server or central server. Preferably, this function is only available from the main page 212.

The About command causes the application to display a box about the software which, preferably, includes the version number and support contact information. Further, the Exit command causes the software to exit. This command is preferably available everywhere except the identification screen 214 since the teller must indicate the disposition of the check.

A map of the back office screens, or pages, is provided in FIGURE 6. The back office screens include a main page 512 that allows the user to mark transactions and customers. The inputs to the main page 512 include Date and Last Name. The Date specifies the date and time range of the transaction the user wishes to view. Further, the last name specifies the last name of the person which the user wants to display.

The commands to the main page include: Find Transactions and Find Customers. The Find Transactions command causes the program to go to the Transaction List page or screen 514 that lists the transactions that occurred in the bank during the time range specified in the main page 512. The Find Customers command causes the program to go to the customer list page 516 that lists the customers with the corresponding last name who have done business at that bank.

As stated previously, the transaction list page 514 lists all the transactions that have been conducted by the bank during the specified time period. The page also allows the user to look at more details on each transaction. Preferably, as shown in FIGURE 7, the transactions are listed in the same format as shown on the identification page 214 (FIGURE 2) except that transactions are listed strictly in ascending order for time. Additionally, each transaction is preceded by three hyperlinks which are described in greater detail further herein.

The inputs to the transaction list page consist of the date and time range for the transactions to list. The commands to the transaction list page include: Refresh; Done; Note; Cust; and, View. The Refresh command causes the software to redisplay the page using the criteria specified in the inputs section. Further, the Done command returns the user to the main page 512.

The Note command is a hyperlink next to each transaction. Selecting the hyperlink brings up the mark transactions dialog 518. If OK is selected on the dialog, the transaction annotation selected in the dialog is set as the transaction annotation. This appears preferably in the transaction list at the end of the transaction line. In an embodiment, only check cashing transactions can be annotated. Enroll type transaction also show the hyperlink for consistency, however, clicking on such a hyperlink simply brings up a message box warning of this situation.

The Cust command is a hyperlink next to each transaction wherein selecting the hyperlink results in the user being brought to the repeat enroll page 520 with the enroll criteria entered for the customer who performed the selected transaction.

The View command is a hyperlink next to each transaction. Selecting the hyperlink results in the user being directed to a different screen depending on the type of transaction. If the transaction is a regular check cashing transaction, a copy of the identification screen 214 (FIGURE 2) that was shown to the teller before that transaction was cashed is shown. This is shown on the repeat identification page 522. This allows the back office staff to see what information the teller had before cashing the check.

If the transaction is an enrollment, then a copy of the original enrollment data as shown in the repeat enrollment page 520 is provided by the View command. If the transaction is a re-enrollment, then a message is displayed indicating such and the date supplied for re-enrollment is shown on the repeat enrollment page 520. If the transaction is a duplicate enrollment, then the duplicate enrollment information is shown in the repeat already enrollment page 524.

The repeat identification page or screen 526 provides a copy of the information a teller was shown before they disposed of a transaction. In a situation where a transaction proved to be fraudulent, this allows the bank management to dig into the transaction and see exactly what data the teller used to determine to cash the check.

The commands for the repeat identification page include Show Alerts wherein the command causes a repeat of the alerts shown when the page was first displayed. As such, any cancelable alerts will be shown as they were originally. However, any attempt to cancel the alert is met with an appropriate warning.

The repeat enroll page or screen 528 consists of an enroll screen for the selected user (i.e., customer). The data shown is the data that was entered at enroll. Any subsequence changes via the change credentials or modification of the notes on this person are not reflected on this screen. This is deliberate so that the exact data on the enroll can be seen. Likewise, the repeat already enrolled page provides a copy of the duplicate enrollment page as it was shown to the teller.

The customer list page 516 lists all the customers in the primary or central server data base that have done business with this bank whose last name matched the one specified in an input box. As shown in FIGURE 7, each customer is listed with the last name followed by the first name, followed by their current registered address in small type. Next to each transaction are three hyperlinks as described further herein.

The input to the customer list page consists of a last name field wherein the user can change the last name to search for. The commands to the customer list page include: Find; Done; Note; Enrl; and, Trans. The Find command refreshes the list by requerying the command at the database. Any changes made by other back office software users, or any additional matching names, or any changes in credentials are reflected by selecting the Find command.

The Done command results in the user being brought back to the back office main page 512. The Note command includes a hyperlink next to each customer that pulls up the edit customer notes dialog 530 on that customer. The Enrl command results in a display of the repeat enroll page 520 for the selected customer. The Trans command results in a transaction list for each customer being provided as if a non-check cashing identification had been applied, and thus shows the information in the repeat identification page 522 as previously described above.

As indicated previously, the mark transaction dialog 518 allows the user to add back office annotations to a transaction. This can be used when a batch of bad checks come into the bank back office. The bank can then indicate the problems associated with the checks, so that the information is available in subsequent identifications.

The input to the mark transaction dialog 518, as shown in FIGURE 8, includes a combo box to select the transaction annotation. The commands to the mark transaction dialog box include OK and Cancel. The OK command marks the transaction with the given annotation (i.e., annotation entered by the user). Preferably, this annotation subsequently appears in any identification screen showing this check. The priority and severity of the display, as well as the allowable annotation are described in greater detail further herein. Moreover, the Cancel command results in the dialog being canceled and does not annotate the transaction.

As shown in FIGURE 9, the edit customer notes dialog 530 allows the back office staff to add notes for association with a particular customer. The dialog includes a list with a one line summary for each note. The commands for this dialog include Add, Edit, Delete, Move Up and Move Down, OK, and Cancel.

The Add command results in a message or note being added and thus opens the edit one customer note dialog 532 to allow the user to edit it. The Edit command results in the edit one customer note dialog being opened for the selected note or message. The Delete command results in the selected note or message being deleted after a confirm message is displayed. The Move Up and Move Down commands consist of arrow buttons or icons that move the selected message or note up or down in the order of display. Moving the note or message effects both the order that the note or message is shown in the identification page 214 (i.e., the portion below the name and address), and also the order that any pop up boxes are shown to the user (i.e., teller) in the identification page. The OK command closes the dialog and saves the changes to the messages or notes that were entered. Further, the Cancel command closes the dialog and cancels any changes that might have been made.

In an embodiment, the command buttons or icons are enabled and disabled according to a scheme. In particular, the Add, OK, and Cancel commands are always enabled. Further, the Edit command is enabled whenever a message or note is selected in the list. Further, the Move Up and Move Down commands are enabled when an item is selected in the list, except that the up arrow is not enabled when the first item is selected, and the down arrow is not enabled when the last item is selected.

Turning to the edit one customer note dialog 532, this allows the user to edit one customer message or, in the case of an Add command, add the text of a new message. The inputs to this dialog allow for a user to edit a message or note in a conventional matter. A combo box is provided that allows the user to choose the type of message such as: Normal permanent message; Pop up permanent message; and Pop up till teller clears. The Normal permanent message causes the system to provide the message in the notes area on the identification page 214. The Pop up permanent message will cause the message to appear in the notes area and also pop-up as a dialog box, with an OK button, when the identification page is displayed. The Pop up till teller clears allows the message to appear in the notes area and also as a pop up as with the pop up permanent message. However, in this case the dialog has both an OK and a Cancel button wherein if the user selected the cancel after a confirmation, the teller can delete this pop up message from the identification screen.

The back office menu bar provides Commands that include: Go To Configuration Screen; Update; About; and Exit. The Go To Configuration Screen command causes the system to take the user to the configuration screen 222. Preferably, this menu item is only available from the main page 512. The Update command causes the software to check for a software update at a central server. The About command results in the system displaying a box about the software that includes the version number and support contact information. Further, the Exit command causes the software to exit.

In an embodiment, a bank is allowed to specify a standard message file. This allows the bank's back office staff and tellers to enter consistent messages for customers. The format of a standard message file is a regular text file, with each message on a separate line. Additionally, in an embodiment, the first character of each line is a special code letter as follows:

1. An "A" indicates that the message is a regular message that appears until the back office staff removes it.
2. A "P" indicates that the message should pop up to the teller to five them high priority information about this individual.
3. A "C" indicates that the message should pop up to the teller to give them high priority information about the individual. However, when the teller clicks cancel, the message is permanently removed from the person's record. This allows the back office staff to put in temporary messages for individual customers.

As indicated previously, fingerprints are matched according to certain rules. Preferably, in an embodiment, these rules are different for identification and enrollment. During identification, a fingerprint is compared against only those fingerprints matching individuals with a similar last name to that given on the main page 212. This heuristic enables a faster identification. In an embodiment, the system compensates for common phonetically based misspelling of last names, such as, for example, D'Arcy rather than Darcy, or Allison rather than Alison, and Smythe instead of Smith. This is accomplished by using a list of related name spellings or fuzzy logic. However, should someone use a false name, then a successfully match will not occur during identification. This is not a risk to security since the person will not be allowed to access the system until they enroll.

In an embodiment, during enrollment, the fingerprint is checked against every fingerprint in the database to search for a match. This methodology prevents someone from re-enrolling under a false name.

It is noted that in rare cases two fingerprints are too similar to distinguish between them. In such cases the secondary identifier comprising the thumbprint is used to distinguish between candidates with matching fingerprints. As such, the system instructs the teller to collect the additional fingerprint.

In an embodiment, checks can have two disposition markers, one disposition given by the teller at the time of the transaction, and the second given in the bank's back office should the check be returned for insufficient funds or other reasons. Preferably, dispositions are rated as to the level of seriousness between 0 (i.e., benign) to 9 (i.e., very serious). A preferred embodiment of the classes of disposition are provided below for tellers and the back office:

Teller Dispositions	Disposition Rating
Abandoned	1
Account Overdrawn	1
Altered Check	4
Appears Counterfeit	4
Check Larger Than Allowed	1
Closed Account	1
Deceptive Customer	4
Does Not Make Sense	1
Forgery Suspected	4
Maker Has Hold On Account	1
Non-Endorsable Item	1
Notes Indicate Problem	4
Not Sufficient Funds In Account	1
Other	1
Scam Suspected	4
Stale Dated Check	1
Stolen Check	4

Transaction History Bad	4
Unable To Reach Maker	1
Unable To Verify Funds	1

Back Office Dispositions	Disposition Rating
Refer To Maker	6
Not Sufficient Funds	1
Uncollected Funds	6
Account Closed	2
Stop Payment	6
Bad Endorsement	9
Other	1

With the above dispositions, the following is a preferred manner of displaying each disposition level in the identification screen 214:

Disposition Rating	Manner of Displaying
0	No Highlighting
1-3	Highlight Text In Blue
4-6	Highlight Text In Red And Bold
7-9	Highlight In Red And Bold, And In Popup Dialog To Teller

While the specific embodiments have been illustrated and described, numerous modifications come to mind without significantly departing from the spirit of the invention and the scope of protection is only limited by the scope of the accompanying Claims.

CLAIMS

I CLAIM:

1. A method for verifying an individual's identity, the method comprising the steps of:
   a. receiving at least one biometric identifier from an individual;
   b. comparing the at least one biometric identifier to biometric identifiers contained in a database;
   c. associating the at least one biometric identifier from the individual with an individual identity contained in a central database; and,
   d. outputting information associated with the individual from the central database.
2. The method of claim 1 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.
3. The method of claim 1 further comprising the steps of:
   i. identifying the zip code of the location wherein the at least one biometric identifier from an individual was received; and,
   ii. creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.
4. The method of claim 1 further comprising the steps of:
   i. identifying a tag for the individual; and,
   ii. creating a smaller database of biometric identifiers previously received from individuals that have the same tag to compare to the at least one biometric identifier from an individual.
5. The method of claim 4 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.
6. A method for verifying a customer's identity, the method comprising the steps of:
   a. receiving at least one biometric identifier from an individual;

b. comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. associating the at least one biometric identifier from the individual with a customer identity contained in a local database;

d. transmitting the customer identity to a central database; and,

e. outputting information associated with the individual from the central database.

7. The method of claim 6 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

8. The method of claim 6 further comprising the steps of:

i. identifying the zip code of the location wherein the at least one biometric identifier from an individual was received; and,

ii. creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

9. The method of claim 6 further comprising the steps of:

i. identifying a tag for the individual; and,

ii. creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

10. The method of claim 9 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

11. The method of claim 6 further comprising the step of updating the local database new data from the central database.

12. A method for verifying a customer's identity, the method comprising the steps of:

a. transmitting at least one biometric identifier from a remote location to a central server;

b. comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. associating the at least one biometric identifier from the remote location with a customer identity contained in a central database; and,

d. outputting information associated with the individual from the central database.

13. The method of claim 12 wherein the at least one data field is a data field shared by the remote location.

14. The method of claim 12 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

15. The method of claim 12 further comprising the steps of:

i. identifying the zip code of the location wherein the at least one biometric identifier from an individual was received; and,

ii. creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

16. The method of claim 12 further comprising the steps of:

i. identifying a tag for the individual; and,

ii. creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

17. The method of claim 16 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

18. A system for verifying a customer's identity, the system comprising:

a. a first component for receiving at least one biometric identifier from an individual;

b. a second component for comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. a third component for associating the at least one biometric identifier from the individual with a customer identity contained in a central database; and,

d. a fourth component for outputting information associated with the individual from the central database.

19. The system of claim 18 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

20. The system of claim 18 further comprising a fifth component for identifying the zip code of the location wherein the at least one biometric identifier from an individual was received and a sixth component for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

21. The system of claim 18 further comprising a fifth component for identifying a tag for the individual and a sixth component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

22. The system of claim 21 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

23. A system for verifying a customer's identity, the system comprising:

a. a first component for receiving at least one biometric identifier from an individual;

b. a second component for comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. a third component for associating the at least one biometric identifier from the individual with a customer identity contained in a local database;

d. a fourth component for transmitting the customer identity to a central database; and,

e. a fifth component for outputting information associated with the individual from the central database.

24. The system of claim 23 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

25. The system of claim 23 further comprising a sixth component for identifying the zip code of the location wherein the at least one biometric identifier from an individual was received and a seventh component for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

26. The system of claim 23 further comprising a sixth component for identifying a tag for the individual and a seventh component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

27. The system of claim 26 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

28. The system of claim 23 further comprising a sixth component for updating the local database new data from the central database.

29. A system for verifying a customer's identity, the system comprising:

a. a first component for transmitting at least one biometric identifier from a remote client to a central server;

b. a second component for comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. a third component for associating the at least one biometric identifier from the remote client with a customer identity contained in a central database; and,

d. a fourth component for outputting information associated with the individual from the central database.

30. The system of claim 29 wherein the at least one data field is a data field shared by the remote client.

31. The system of claim 29 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

32. The system of claim 29 further comprising a fifth component for identifying the zip code of the location wherein the at least one biometric identifier from an individual was received and a sixth component for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

33. The system of claim 29 further comprising a fifth component for identifying a tag for the individual and a sixth component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

34. The system of claim 33 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

35. A computer program product for verifying a customer's identity, the computer program product comprising:

    a. a first code segment for receiving at least one biometric identifier from an individual;

    b. a second code segment for comparing the at least one biometric identifier to biometric identifiers contained in a database;

    c. a third code segment for associating the at least one biometric identifier from the individual with a customer identity contained in a central database; and,

    d. a fourth code segment for outputting information associated with the individual from the central database.

36. The computer program product of claim 35 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal

images, and voice prints.

37. The computer program product of claim 35 further comprising fifth code segment for identifying the zip code of the location wherein the at least one biometric identifier from an individual was received and a sixth code segment for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

38. The computer program product of claim 35 further comprising a fifth code segment for identifying a tag for the individual and a sixth component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

39. The computer program product claim 38 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

40. A computer program product for verifying a customer's identity, the computer program product comprising:

a. a first code segment for receiving at least one biometric identifier from an individual;

b. a second code segment for comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. a third code segment for associating the at least one biometric identifier from the individual with a customer identity contained in a local database;

d. a fourth code segment for transmitting the customer identity to a central database; and,

e. a fifth code segment for outputting information associated with the individual from the central database.

41. The computer program product of claim 40 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

42. The computer program product of claim 40 further comprising sixth code segment for identifying the zip code of the location wherein the at least one biometric identifier from

an individual was received and a seventh code segment for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

43. The computer program of claim 40 further comprising a sixth code segment for identifying a tag for the individual and a seventh component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

44. The computer program product of claim 43 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

45. The computer program product of claim 40 further comprising a sixth code segment for updating the local database new data from the central database.

46. A computer program product for verifying a customer's identity, the computer program product comprising:

a. a first code segment for transmitting at least one biometric identifier from a remote location to a central server;

b. a second code segment for comparing the at least one biometric identifier to biometric identifiers contained in a database;

c. a third code segment for associating the at least one biometric identifier from the remote location with a customer identity contained in a central database; and,

d. a fourth code segment for outputting information associated with the individual from the central database.

47. The computer program product of claim 46 wherein the at least one data field is a data field shared by the remote location.

48. The computer program product of claim 46 wherein the at least one biometric identifier is selected from the group comprising fingerprints, palm prints, facial images, retinal images, and voice prints.

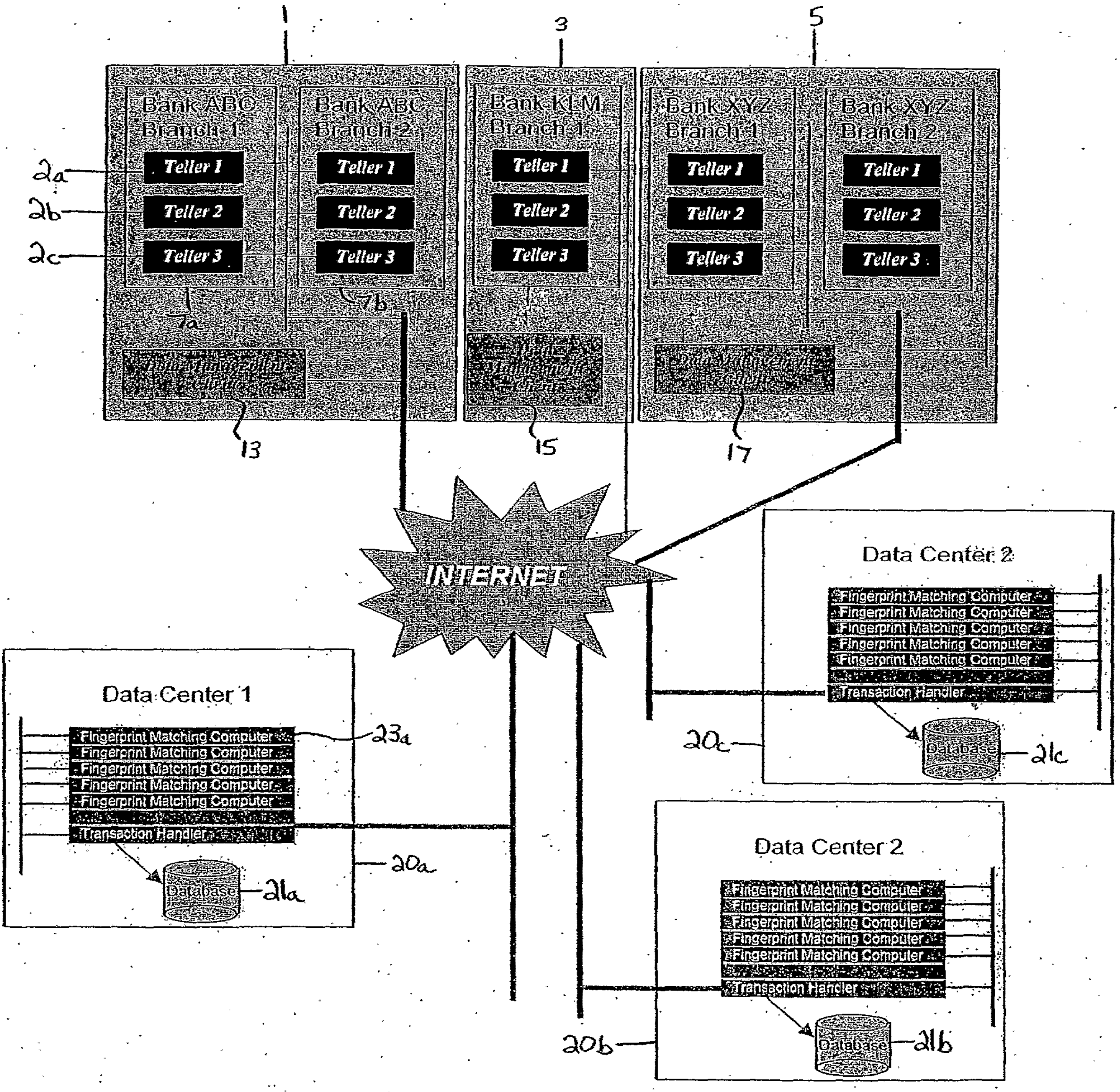
49. The computer program product of claim 46 further comprising fifth code segment for identifying the zip code of the location wherein the at least one biometric identifier from

an individual was received and a sixth code segment for creating a smaller database of biometric identifiers previously received from surrounding zip codes to compare to the at least one biometric identifier from an individual.

50. The computer program of claim 46 further comprising a fifth code segment for identifying a tag for the individual and a sixth component for creating a smaller database of biometric identifiers previously received from identifiable individuals that have the same tag to compare to the at least one biometric identifier from an individual.

51. The computer program product of claim 50 wherein the tag is selected from the group comprising birth dates, phone numbers, last names, and Metaphone encoded last names.

Figure 1


1
3
5
Bank ABC Branch 1
Bank ABC Branch 2
Bank KLM Branch 1
Bank XYZ Branch 1
Bank XYZ Branch 2
Teller 1
Teller 2
Teller 3
2a
2b
2c
7a
7b
13
15
17
INTERNET
Data Center 1
Data Center 2
Data Center 2
Fingerprint Matching Computer
Transaction Handler
Database
23a
20a
21a
20b
21b
20c
21c

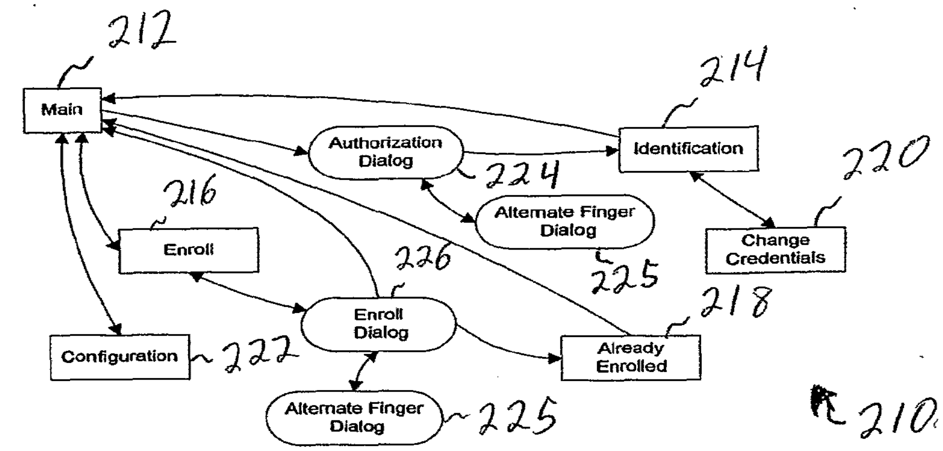
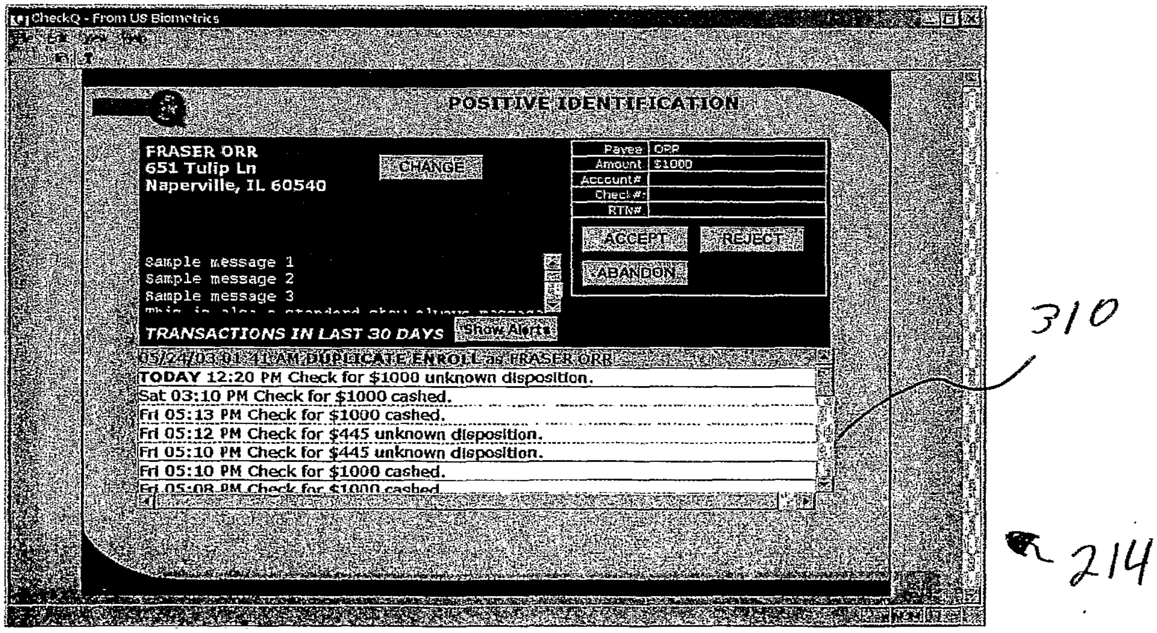


FIGURE 2



FRASER ORR
651 Tulip Ln
Naperville, IL 60540

Payee	ORR
Amount	$1000
Account#	
Check#:	
RTN#	

Sample message 1
Sample message 2
Sample message 3
This is also a standard okay always message

TRANSACTIONS IN LAST 30 DAYS

05/24/03 01:41 AM DUPLICATE ENROLL as FRASER ORR
TODAY 12:20 PM Check for $1000 unknown disposition.
Sat 03:10 PM Check for $1000 cashed.
Fri 05:13 PM Check for $1000 cashed.
Fri 05:12 PM Check for $445 unknown disposition.
Fri 05:10 PM Check for $445 unknown disposition.
Fri 05:10 PM Check for $1000 cashed.
Fri 05:08 PM Check for $1000 cashed.

FIGURE 3

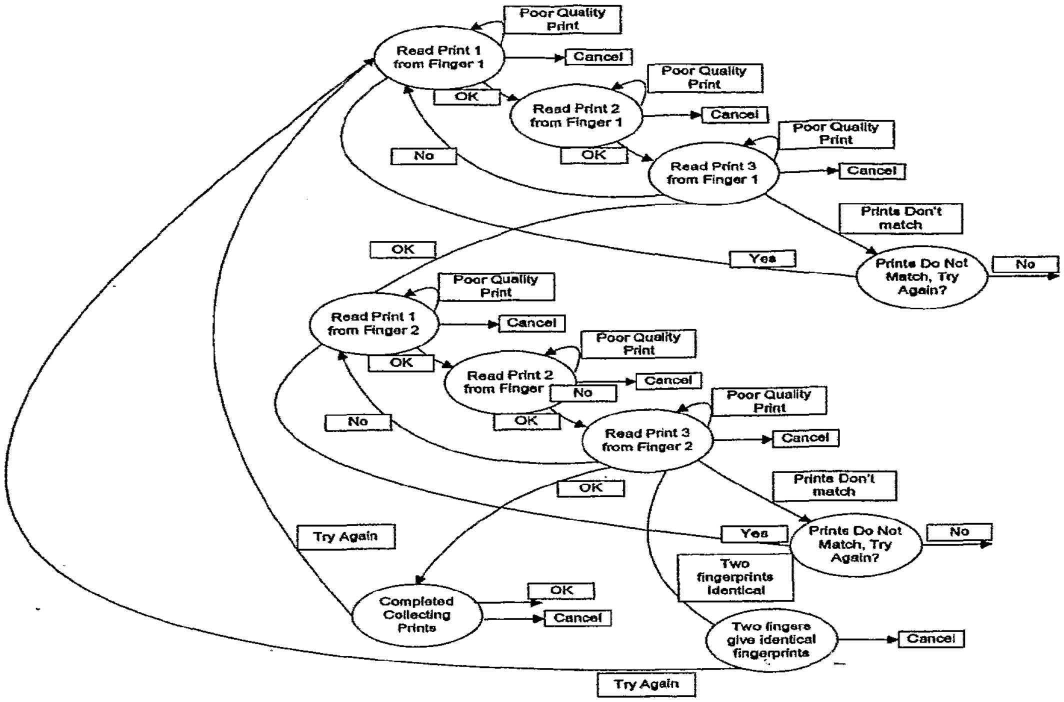
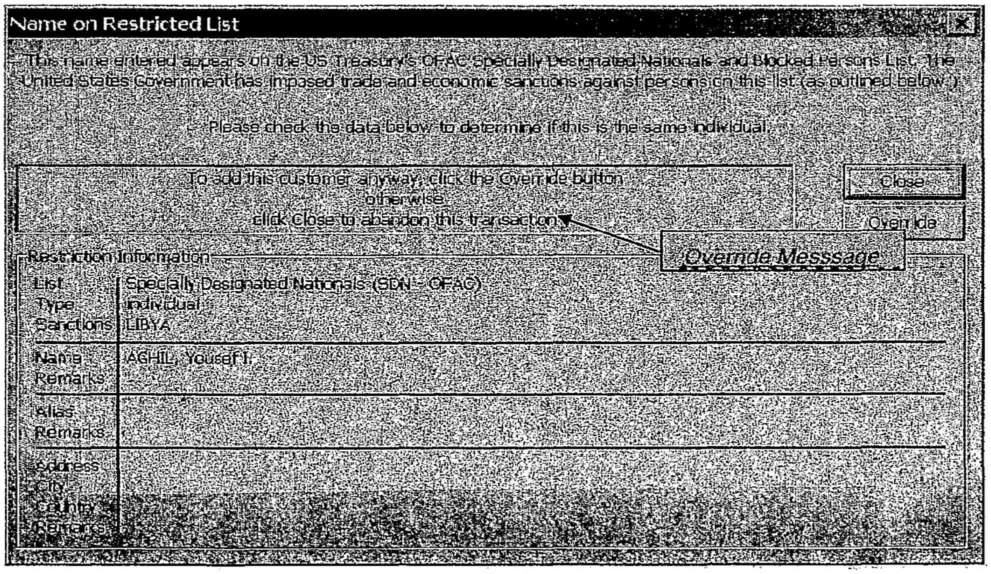

Poor Quality Print
Read Print 1 from Finger 1
Cancel
OK
Poor Quality Print
Read Print 2 from Finger 1
Cancel
No
OK
Poor Quality Print
Read Print 3 from Finger 1
Cancel
Prints Don't match
OK
Yes
Prints Do Not Match, Try Again?
No
Poor Quality Print
Read Print 1 from Finger 2
Cancel
OK
Poor Quality Print
Read Print 2 from Finger
Cancel
No
No
OK
Poor Quality Print
Read Print 3 from Finger 2
Cancel
Prints Don't match
OK
Try Again
Yes
Prints Do Not Match, Try Again?
No
Two fingerprints identical
Completed Collecting Prints
OK
Cancel
Two fingers give identical fingerprints
Cancel
Try Again

FIGURE 4



This name entered appears on the US Treasury's OFAC Specially Designated Nationals and Blocked Persons List. The United States Government has imposed trade and economic sanctions against persons on this list (as outlined below.)

Please check the data below to determine if this is the same individual.

To add this customer anyway, click the Override button
otherwise
click Close to abandon this transaction.

Restriction Information

List	Specially Designated Nationals (SDN - OFAC)
Type	individual
Sanctions	LIBYA
Name	AGHIL, Yousef I.
Remarks	
Alias	
Remarks	
Address	
City	
Country	
Remarks	

FIGURE 5

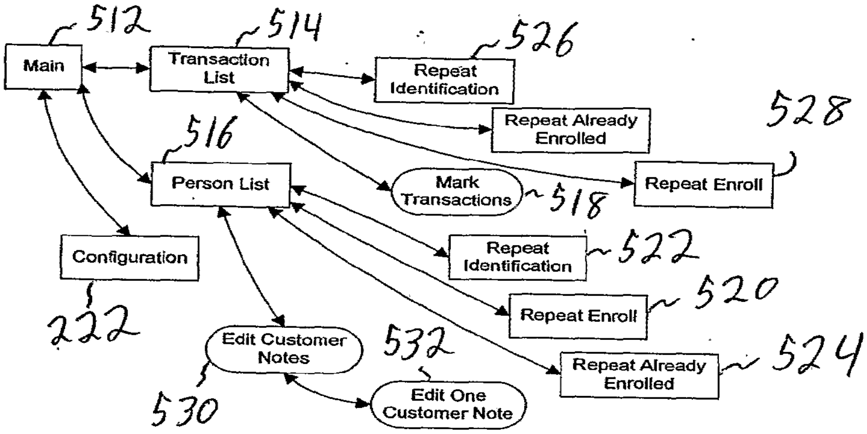
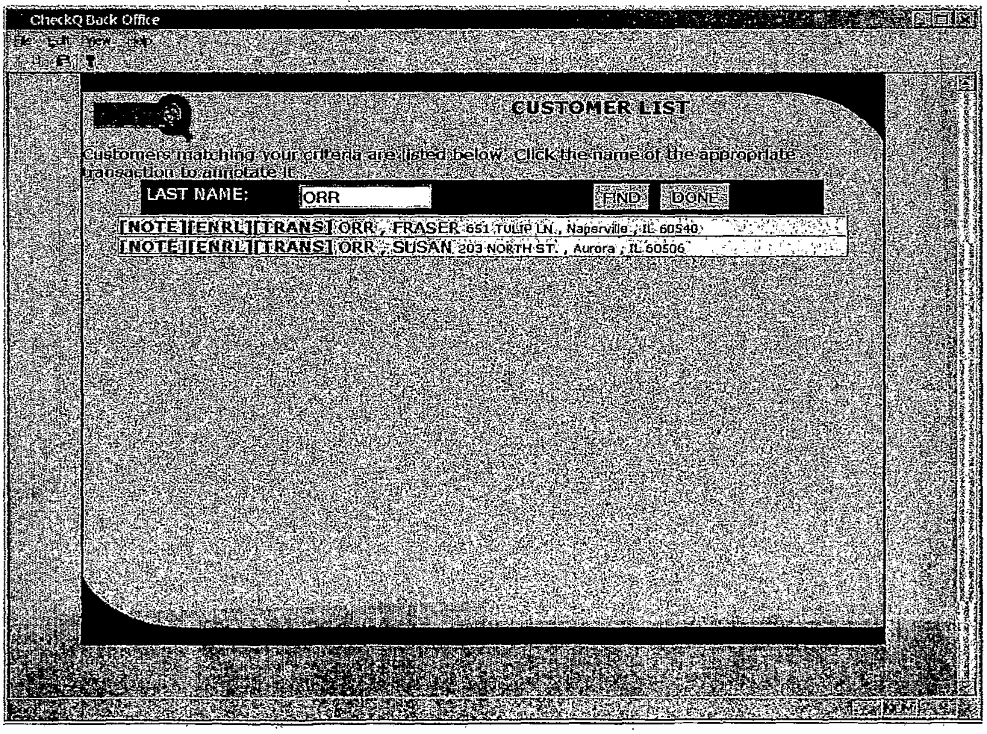


FIGURE 6



CUSTOMER LIST

Customers matching your criteria are listed below. Click the name of the appropriate transaction to annotate it.

LAST NAME: ORR FIND DONE

[NOTE][ENRL][TRANS] ORR , FRASER 651 TULIP LN., Naperville , IL 60540

[NOTE][ENRL][TRANS] ORR , SUSAN 203 NORTH ST. , Aurora , IL 60506

FIGURE 7

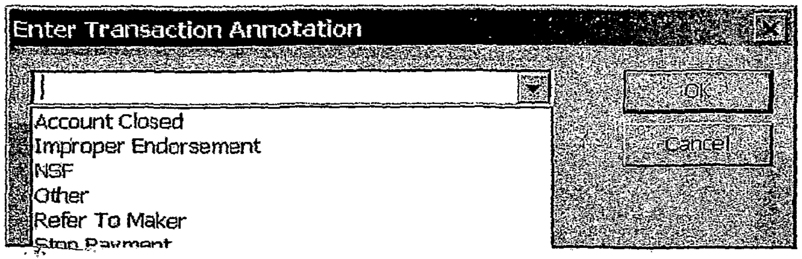
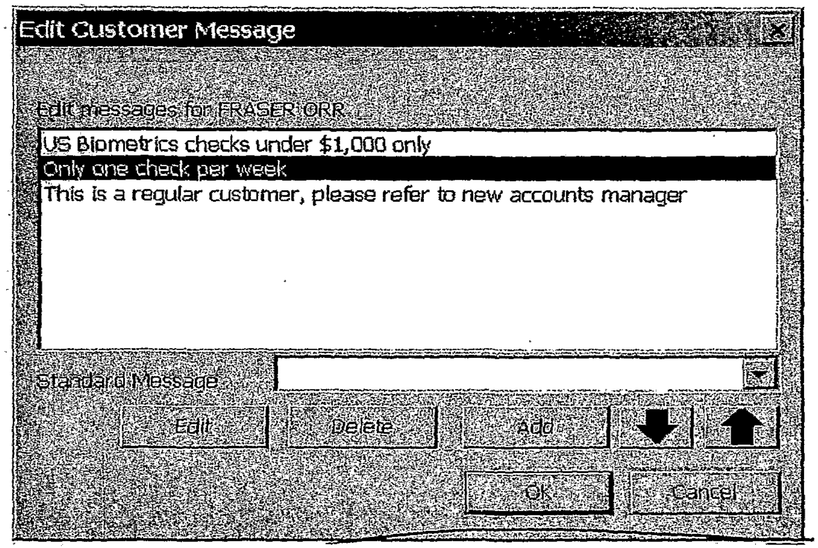


FIGURE 8



Edit messages for FRASER ORR

US Biometrics checks under $1,000 only
Only one check per week
This is a regular customer, please refer to new accounts manager

FIGURE 9

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/013788

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K9/00 G06F21/00 G07C9/00

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)
IPC 7 G06K G06F G07C

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 practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/025718 A (MAGGS MICHAEL NORMAN ; DATA TREASURY CORPORTION (US)) 27 March 2003 (2003-03-27)	1-10,12, 14-27, 29, 31-44, 46,48-51
Y	abstract; figures 1-3,8,9 page 4 - page 6 page 17, paragraph 6 - page 20, paragraph 1 ----- -/--	11,13, 28,30, 45,47

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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 document 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

31 August 2004

Date of mailing of the international search report

04/10/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,
Fax: (+31–70) 340–3016

Authorized officer

Müller, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/013788

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DRISCOLL E C ET AL: "A comparison of centralized versus distributed architectures in biometric access control systems" PROC. INT. CONF. ON COMPOSITE SCIENCE AND TECHNOLOGY, ICCST 89, 3 October 1989 (1989-10-03), pages 193-198, XP010324640 ZURICH, SWITZERLAND the whole document -----	11,13, 28,30, 45,47
A	US 6 070 159 A (MOMCHEV ORLIN ET AL) 30 May 2000 (2000-05-30) abstract; figures 1,2 column 2, line 51 - column 4, line 21 -----	1-51
P,A	US 2003/093690 A1 (KEMPER STEFAN) 15 May 2003 (2003-05-15) abstract; figures 1,2 -----	11,13, 28,30, 45,47

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/013788

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 03025718	A	27-03-2003	WO	03025718 A2	27-03-2003
			US	2003225693 A1	04-12-2003
US 6070159	A	30-05-2000	NONE		
US 2003093690	A1	15-05-2003	NONE		

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on August 13, 2013.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: 12/063,650

371 Filing Date: August 12, 2010

For: CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Johns, Andrew W.

Group Art Unit: 2665

Confirmation No.: 9949

Mail Stop RCE
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL

Attached are:

☒ Transmittal Letter; First Supplemental Information Disclosure Statement; PTO Form 1449; copies of cited references B3-B4; Request for Continued Examination (RCE).

Fee calculation:

☐ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicant is small entity ☐ Applicant is micro entity.

☐ An extension fee in an amount of $____ for a ___-month extension of time under 37 C.F.R. § 1.136(a).

☒ A petition or processing fee in an amount of $600.00 under 37 CFR § 1.17(e)(1).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

☒ Please charge Deposit Account No. 23-1925 in the amount of $600.00 for the RCE filing fee.

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

August 13, 2013
Date

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on August 13, 2013.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

BRINKS
HOFER
GILSON
&LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	BURKE, Christopher John	
Appln. No.:	12/063,650	Examiner: Johns, Andrew W.
371 Filing Date:	August 12, 2010	Group Art Unit: 2665
For:	CARD DEVICE SECURITY USING BIOMETRICS	Confirmation No.: 9949
Attorney Docket No:	12838/5 (729727US)	

Mail Stop RCE
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CONTINUED EXAMINATION (37 CFR § 1.114)

Dear Sir/Madam:

Applicant requests continued examination of the above-identified application under 37 CFR §1.114.

☒ This is the first request under 37 CFR_§1.17(e) in this application.

☒ Submission under 37 CFR 1.114 (*check at least one of the following*):

- □ Previously submitted:
  - □ Applicant(s) requests nonentry of any previously-filed unentered amendments.
  - □ Please enter and consider the Amendment After Final Under 37 CFR §1.116 previously filed on _____.
  - □ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____.
  - □ Other: _____.
- ☒ Attached is:
  - ☒ A First Supplemental Information Disclosure Statement; PTO Form 1449; and copies of cited references B3-B4
  - □ An Amendment to the written description, claims, or drawings
  - □ New Arguments and/or New Evidence in support of Patentability
  - □ Other: _____

☐ Request for suspension of action:

Applicant(s) hereby requests suspension of action on the above-identified application under 37 CFR §1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; requires Processing Fee under 37 CFR §1.17(i)).

☒ Small/Micro Entity Status:

- ☒ Applicant hereby asserts entitlement to claim ☒ small or ☐ micro entity status under 37 CFR §§ 1.9 and 1.27.
- ☐ A small/micro entity statement or assertion of entitlement to claim small/micro entity status was filed in prior application no. _____/_____ and such status is still proper and desired.
- ☐ Is no longer desired.

☒ Applicant calculates the following fees to be due in connection with this Request:

- ☒ A request fee of $600.00 under 37 CFR §1.17(e)(1) or (2).
- ☐ A suspension processing fee of $_____ under 37 CFR §1.17(i).
- ☐ An additional filing fee of $_____ under 37 CFR §1.16 (_____ additional independent claims and/or _____ additional total claims).
- ☐ An extension fee of $_____ under 37 CFR §1.17(a) for a _______-month extension of time.

☒ Fee payment to cover the above-enumerated fee(s):

- ☒ Please charge Deposit Account No. 23-1925 (BRINKS HOFER GILSON & LIONE) in the amount of $600.00.
- ☐ A payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
- ☒ The Commissioner is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925 (BRINKS HOFER GILSON & LIONE).

Respectfully submitted,

August 13, 2013
Date

/Robert D. Summers, Jr./
Robert D. Summers (Reg. No. 57,844)

Electronic Patent Application Fee Transmittal

Application Number:	12063650
Filing Date:	12-Aug-2010
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Robert Dalton Summers/Lori Peterson
Attorney Docket Number:	12838/5

Filed as Small Entity

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt

EFS ID:	16570832
Application Number:	12063650
International Application Number:	
Confirmation Number:	9949
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers/Maggie Pieczonka
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/5
Receipt Date:	13-AUG-2013
Filing Date:	12-AUG-2010
Time Stamp:	12:23:17
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$600
RAM confirmation Number	10868
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	128385IDS1.pdf	56064 3508ac0333699adfa4b695406e10affa1fdffb49	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	12838514491.pdf	30165 e4e695ca7402e9ea6ed6afdd19acc709cb7b6c33	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	128385B3.pdf	3683359 5e7e2c321f0ee3e1409ca3a0467b7c4a6fb2a113	no	53
Warnings:					
Information:					
4	Non Patent Literature	128385B4.pdf	476966 4a372a5f296ed087bcb8d0bfaf5d8433bf92d934	no	8
Warnings:					
Information:					
5	Miscellaneous Incoming Letter	128385tl.pdf	44239 3228f61f0767283f9e6be9452c05b435f5d63fbc	no	1
Warnings:					
Information:					
6	Request for Continued Examination (RCE)	128385RCE.pdf	74523 5965fd90f1a94f7a51ecec88f137640055 1cc02f	no	2
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	30580 01eba2f38eabc78e6e6a8ed3496296df34619a2b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4395896		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Certificate Under 37 CFR 1.8

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office, Commissioner for Patents, via the EFS on August 13, 2013.

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of:	BURKE, Christopher John	
Appln. No.:	12/063,650	Examiner: Johns, Andrew W.
371 Filing Date:	August 12, 2010	Group Art Unit: 2665
For:	CARD DEVICE SECURITY USING BIOMETRICS	Confirmation No.: 9949
Attorney Docket No: 12838/5 (729727US)		

FIRST SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and §§1.97-1.98, and more particularly in accordance with 37 C.F.R. §1.97(b), Applicant hereby cites the following references:

U.S. PATENT DOCUMENTS

Document No.	Date	Patentee
2004/0041690 A1	03/04/2004	Yamagishi
6,665,601 B1	12/16/2003	Nielsen

FOREIGN PATENT DOCUMENT		
DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY
WO 2004/100053 A1	11/18/2004	WIPO

OTHER ART

Supplementary European Search Report dated August 29, 2011 for EPO Application No. EP 06760981.8.

Applicant is enclosing Form PTO-1449 (one sheet), along with copies of cited references B3-B4, which are required under 37 C.F.R. §1.98(a)(2). As the listed references are in English, no further commentary is believed to be necessary, 37 C.F.R §1.98(a)(3). Applicant respectfully requests the Examiner's consideration of the above references and entry thereof into the record of this application.

By submitting this Statement, Applicant is attempting to fully comply with the duty of candor and good faith mandated by 37 C.F.R. §1.56. As such, this Statement is not intended to constitute an admission that the enclosed references, or other information referred to therein, constitute “prior art” or is otherwise "material to patentability," as that phrase is defined in 37 C.F.R. §1.56(a).

Applicant has calculated no fee to be due upon filing this Statement. However, the Director is authorized to charge any fee deficiency associated with the filing of this Statement to a deposit account, as authorized in the accompanying Transmittal.

Respectfully submitted,

Dated: August 13, 2013

/Robert D. Summers, Jr./
Robert D. Summers, Jr.
Reg. No. 57,844

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

757 7590 08/29/2013

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
JOHNS, ANDREW W	
ART UNIT	**PAPER NUMBER**
2665	

DATE MAILED: 08/29/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

TITLE OF INVENTION: CARD DEVICE SECURITY USING BIOMETRICS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	11/29/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

757 7590 08/29/2013

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

TITLE OF INVENTION: CARD DEVICE SECURITY USING BIOMETRICS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	11/29/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
JOHNS, ANDREW W	2665	382-119000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________________
2____________________________
3____________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ____________________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ____________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
□ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
□ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

757 7590 08/29/2013

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

EXAMINER	
JOHNS, ANDREW W	
ART UNIT	**PAPER NUMBER**
2665	

DATE MAILED: 08/29/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 503 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 503 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 12/063,650	Applicant(s) BURKE	
	Examiner Andrew W. Johns	Art Unit 2665	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the RCE and IDS filed 13 August 2013*.

   □ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.

2. □ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1-20*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☒ All b) □ Some *c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 8/13/13
3. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. □ Examiner's Amendment/Comment
6. □ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/Andrew W Johns/
Primary Examiner, Art Unit 2665

Index of Claims	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

✓	**Rejected**	-	**Cancelled**	N	**Non-Elected**	A	**Appeal**
=	**Allowed**	÷	**Restricted**	I	**Interference**	O	**Objected**

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

CLAIM		DATE								
Final	Original	02/21/2013	05/31/2013	08/22/2013						
1	1	=	=	=						
2	2	=	=	=						
3	3	=	=	=						
4	4	=	=	=						
5	5	=	=	=						
6	6	=	=	=						
7	7	=	=	=						
10	8	=	=	=						
9	9	=	=	=						
12	10	=	=	=						
13	11	=	=	=						
14	12	=	=	=						
15	13	=	=	=						
16	14	=	=	=						
17	15	=	=	=						
18	16	✓	=	=						
19	17	✓	=	=						
20	18	✓	=	=						
8	19	=	=	=						
11	20	=	=	=						

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	239	(biometric near4 enroll$5).clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L2	14259	(memory near4 location).clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L3	123	L2 near8 card.clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L4	1	L1 same L3	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L5	304	L2 near6 (open or available or unoccupied).clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L6	1	L1 same L5	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L7	1	L1 and L5	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L8	673	(verification near4 (station or terminal)).clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L9	559	(card near6 previous$4).clm.	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39
L10	2	L8 same L9	US-PGPUB; UPAD	OR	ON	2013/08/22 13:39

8/22/2013 1:40:00 PM
C:\Users\ajohns\Documents\EAST\Workspaces\Applications\12\000\12063650.wsp

Search Notes	Application/Control No. 12063650	Applicant(s)/Patent Under Reexamination BURKE
	Examiner ANDREW W JOHNS	Art Unit 2665

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
382	115, 119, 155, 159	2/21/2013	/AWJ/
356	71	2/21/2013	/AWJ/
340	5.2, 5.52, 5.53, 5.8, 5.81, 5.82, 5.83	2/21/2013	/AWJ/
235	380, 382	2/21/2013	/AWJ/
Above updated		5/31/2013	/AWJ/
above updated		8/22/2013	/AWJ/

SEARCH NOTES

Search Notes	Date	Examiner

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Interference text search in PGPUB and UPAD files in EAST	(search history attached)	5/31/2013	/AWJ/

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
Updated intereference text search in PGPUB and UPAD files in EAST	(search history attached)	8/22/2013	/AWJ/

FIRST SUPPLEMENTAL FORM PTO-1449	SERIAL NO. **12/063,650**	CASE NO. **12838/5**
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT	FILING DATE **August 12, 2010**	GROUP ART UNIT **2665**
	APPLICANT: **BURKE, Christopher John**	

REFERENCE DESIGNATION U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
/AWJ/	B1	2004/0041690 A1	03/04/2004	Yamagishi	340/5.52	
/AWJ/	B2	6,665,601 B1	12/16/2003	Nielsen	701/50	

FOREIGN PATENT DOCUMENT

EXAMINER INITIAL		DOCUMENT NUMBER Number-Kind Code (if known)	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES OR NO
/AWJ/	B3	WO 2004/100053 A1	11/18/2004	WIPO	G06K 9/00	n/a

EXAMINER INITIAL	OTHER ART – NON PATENT LITERATURE DOCUMENT (Include name of author, title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date page(s), volume-issue number(s), publisher, city and/or country where published.	
/AWJ/	B4	Supplementary European Search Report dated August 29, 2011 for EPO Application No. EP 06760981.8.

EXAMINER /Andrew W. Johns/	DATE CONSIDERED 08/22/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12063650	BURKE
	Examiner	**Art Unit**
	ANDREW W JOHNS	2665

CPC						
Symbol					**Type**	**Version**
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	08/22/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

U.S. Patent and Trademark Office

Part of Paper No. 20130822

Issue Classification	**Application/Control No.**	**Applicant(s)/Patent Under Reexamination**
	12063650	BURKE
	Examiner	**Art Unit**
	ANDREW W JOHNS	2665

US ORIGINAL CLASSIFICATION

CLASS	SUBCLASS
382	119

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
340	5.82				

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
G	0	6	K	9 / 00 (2006.0)					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	08/22/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

Issue Classification

Issue Classification	**Application/Control No.** 12063650	**Applicant(s)/Patent Under Reexamination** BURKE
	Examiner ANDREW W JOHNS	**Art Unit** 2665

□ **Claims renumbered in the same order as presented by applicant** □ **CPA** □ **T.D.** □ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	19	17												
2	2	20	18												
3	3	8	19												
4	4	11	20												
5	5														
6	6														
7	7														
10	8														
9	9														
12	10														
13	11														
14	12														
15	13														
16	14														
17	15														
18	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/ANDREW W JOHNS/ Primary Examiner.Art Unit 2665 (Primary Examiner)	08/22/2013 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

757 7590 06/10/2013

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, IL 60610

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee Transmittal is being transmitted to the United States Patent and Trademark Office via EFS Transmission under 37 CFR 1.8, on the date indicated below:

Robert D. Summers, Jr.	(Depositor's name)
/Robert D. Summers, Jr./	(Signature)
November 26, 2013	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	08/12/2010	Christopher John Burke	12838/5	9949

TITLE OF INVENTION: CARD DEVICE SECURITY USING BIOMETRICS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$890	$300	$0	$1190	09/10/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
JOHNS, ANDREW W	2665	382-119000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Brinks Gilson
2 & Lione
3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Securicom (NSW) Pty Ltd	New South Wales, Australia

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual ☒ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ______

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 23-1925 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
□ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
□ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Robert D. Summers, Jr./ Date November 26, 2013

Typed or printed name Robert D. Summers, Jr. Registration No. 57,844

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	12063650
Filing Date:	12-Aug-2010
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Filer:	Robert Dalton Summers/Lori Peterson
Attorney Docket Number:	12838/5
Filed as Small Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	890	890
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**1190**

Electronic Acknowledgement Receipt

EFS ID:	17503517
Application Number:	12063650
International Application Number:	
Confirmation Number:	9949
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	Robert Dalton Summers/Maggie Pieczonka
Filer Authorized By:	Robert Dalton Summers
Attorney Docket Number:	12838/5
Receipt Date:	26-NOV-2013
Filing Date:	12-AUG-2010
Time Stamp:	14:02:48
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1190
RAM confirmation Number	331
Deposit Account	231925
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		128385if.pdf	140194 37f8f3a42910be20f843d021d7792a84317e404d	yes	3

Multipart Description/PDF files in .zip description

Document Description	Start	End
Miscellaneous Incoming Letter	1	1
Issue Fee Payment (PTO-85B)	2	3

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	32054 89fd152a6edbfb850fd8f3c352a42622391218a8	no	2

Warnings:

Information:

Total Files Size (in bytes):	172248

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8
I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS on the below date:

Date: November 26, 2013 Name: Robert D. Summers, Jr., Reg. No. 57,844 Signature: /Robert D. Summers, Jr./

BRINKS
GILSON
& LIONE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: BURKE, Christopher John

Appln. No.: 12/063,650

371 Filing Date: August 12, 2010

For: CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No: 12838/5 (729727US)

Examiner: Johns, Andrew W.

Group Art Unit: 2665

Confirmation No.: 9949

TRANSMITTAL

Mail Stop Issue Fee
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

☒ Transmittal Letter; Issue Fee Transmittal – Part B (2 pp.).

Fee calculation:

☐ No additional fee is required.

☒ Per 37 CFR §1.27, ☒ Applicants are small entity ☐ Applicants are micro entity.

☐ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

☐ A petition or processing fee in an amount of $_____ under 37 CFR § 1.17(_____).

☐ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

☒ Please charge Deposit Account No. 23-1925 in the amount of $890.00 for the Issue Fee and $300.00 for the Publication Fee.

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 associated with this paper (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

November 26, 2013
Date

/Robert D. Summers, Jr./
Robert D. Summers, Jr., Reg. No. 57,844

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/063,650	12/31/2013	8620039	12838/5	9949

757 7590 12/11/2013

BGL
P.O. BOX 10395
CHICAGO, IL 60610

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 912 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Christopher John Burke, New South Wales, AUSTRALIA;

Doc Code: PET.PTA.AIA1
Document Description: **Request for Recalculation in view of AIA**

REQUEST FOR RECALCULATION OF PATENT TERM ADJUSTMENT IN VIEW OF *AIA TECHNICAL CORRECTIONS ACT*

Attorney Docket Number: 12838-5	Patent Number: 8,620,039
Filing Date (or 371(b) or (f) Date): August 12, 2010	Issue Date: December 31, 2013

First Named Inventor: Christopher John Burke

Title: CARD DEVICE SECURITY USING BIOMETRICS

Patentee hereby requests Recalculation of the Patent Term Adjustment (PTA) under 35 U.S.C. 154(b) indicated on the above-identified patent. The international application issued as a patent after January 13, 2013 and before May 20, 2014.

A Request for Recalculation of Patent Term Adjustment under this optional procedure is not considered a Request for Reconsideration within the meaning of 35 U.S.C. 154(b)(3) and a Recalculation of Patent Term Adjustment under this procedure in not the Director's decision on an applicant's request for reconsideration within the meaning of 35 U.S.C. 154(b)(3)and (b)(4).

NOTE: This form must be filed prior to August 1, 2014. On or after August 1, 2014, patentee cannot use this optional procedure and must comply with the requirements of 37 CFR 1.705(b).

Signature /E. Brandon Nykiel/	Date July 30, 2014
Name (Print/Typed) E. Brandon Nykiel	Registration Number 62,972

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☑ *Total of 1 forms are submitted.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	19725980
Application Number:	12063650
International Application Number:	
Confirmation Number:	9949
Title of Invention:	CARD DEVICE SECURITY USING BIOMETRICS
First Named Inventor/Applicant Name:	Christopher John Burke
Customer Number:	757
Filer:	E. Brandon Nykiel/Maggie Pieczonka
Filer Authorized By:	E. Brandon Nykiel
Attorney Docket Number:	12838/5
Receipt Date:	30-JUL-2014
Filing Date:	12-AUG-2010
Time Stamp:	15:05:26
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		12838_5_RequestFiling_073014.pdf	70002 5c71c4404381157c745e8a130e764afee1ff605c	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Miscellaneous Incoming Letter	1	1
	Request for Recalculation in view of AIA	2	2
Warnings:			
Information:			
Total Files Size (in bytes):		70002	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

BRINKS
GILSON
& LIONE

CERTIFICATE OF EFS FILING UNDER 37 CFR §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, Commissioner for Patents, via the EFS pursuant to 37 CFR §1.8 on the below date:

Date: July 30, 2014 Name: E. Brandon Nykiel Signature: /E. Brandon Nykiel/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Christopher John Burke

Appln. No.: 12/063,650

Filed: August 12, 2010

For: CARD DEVICE SECURITY USING BIOMETRICS

Attorney Docket No.: 12838-5

Examiner: Johns, Andrew W.

Art Unit: 2665

Conf. No.: 9949

TRANSMITTAL

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is/are:

☒ Request for Recalculation of Patent Term Adjustment in View of AIA Technical Corrections Act.

Fee calculation:

□ No additional fee is required.

□ Per 37 CFR §1.27, □ Applicant is small entity □ Applicant is micro entity.

□ An extension fee in an amount of $_____ for a _____-month extension of time under 37 CFR § 1.136(a).

□ A petition or processing fee in an amount of $______ under 37 CFR § 1.17(_).

□ An additional filing fee has been calculated as shown below:

					Fee		Small Entity Fee		Micro Entity Fee	
	Claims Remaining After Amendment		Highest No. Previously Paid	Present Extra	Rate	Add'l Fee	Rate	Add'l Fee	Rate	Add'l Fee
Total		Minus			x $ 80 =	$	x $ 40 =	$	x $20 =	$
Independent		Minus			x $420 =	$	x $210 =	$	x $105 =	$
First Presentation of Multiple Dep. Claim					+ $780 =	$	+ $390 =	$	+ $195 =	$
					Total	$	Total	$	Total	$

Fee payment:

□ Please charge Deposit Account No. 23-1925 in the amount of $_____ for _____.

□ Payment by credit card in the amount of $_____ (Form PTO-2038 is attached).
WARNING: Information on this form may become public. **Credit card information should not be included on this form.**

☒ The Director is hereby authorized to charge payment of any additional filing fees required under 37 CFR § 1.16 and any patent application processing fees under 37 CFR § 1.17 (including any extension fee required to ensure that this paper is timely filed), or to credit any overpayment, to Deposit Account No. 23-1925.

Respectfully submitted,

July 30, 2014
Date

/E. Brandon Nykiel/
E. Brandon Nykiel (Reg. No. 62,972)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MAIL DATE : 09/29/2014

BGL
P.O. BOX 10395
CHICAGO, ILLINOIS 60610

Applicant: Christopher Burke
Patent Number: 8,620,039
Issue Date: 12/31/2013
Application No: 12/063,650
Filed: 08/12/2010

RECALCULATION OF PATENT
TERM ADJUSTMENT
AND
NOTICE OF INTENT TO ISSUE
CERTIFICATE OF CORRECTION

In view of patentee's request for recalculation of patent term adjustment in view of the AIA Technical Corrections Act, the patent term adjustment has been recalculated and determined to be 1707 days.

This recalculation of the patent term adjustment is a new patent term adjustment determination under 35 U.S.C. § 154(b)(3).

This recalculation is NOT a request for reconsideration within the meaning of 35 U.S.C. §154(b)(3) and a recalculation of patent term adjustment under this optional procedure is NOT the Director's decision on a patentee's request for reconsideration within the meaning of 35 U.S.C. §§ 154(b)(3) and (4).

A patentee who is satisfied with this recalculation need not respond. The Office will sua sponte issue a certificate of correction in the amount recalculated under this optional procedure in due course if the determination is in an amount different than what is printed on the front of the patent.

A patentee dissatisfied with the recalculation can request reconsideration under 35 U.S.C. § 154(b)(3) and § 1.705 of a new patent term adjustment determination done under this optional procedure by complying with the requirements of §§ 1.705(b)(1) and (2) no later than two months from the mail date of the new patent term adjustment resulting from the recalculation. This two-month period may be extended under the provisions of 37 CFR 1.136(a).

Patentee should use document code PET.OP if electronically filing a request for reconsideration of this patent term recalculation. The patentee must also include the information required by 37 CFR 1.705(b)(2) and the fee required by 37 CFR 1.18(e).

Patentee should be aware that in order to preserve the right to review in the United States District Court for the District of Columbia of the USPTO patent term adjustment determination, patentee must ensure that he or she also take the steps required under 35 U.S.C. 154(b)(3) and (b)(4) and 37 CFR 1.705 in a timely manner.

Any questions concerning this matter should be directed to Kery A. Fries Senior Legal Advisor, Office of Patent Legal Administration, Office of Deputy Commissioner for Patent Examination Policy at 571-272-7757.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MAIL DATE : 09/29/2014

BGL
P.O. BOX 10395
CHICAGO, ILLINOIS 60610

Applicant: Christopher Burke
Patent Number: 8,620,039
Issue Date: 12/31/2013
Application No: 12/063,650
Filed: 08/12/2010

RECALCULATION OF PATENT TERM ADJUSTMENT
AND
NOTICE OF INTENT TO ISSUE CERTIFICATE OF CORRECTION

In view of patentee's request for recalculation of patent term adjustment in view of the AIA Technical Corrections Act, the patent term adjustment has been recalculated and determined to be 1707 days.

This recalculation of the patent term adjustment is a new patent term adjustment determination under 35 U.S.C. § 154(b)(3).

This recalculation is NOT a request for reconsideration within the meaning of 35 U.S.C. §154(b)(3) and a recalculation of patent term adjustment under this optional procedure is NOT the Director's decision on a patentee's request for reconsideration within the meaning of 35 U.S.C. §§ 154(b)(3) and (4).

A patentee who is satisfied with this recalculation need not respond. The Office will sua sponte issue a certificate of correction in the amount recalculated under this optional procedure in due course if the determination is in an amount different than what is printed on the front of the patent.

A patentee dissatisfied with the recalculation can request reconsideration under 35 U.S.C. § 154(b)(3) and § 1.705 of a new patent term adjustment determination done under this optional procedure by complying with the requirements of §§ 1.705(b)(1) and (2) no later than two months from the mail date of the new patent term adjustment resulting from the recalculation. This two-month period may be extended under the provisions of 37 CFR 1.136(a).

Patentee should use document code PET.OP if electronically filing a request for reconsideration of this patent term recalculation. The patentee must also include the information required by 37 CFR 1.705(b)(2) and the fee required by 37 CFR 1.18(e).

Patentee should be aware that in order to preserve the right to review in the United States District Court for the District of Columbia of the USPTO patent term adjustment determination, patentee must ensure that he or she also take the steps required under 35 U.S.C. 154(b)(3) and (b)(4) and 37 CFR 1.705 in a timely manner.

Any questions concerning this matter should be directed to Kery A. Fries Senior Legal Advisor, Office of Patent Legal Administration, Office of Deputy Commissioner for Patent Examination Policy at 571-272-7757.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,620,039 B2 Page 1 of 1
APPLICATION NO. : 12/063650
DATED : December 31, 2013
INVENTOR(S) : Christopher John Burke

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

The first or sole Notice should read --

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1707 days.

Signed and Sealed this
Twenty-second Day of September, 2015

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Waco Divison on the following

□ Trademarks or ☑ Patents. (□ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:21-cv-00165	DATE FILED 2/23/2021	U.S. DISTRICT COURT Western District of Texas, Waco Divison	
PLAINTIFF CPC Patent Technologies Pty Ltd.		DEFENDANT Apple Inc.	

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 8,620,039	12/31/2013	CPC Patent Technologies Pty Ltd. by assignment
2 US 9,269,208	2/23/2016	CPC Patent Technologies Pty Ltd. by assignment
3 US 9,665,705	5/30/2017	CPC Patent Technologies Pty Ltd. by assignment
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY □ Amendment □ Answer □ Cross Bill □ Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy