



Industria y Comercio

SUPERINTENDENCIA

Delegatura de Propiedad Industrial

División de Nuevas Creaciones

PCT
SOLICITUD

PATENTE DE INVENCION

05-31213

21. EXPEDIENTE No. 05-31213

54. TITULO VERIFICACION DE IDENTIDAD BIOMETRICA SEGURA

51. CLASIFICACION INTERNACIONAL _____

71. SOLICITANTE IVI SMART TECHNOLOGIES, INC.

DOMICILIO San Jose, California, Estados Unidos de América.

74. APODERADO EMILIO FERRERO

C.C. 438.019 de Usaquén.

22. BOGOTA, D.C., _____

**Industria y Comercio**

SUPERINTENDENCIA

PETITORIO

SUPERINTENDENCIA Y COMERCIO
Rad. 2010 950111 00002080 Folios 12/1
Fecha (AND) 2005-04-07 17:40:43 el administrador
Trámite 011 PCT-PATENT 379 FASE NAC: 411 PRESENTA
Dependencia 2020 DIVISION DE NUEVAS CREACIONES

**FORMULARIO UNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL****SOLICITUD DE****1**☒ Patente de Invención☐ Patente de Modelo de Utilidad☐ Capítulo I☒ Capítulo II**2****SOLICITANTE
(71)**

Nombre **IVI SMART TECHNOLOGIES, INC**
sociedad constituida y existente bajo las
leyes del Estado de California Estados
Unidos de América

Dirección 1810 Old Oakland Road # F
San Jose California 95131
Estados Unidos de América
Domicilio San Jose California
Estados Unidos de América

IDENTIFICACIONC C ☐ NIT ☐C E ☐ Otro ☐

Cual _____

Numero _____

3**REPRESENTANTE
O APODERADO**

Nombre **EMILIO FERRERO**
Dirección Carrera 4ª No 72-35
Teléfono 347 36 11
Fax 217 92 11
E-mail clientes@camyp.com
Domicilio Bogotá Colombia

IDENTIFICACIÓNC C ☒ NIT ☐C E ☐ Otro ☐

Cual _____

Numero 438 019 T P 31 929**4****INVENTOR (ES)
(72)**

1 **Tamio SAITO**
388 Beale Street # 1507
San Francisco California 94105
Estados Unidos de América
3 **Wayne DRIZIN**
1810 Old Oakland Rd Suite F
San José California 95131
Estados Unidos de América

2 **Takashi AIDA**
928 Desert Isle Drive-
San Jose California 95117
Estados Unidos de América

5**PCT (86)**Solicitud Internacional No PCT/US2003/028602Fecha 10 de septiembre de 2003Publicación Internacional No WO 2004/025545 A3Fecha 25 de marzo de 2004**6****Título (54)****VERIFICACIÓN DE IDENTIDAD BIOMETRICA SEGURA****7****Clasificación Internacional (51) G06K 19/077****8****Prioridad**SI ☒ NO ☐**(33) País de Origen**USUSUSUSUS**(32) Fecha**10 de septiembre de 200210 de septiembre de 200227 de noviembre de 200213 de diciembre de 20023 de julio de 2003**(31) Número de Solicitud**60/409 71560/409 71660/429 91960/433 25460/484 692**9****Comprobante de pago No 05 - 19 198****Fecha 14 de marzo de 2005**

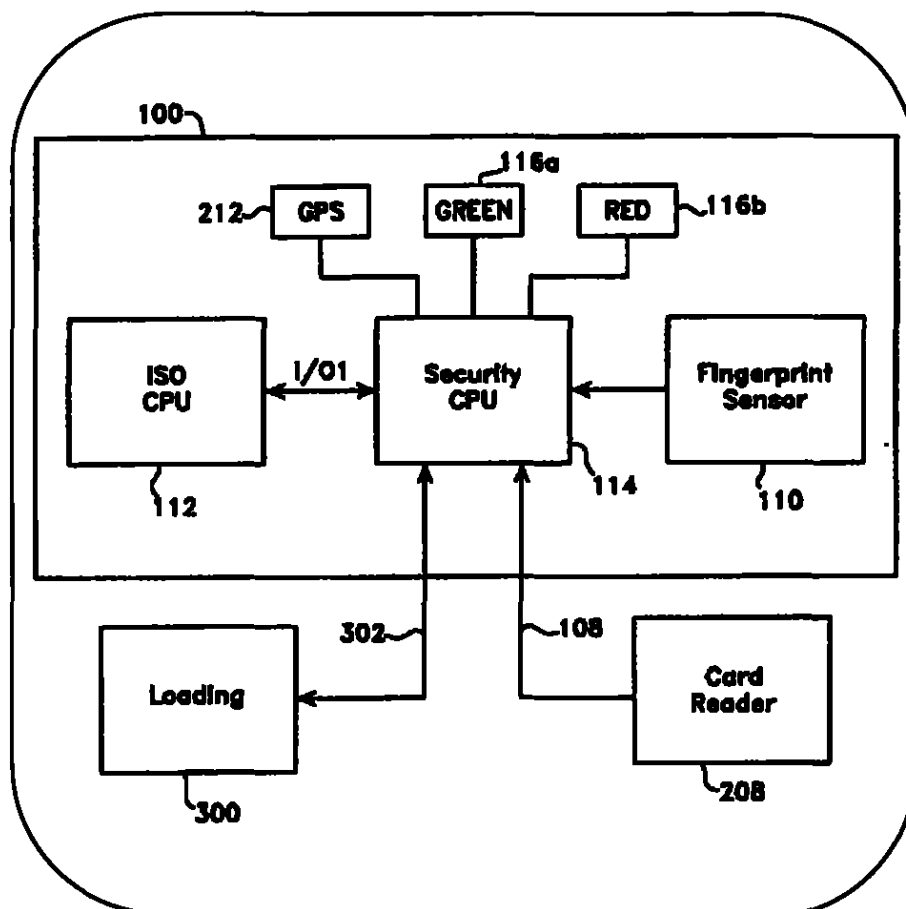
10

Anexos:

- ☒ Comprobante de pago de la tasa de presentación de la solicitud por \$ 443.000.00.
- ☐ Comprobante de pago por reivindicación de prioridad.
- ☐ Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Poderes, si fuere el caso.
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Declaraciones.
- ☒ Copia de la solicitud internacional. (Resumen, descripción, reivindicaciones, dibujos)
- ☒ Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones, dibujos)
- ☐ Copia del examen preliminar efectuado por la IPEA.
- ☐ Traducción del examen preliminar efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☒ Arte final 12x12
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☒ Otros: PCT/IB/306 Donde se notifica el cambio de domicilio del Inventor Tamio SAITO.

11

FIGURA CARACTERÍSTICA



12

Solicito la concesión de la patente,

NOMBRE: EMILIO FERREROFIRMA: *Emilio Ferrero*

C.C. 438.019 de Usaquén T.P. 31.929

RECEIVED PATENT COOPERATION TREATY

OCT - 1 2004

FULBRIGHT & JAWORSKI
PCT

From the INTERNATIONAL BUREAU

**NOTIFICATION OF THE RECORDING
OF A CHANGE**(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

To:

MAY, John, M.
Fulbright & Jaworski L.L.P.
29th floor
865 South Figueroa
Los Angeles, CA 90017-2571
United States of America

Date of mailing (day/month/year) 21 September 2004 (21.09.2004)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference LA-7167-102.PC	
International application No. PCT/US2003/028602	International filing date (day/month/year) 10 September 2003 (10.09.2003)

1. The following indications appeared on record concerning:

☒ the applicant
 ☒ the inventor
 ☐ the agent
 ☐ the common representative

Name and Address SAITO, Tamio 999 Bush, #205 San Francisco, CA 94109 United States of America	State of Nationality US	State of Residence US
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person
 ☐ the name
 ☒ the address
 ☐ the nationality
 ☐ the residence

Name and Address SAITO, Tamio 388 Beale Street #1507 San Francisco, CA 94105 United States of America	State of Nationality US	State of Residence US
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
 ☐ the designated Offices concerned
☐ the International Searching Authority
 ☒ the elected Offices concerned
☒ the International Preliminary Examining Authority
 ☐ other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Yuri POROHOVSKY (Fax 338-87-20)
Facsimile No. (41-22) 338.87.20	Telephone No. (41-22) 338 8787

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:

MAY, John, M.
Fulbright & Jaworski L.L.P.
29th floor
885 South Figueroa
Los Angeles, CA 90017-2571
ETATS-UNIS D'AMERIQUE

RECEIVED

Date of mailing (day/month/year) 25 March 2004 (25.03.2004)		APR 1 2 2004
Applicant's or agent's file reference LA-7167-102.PC		FULBRIGHT & JAWORSKI
IMPORTANT NOTICE		
International application No. PCT/US2003/028602	International filing date (day/month/year) 10 September 2003 (10.09.2003)	Priority date (day/month/year) 10 September 2002 (10.09.2002)
Applicant IVI SMART TECHNOLOGIES, INC. et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this notice:

AU, AZ, BY, CH, CN, CO, DZ, EP, HU, JP, KG, KP, KR, MD, MK, MZ, RU, TM, US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

AE, AG, AL, AM, AP, AT, BA, BB, BG, BR, BZ, CA, CR, CU, CZ, DE, DK, DM, EA, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, ID, IL, IN, IS, KE, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MG, MN, MW, MX, NI, NO, NZ, OA, OM, PG, PH, PL, PT, RO, SC, SD, SE, SG, SK, SL, SY, TJ, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this notice is a copy of the international application as published by the International Bureau on 25 March 2004 (25.03.2004) under No. WO 2004/025545

4. **TIME LIMITS** for filing a demand for international preliminary examination and for entry into the national phase

The applicable time limit for entering the national phase will, subject to what is said in the following paragraph, be 30 MONTHS from the priority date, not only in respect of any elected Office if a demand for international preliminary examination is filed before the expiration of 19 months from the priority date, but also in respect of any designated Office, in the absence of filing of such demand, where Article 22(1) as modified with effect from 1 April 2002 applies in respect of that designated Office. For further details, see *PCT Gazette* No. 44/2001 of 1 November 2001, pages 19926, 19932 and 19934, as well as the *PCT Newsletter*, October and November 2001 and February 2002 issues.

In practice, time limits other than the 30-month time limit will continue to apply, for various periods of time, in respect of certain designated or elected Offices. For regular updates on the applicable time limits (20, 21, 30 or 31 months, or other time limit), Office by Office, refer to the *PCT Gazette*, the *PCT Newsletter* and the *PCT Applicant's Guide*, Volume II, National Chapters, all available from WIPO's Internet site, at <http://www.wipo.int/pct/en/index.html>.

For filing a demand for international preliminary examination, see the *PCT Applicant's Guide*, Volume I/A, Chapter IX. Only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination (at present, all PCT Contracting States are bound by Chapter II).

It is the applicant's sole responsibility to monitor all these time limits.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Gijsbertus Beijer - Carlos Roy
Facsimile No.(41-22) 740.14.35	Telephone No.(41-22) 338.91.11

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
25 March 2004 (25.03.2004)

PCT

(10) International Publication Number
WO 2004/025545 A3

(51) International Patent Classification⁷: G06K 19/077,
G07C 9/00

(21) International Application Number:
PCT/US2003/028602

(22) International Filing Date:
10 September 2003 (10.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/409,716 10 September 2002 (10.09.2002) US
60/409,715 ~ 10 September 2002 (10.09.2002) US
60/429,919 ~ 27 November 2002 (27.11.2002) US
60/433,254 ~ 13 December 2002 (13.12.2002) US
60/484,692 3 July 2003 (03.07.2003) US

(71) Applicant (for all designated States except US): IVI
SMART TECHNOLOGIES, INC. [US/US]; 1810 Old
Oakland Road, #F, San Jose, CA 95131 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): SAITO, Tamio
[US/US]; 999 Bush, #205, San Francisco, CA 94109 (US).

AIDA, Takashi [JP/US]; 928 Desert Isle Drive, San Jose,
CA 95117 (US). DRIZIN, Wayne [US/US]; 1810 Old
Oakland Rd. Suite F, San Jose, CA 95131 (US).

(74) Agent: MAY, John, M.: Fulbright & Jaworski L.L.P., 29th
floor, 865 South Figueroa, Los Angeles, CA 90017-2571
(US).

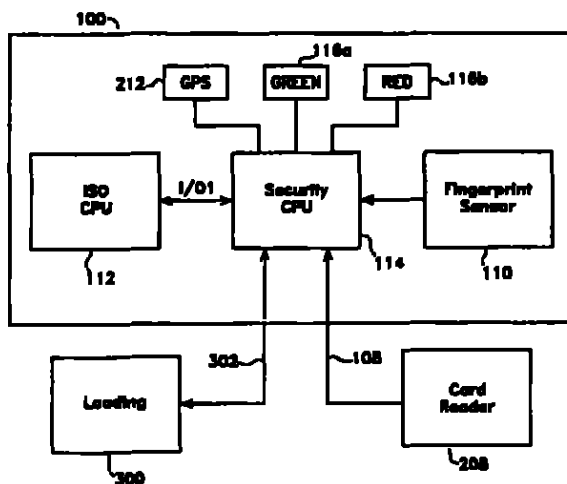
(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE,
GH, GM, GR, GU, HK, IL, IN, IS, JP, KE, KG, KP, KR,
KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,
MN, MW, MX, MY, MZ, NI, NO, NZ, OM, PG, 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 (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, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (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: SECURE BIOMETRIC VERIFICATION OF IDENTITY



(57) Abstract: A high security identification card includes an on-board memory for stored biometric data and an on-board sensor for capturing live biometric data. An on-board processor on the card performs a matching operation to verify that the captured biometric data matches the locally stored biometric data. Only if there is a positive match is any data transmitted from the card for additional verification and/or further processing. Preferably, the card is ISO SmartCard compatible. In one embodiment, the ISO SmartCard functions as a firewall for protecting the security processor used for storing and processing the protected biometric data from malicious external attack via the ISO SmartCard interface. In another embodiment, the security processor is inserted between the ISO SmartCard interface and an unmodified ISO SmartCard processor and blocks any external communications until the user's fingerprint has been matched with a previously registered fingerprint. Real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor. The card may be used to enable communication with a transactional network or to obtain physical access into a secure area.



— 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.

(88) Date of publication of the international search report:
24 June 2004

SECURE BIOMETRIC VERIFICATION OF IDENTITY

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is based on, and claims priority from, provisional applications 60/409,716 filed September 10, 2002 (docket number 7167-102P1), 60/409,715 filed September 10, 2002 (docket number 7167-103P), 60/429,919 filed November 27, 2002 (docket number 7167-104P), 60/433,254 filed December 13, 2002 (docket number 7167-105P), and 60/484,692 filed July 3, 2003 (docket number 7167-106P), which are hereby incorporated by reference in their entirety.

BACKGROUND

[0002] Computerization and especially internet technology has been providing ever greater access to data, including financial data, medical data, personal data, and with means to expedite financial and other transactions in which confidential data is updated or exchanged.

[0003] Passwords are commonly used to maintain the confidentiality of such data; however, passwords are frequently based on a birth date or phone number that is simple to guess and that is not secure at all. Furthermore, even a complicated randomly generated password can often be readily stolen. Password-based data accessing systems are thus vulnerable to criminal attack with resultant risk and damage to industry and the economy and even to people's lives. Accordingly, there is a need for an improved method for securing data and protecting that data from unauthorized access.

[0004] Biometric data can include precise details that are difficult to capture but easy to analyze (such as a sequence of fingerprint minutia) or overall patterns that are easy to capture but difficult to analyze (such as the spatial characteristics of adjacent fingerprint whorls).

[0005] Encryption algorithms exist that require a digital key available only to authorized users. Without the proper key, the encrypted data can be decrypted

into a usable format only with a substantial investment of time and processing resources, and even then, only if certain characteristics of the unencrypted data are known (or at least are predictable).

[0006] Japan Published Patent Application JP 60-029868 dated February 15, 1985 in the name of Tamio SAITO teaches an individual identification system that employs an identity card with an integrated memory for registering enciphered biometric data obtained from the card holder. The biometric data may include a voiceprint, fingerprint, physical appearance, and/or a biological assay. In use, the data on the card is read and deciphered for comparison with corresponding data captured from the person presenting the card. Such a system permits a registered individual to be positively identified with a high degree of accuracy. However, because the biometric data is obtained and processed by external equipment, it is difficult to protect the information stored on the card against possible alteration and/or identity theft.

[0007] An improved identification card has been proposed which includes a data driven multi-processor chip on the card to provide a hardware firewall that both encrypts and isolates the biometric data stored on the card, thereby providing substantially greater protection against unauthorized alteration of the stored data. However, the actual matching process was performed in the same external reader terminal that captured the live biometric data, and was thus still potentially vulnerable to external fraudulent manipulation.

SUMMARY

[0008] A first embodiment of a high security identification card includes not only an on-board memory for the stored biometric data, but also an on-board sensor for capturing the live biometric data. A remote authentication system maintains a secure database including the biometric data. An on-board processor on the card performs a preliminary matching operation to verify that the captured biometric data matches the locally stored biometric data. Only if there is a positive local match is any captured data or any sensitive stored data transmitted to the remote authentication system for additional verification and further

processing. As a further protection against malicious attack, the locally stored data is preferably different from the remotely stored data, and the local match and the remote match preferably are conducted utilizing different matching algorithms. Thus even if the card, the locally stored data, and/or the local terminal to which the card is connected is ever compromised, there is a high probability that the remote authorization system will still be able to detect the attempted intrusion.

[0009] A second embodiment also includes an on-board memory for the stored biometric data, an on-board sensor for capturing the live biometric data and an on-board processor; however, in that embodiment the entire matching process is performed by the on-board processor and both the originally captured biometric data and any other "private" information stored in the on-board memory are not made available to any external processes. Instead, only a verification message is generated in response to a successful match between the newly captured biometric data and the previously captured biometric data. The verification message causes the card to function in a manner similar to a conventional ISO SmartCard upon the successful/unsuccessful entry of a conventional Personal Identification Number (PIN), but with the additional security afforded by a more secure verification process. In either of those embodiments, the stored biometric data and any associated locally stored encryption algorithm or encryption key is preferably loaded onto the card at the time of original issuance to the card holder in a manner that discourages any subsequent external access, thereby further enhancing the integrity of stored biometric data and of the entire verification process.

[0010] In one embodiment, the ISO SmartCard functions as a firewall for protecting the security processor used for storing and processing the protected biometric data from malicious external attack via the ISO SmartCard Interface. In another embodiment, the security processor is inserted between the ISO SmartCard Interface and an unmodified ISO SmartCard processor and blocks any external communications until the user's fingerprint has been matched with a previously registered fingerprint.

[0011] In one preferred embodiment of a high security identification card with on-board fingerprint matching capability, real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor. This feedback not only reduces computational complexity but also provides additional means for discriminating between an inexperienced user and a fraudulent user, thereby further reducing the probability of false negatives and/or false positives. In another preferred embodiment, the fingerprint sensor is retained in a carrier that provides additional stiffness.

[0012] In one exemplary application, the captured biometric data and/or an indication of the cardholder's identity is encrypted and input to a transactional network including a financial institution and a separate authentication server prior to any grant of on-line access to confidential data or to any automated process for completing a secure transaction. In another exemplary application, the output from the card is used to obtain physical access into a secure area. In either application, a record of successful and unsuccessful access attempts can be maintained either on the card or at an external security server, or both.

DRAWINGS

[0013] Fig. 1 shows one embodiment of a smart card with on-board biometric verification of the identity of the person presenting the card.

[0014] Fig. 2 is a flowchart showing an exemplary process for assisting the user in the optimal placement of a finger on the fingerprint sensor.

[0015] Fig. 3 is a functional block diagram of a biometric verification system capable of both local and remote verification of the identity of a person presenting a secure identification card.

[0016] Fig. 4 is a functional block diagram of an exemplary biometric verification card with different physical data paths for use during initial loading of the cardholder's biometric data and during verification of the cardholder's identity to a remote application.

[0017] Fig. 5 shows an alternative embodiment to the exemplary biometric verification card of Fig. 4, which is intended for use with an unmodified ISO SmartCard CPU.

[0018] Fig. 6 is a flowchart showing the communication between an exemplary application and an exemplary verification card in which only local verification of the card holder's identity is performed.

[0019] Fig. 7 is similar to the flowchart of Fig. 6, but modified for use with the exemplary biometric verification card of Fig. 5.

[0020] Fig. 8 shows a second embodiment of a smart card with on board biometric verification that can be connected to a local terminal either wireless or by means of an electrical connector.

[0021] Fig. 9 is a cross section through the card of Fig. 8.

[0022] Fig. 10 is a circuit diagram of an exemplary fingerprint sensor.

[0023] Fig. 11 shows one embodiment of a carrier assembly for the sensor of Fig. 10.

DETAILED DESCRIPTION

Smart Card.

[0024] The phrase "smart card" or "intelligent card" is used herein in a generic sense to refer to any physical object that is small enough to be held in the hand, worn about the neck, or otherwise carried about the person and that includes a microprocessor that is capable of storing, processing and communicating digitally encoded information concerning or otherwise related to an individual cardholder. One well known example of such a smart card is the ISO (International Standards Organization) SmartCard, which has the same physical size and shape of a conventional credit card, but which includes flash memory for storage of user specified data and a microprocessor which can be programmed with a powerful encryption algorithm that indicates whether or not a PIN (Personal Identification Number) received from a user terminal matches an encrypted PIN

stored on the card, thereby providing a higher degree of confidence that the person presenting the card is the real card holder than would be possible in a verification system that merely relies on a visual comparison of signatures and/or physical likeness.

[0025] Reference should now be made to Fig. 1, which shows one embodiment of a smart card with on-board biometric verification. The card 100 is generally made of a plastic material and has the overall appearance of a conventional credit card, of approximate dimensions as specified in ISO 7816 of approximately 53.98 x 85.6 mm and thickness of approximately 0.76 mm or more.

[0026] Similar to a conventional credit card, card 100 includes a free upper region 102 extending along the entire transverse width of the card for supporting a magnetic stripe (as specified by ISO 7811-2 & 7811-6) on the back surface of the card, on which may be stored conventionally encoded alphanumeric information about the card holder and any associated account, thereby permitting card 100 to be used in a conventional magnetic stripe reader. However, because any data embedded in the magnetic stripe can easily be altered, such a magnetic stripe is intended only for use in certain applications where the need for backwards compatibility with older magnetic stripe based terminals outweighs the potential degradation of security that a magnetic stripe brings to the system.

[0027] Upper region 102 may also be used to support various fraud prevention measures, such as a tamper-resistant colored photograph of the cardholder and/or a holographic logo of the card issuer. The lower region 104 of card 100 may be used in conventional fashion for embossed information (as specified by ISO 7811-1) such as the name of the cardholder, a numerical account (or card) identifier, and an expiration date, to permit the use of card 100 in a conventional card imprinter.

[0028] Upper region 102 and lower region 104 are separated by a middle region 106 in which are embedded a set of 8 visible ISO SmartCard contact pads 108, which provide a convenient electrical connection between the card and corresponding contacts on a card reader. By this means, not only data, but also

power, timing and control signals may be exchanged between the reader and the card as specified in ISO 7816-3.

[0029] On the right side of region 106 a sensor pad 110 is visible, which is used to capture fingerprint data from the cardholder's finger. The card preferably is provided with an ID code that is unique to sensor 110 or other electronic component embedded in the card; for example, a code in the format of a conventional IP and/or MAC address.

[0030] Also indicated schematically in Fig. 1 are several additional electronic components that cooperate with contact pad 108 and sensor 110 to provide greater functionality, and in particular better security, than would otherwise be possible.

[0031] In one embodiment, ISO SmartCard compatible processor 112 is directly connected to ISO contact pads 108 to provide an electrical connection with an external ISO compatible card reader (not shown) to thereby not only provide power to the on-board electronics, but also a means for communicating data between the card and any external communication software, security software, transactional software, and/or other application software running on the card reader or any associated computing devices networked with the card reader.

[0032] Although in the depicted embodiment the data path between the card 100 and the external card reader is in the form of a wired connection using an ISO specified SmartCard contact arrangement, it should be understood that in other embodiments, other transmission technologies can also be used such as USB or RS 232C or SPI (serial) connections, possibly over wireless RF (Radio Frequency), microwave and/or and IR (InfraRed) communication links.

[0033] Also, although the described embodiment receives power from the card reader, other embodiments could have an on-board source of power such as a solar cell or a battery. Such an on-board power source might be advantageous, for example, if the mechanical interface between the card 100 and a particular type of card reader is such that the fingerprint sensor 110 is not accessible to the user when the contacts 108 are connected to the corresponding connections

inside the card reader, and thus the user's fingerprint data must be captured when the card 100 is not directly wired to the card reader.

Security Processor

[0034] As illustrated, Security processor 114 is connected between ISO processor 112 and sensor 110 for providing secure processing and storage of the captured data, as well as a secure "firewall" to protect the data and programs stored in its dedicated memory from any improper access attempt via the ISO processor 112, as will be described hereinafter. Such a firewall may be designed pass only encrypted data using an encryption key which is based on a uniquely assigned network address or that otherwise is unique to the particular card, such as data extracted from a previously stored fingerprint pattern or a uniquely assigned device number such as CPU number or a fingerprint sensor number. In another embodiment, the Firewall only passes data which contains unique identifying data from a previous transmission, or data. In yet other embodiments, the Firewall maintains different keys for different applications, and uses those keys to route the data to a respective different processor or memory partition.

[0035] In another embodiment (not illustrated), the Security processor 114 is directly connected to the ISO contacts 108 and acts as a secure gatekeeper between the ISO processor 112 and the ISO contacts 108. Such an alternate arrangement has the advantage of providing the additional security afforded by Security processor 114 and sensor 110, without any possible compromise of any security features that may already be incorporated into ISO processor 112.

[0036] Security processor 114 preferably includes a non-volatile semi-conductor or non-semi conductor memory, such as FRAM, OTP, E²PROM, MRAM, MROM, for storing a previously enrolled fingerprint pattern and/or other personal biometric information. In other embodiments, some or all of the functions of security processor 114 could be implemented in ISO processor 112 and/or some or all of the functions of ISO processor 112 could be implemented in security processor 114. Such a combined implementation could still maintain a software firewall between the various functions, which would be especially advantageous

if the device was implemented with a process that did not permit any subsequent modification to the stored software programs. Alternatively, both processors 112, 114 could be separate processors in a single multi-processor device designed to protect each process from any interference from another process running in a different processor. One example of such a multi-processor device is the DDMP (Data Driven Multiple Processor) from Sharp of Japan.

[0037] Although these various sensors, contacts, and other electronic components, as well as the printed circuits or other electrical wiring with which they are interconnected, are all preferably incorporated entirely inside the body of the card 100 such that they are protected from abrasion and external contaminants, the preferred location within the middle region 106 between upper region 102 and lower region 104 further protects them from possible damage from the conventional magnetic stripe readers, embossers, and imprinting equipment that mechanically interfaces with those other regions.

LED Feedback

[0038] LEDs 116a, 116b are controlled by security processor 114 and provide visible feedback to the user. In the illustrated embodiment, they are located in lower region 104 preferably at a location at the side edge of the card remote from contact pads 108. In any event, LEDs 116a, 116b are preferably located where they will not be damaged during any embossing process and where they will be visible when the card is inserted into a conventional ISO SmartCard reader and/or while the user's finger is placed over the fingerprint sensor 110. For example:

In Verify Mode:

- RED blinking: Waiting for finger
- stop blinking: Finger placed on sensor
- RED blink once: Unable to match, ok to move finger
- GREEN long blink once: Matched, ok to remove finger

In Enroll Mode

- GREEN blinking: Waiting for finger
- stop blinking: Finger placed on sensor
- RED blink once: Unable to enroll, ok to move finger
- GREEN blink once : Enrolled, ok to remove finger

In Erase Mode

- GREEN and RED blinking: Ready to erase
- GREEN blink once: Erased

[0039] The User is preferably given multiple opportunities to position his finger for a successful Match or Enroll before any negative report is transmitted. In one embodiment, a negative report is transmitted to the Authentication Server only if the User has removed his finger before receiving the green ok indication, or if a predetermined time limit has been exceeded. Such a process not only trains the User to make an optimal placement of his finger over the sensor, which not only reduces computational complexity but also permits the use of more discriminating thresholds. This visible feedback also provides a psychological basis for discriminating between an inexperienced user (who will typically keep trying until he achieves the proper placement) and a fraudulent user (who will typically not want to attract any attention and will leave before his malicious intentions are discovered). The net result is a significant reduction in the probability of false negatives and/or false positives.

[0040] Fig. 2 illustrates an exemplary process for assisting the User to place his finger on sensor 110. In block 150, the RED LED 116b is blinking. Once a finger has been detected (block 152), the LED stops blinking and a test (block 154) made for image quality (defined elongated regions corresponding to the mountains and valleys of the finger's skin). If the quality is inadequate (NO branch 156), a single blink of RED LED 116b instructs the User to move his finger to a different position (block 158); otherwise (YES branch 160) a second

test (block 162) is performed to determine whether the same finger has been placed in the same position as was used to enroll the User such that a relatively simple Matching algorithm can verify the live data corresponds to the stored data within a predetermined threshold, thereby verifying that the live finger is the same as the finger that was originally enrolled (YES branch 164) and the GREEN LED 116a is activated (block 166) for a sufficient time (block 168) to verify that a successful match has been made and the User may now remove his finger. Alternatively, if the matching threshold is not met (NO branch 170), a single blink of RED LED 116b (block 158) instructs the User to move his finger to a different position and the process is repeated.

Exemplary Network architectures

[0041] Reference should now be made to Fig. 3 which illustrates one possible embodiment of a biometric verification system capable of both local and remote verification of the identity of a person presenting a secure Identification card. It includes three main components: a client terminal 200, an application server 202 and an authentication server 204. The client terminal 200 includes functionality for live capture and local processing of a user's fingerprint, for encryption of the locally processed data, and for secure communication with the application server and the authentication server, preferably over the Internet using the IP/TCP addressing scheme and transmission protocol, with protection from malicious access being provided by conventional IP firewalls 206. In other embodiments the firewalls 206 may be provided with Filters and Encryption Encoder/Decoder which encode transmitted data after it has been verified to be Authorized data and which decode received data before deciding whether it is in fact Authorized data, for example using an encryption algorithm such as DES128. By this means, the firewall 206 can classify data as Authorized or potentially Malicious based not only on the message header, but also based on the message content.

[0042] The Client Terminal 200 may be implemented as a dedicated web appliance, or may be implemented in software installed on a programmable desktop, notebook or other workstation or personal computer controlled by a

general purpose operating system such as Windows XXX, OS X, Solaris XX, Linux or Free BSD. Client Terminal 200 preferably includes up-to-date "negative" databases (for example identities of lost or stolen cards, or restrictions on a particular card or group of cards) that afford an additional measure of security.

[0043] The application server 202 includes functionality for conducting a transaction or otherwise responding to instructions from the remote user at client terminal 200 after the user's identity has been verified by authentication server 204. The authentication server 204 includes functionality for secure communication with both client terminal 200 and application server 202, for storing authentic fingerprint data and other information concerning previously registered users, for comparing the stored data with the encrypted live data received from the client terminal 200, and for advising the application server 202 whether or not specified live fingerprint data matches specified stored fingerprint data.

[0044] More particularly, Client Terminal 200 further comprises two main components: a fixed card reader 208 component including an internet browser terminal 210 and a card reader interface 108a (which may be a simple USB cable terminating in a set of electrical contacts for forming respective electrical connection with ISO SmartCard contact pads 108) and a portable smart card component 100'. In one embodiment, the portable component 100' may be the previously described smart card 100 including the fingerprint sensor 110, the security processor 114 and the ISO SmartCard processor 112.

[0045] Application Server 202 further comprises an Internet server interface including the firewall 206 and internet browser 214, as well as a transactional application module 216 and a validation module 218. In the event the application server and application module 216 are legacy devices that were not designed to communicate externally by means of the IP/TCP protocol, the firewall 206 can be replaced with an appropriate protocol converter which incorporates the validation module 218 and which has a fixed IP address. Application Service Server may

for example be operated by a third party who is willing to provide service through Internet to an authorized User.

[0046] Authentication Server 204 further comprises an internet server interface 220, a processing module 222 including a fingerprint matching algorithm 224, and a database 226 for storing fingerprint and other authentic information collected from individuals at the time those individuals were registered with the system and their identity was guaranteed to the satisfaction of the system operator. As a further security enhancement, the stored data for any particular individual is preferably not stored on the Application Server as a single sequence of information but rather each item is stored separately and any required indices or relationships connecting those items are accessible only by means of a corresponding key that is maintained as part of that individual's private data in the Authentication Server.

Location

[0047] In certain embodiments, the fixed reader 208 and/or the portable card 100" may also be equipped with an integral Global Positioning Satellite ("GPS") receiver 212 which can provide useful information about the current location of the reader and card at or about the time a particular transaction is taking place. In particular, the location data from GPS receiver 212 may be used to disable (either permanently or temporarily) the reader and/or the card in the event either is removed to a location at which their use is not authorized. Position may also be automatically determined by means other than GPS, for example using PHS (Japanese Cellular Telephone) caller location technology, or location sensors responsive to local variations in the earth's electro-magnetic fields. In the particular case of a GPS equipped card, the various GPS components including antennae; signal amplification, AD converter and sample and hold circuits; and digital processor to calculate the position are preferably all part of a single integrated circuit or discrete devices mounted on a single circuit board, which is integrated with, embedded in, or laminated to the body of the card.

Card architecture for ISO card with on-board matching

ISO Processor Interfaces

[0048] Fig. 4 is a functional block diagram of an exemplary ISO-SmartCard compatible biometric verification card 100 or 100' with different physical data paths for use during initial loading of the cardholder's biometric data and during verification of the cardholder's identity to a remote application.

[0049] In particular, in addition to the previously described ISO Processor 112, Security Processor 114, Fingerprint Sensor 110, LED's 116a, 116b and optional GPS receiver 212, with only ISO Processor 112 being directly connected to Card Reader 208 via ISO SmartCard contact pads 108, there is shown a separate Loading module 300 and associated temporary connection 302, which provides for direct communication with Security Processor 114 during initial User Registration. It may be noted that ISO Processor 112 communicates with Security Processor 114 by means of I/O ports 304, 306, while temporary Loading connection 302 is connected to a separate I/O port 308. Security Processor is preferably programmed such that any sensitive security related data or software are accessible only from port 308 and not from ports 304 and 306, thereby avoiding any possibility of malicious access to these sensitive data after connection 302 has been disabled.

[0050] Most commercially available ISO processors have at least two I/O ports and some have at least three. Only one of these ports (I/O 1) is designated for the conventional ISO SmartCard serial data connection 108 to the external ISO compatible Card Reader 208. The extra one or two I/O ports preferably provide a dedicated hardwired communication between the ISO Processor 112 and Security Processor 114 which acts as a hardware firewall to block any malicious attempts to reprogram the Security Processor 114 or to gain access to any sensitive information which may have been previously captured by sensor 110 or which may otherwise be stored within Processor 114. In the particular case of an ISO Processor with more than two I/O lines, it is possible to present more than two states of static status information on the dedicated communication path

between the ISO Processor and the Security Processor, such as 1) Ready, 2) Busy 3) Fail, and 4) Pass even when the Security Processor is completely powered down. Of course, even if only one I/O port is available those four conditions can be transmitted dynamically as serial data.

[0051] Among the possible commands and data that may be transmitted between the ISO CPU and the Security CPU over the ISO interfaces I/O 2 and I/O 3 are the following:

- Commands to enroll or authenticate a User, to which the Security CPU will send result of enrollment or result of authentication for local storage and/or transmission to a remote application.
- Fingerprint information as a template (reference) can be sent from Security CPU to ISO CPU for storage in the ISO SmartCard memory for transmission to remote applications. For increased security of sensitive personal information, the reference data can be encrypted by the security CPU before it is sent to the ISO CPU.

[0052] Loading connection 302 provides a direct connection to security CPU 114 that bypasses any firewall protection afforded the ISO connection and associated dedicated I/O ports 304 and 306, while possibly maintaining communication between ISO CPU 112 and ISO reader 208 so that power will also be available to Security CPU 114. It is primarily used during initial registration of the card to a particular user, and should be protected against unauthorized access.

[0053] Fig. 5 shows an alternative embodiment to the exemplary biometric verification card of Fig. 4, which is intended for use with an unmodified ISO SmartCard CPU. In particular, the ISO CPU 112' no longer must perform any gateway functions between Card Reader 208 and Security CPU 114', either during normal use or during loading, and thus it can be any ISO approved chip, not modified in any way and used only in a manner that is absolutely transparent to both the Card Reader 208 and to any external application. In such an alternative embodiment, Security CPU 114' acts as a transparent firewall

between the ISO CPU 112' and any external application if the captured fingerprint matches the stored fingerprint, and blocks all such communication if the captured fingerprint does not match the stored fingerprint.

Card Initialization and Protection of Stored Data

Gullotine

[0054] In one embodiment, the originally manufactured Card has a protruding printed circuit extension which provides a direct connection to the Security CPU, as well as to at least portions of the ISO interface and/or any discrete on board memory. This direct connection interface is used only for testing card and enrolling fingerprint data and includes the signal which enables the enrollment process. After the enrollment has been completed, this circuit extension is mechanically cut off so that no further enrollment will be possible, and the Security CPU memory is accessible only through the ISO CPU and the previously mentioned Firewall between the ISO CPU and the Security CPU.

Fuse

[0055] In another embodiment, the Security CPU has a type of memory which once the enrolled fingerprint pattern is written, will then be inaccessible. One example of such a memory is one time PROM ("OTP") which is similar in construction to EEPROM, but is opaque to UV and thus cannot be erased. Another example is Flash ROM which is rendered read only after enrollment has been completed, for example by applying sufficient current to a portion of the Enable or Address or Data signal path to form a physical break ("fuse") in that signal path.

Exemplary Authentication Processes

[0056] In one embodiment, an exemplary authentication process involves capturing physical fingerprint data, for example, using optical or pressure or conductive or capacitive or acoustical or elastic or photographic technologies at the Client Terminal used by the accessing person to connect to the Application Service Server, which is then sent (preferably in encrypted form) to a separate Fingerprint Authentication Server. The Fingerprint Authentication Server

compares the captured fingerprint data to a Fingerprint File, which includes the User's registered fingerprint data, using Authentication Software, and if the data is matched the Authentication Server sends an enabling instruction to the Application Service Server.

[0057] In another embodiment, the User accesses the secured WEB browser of the Fingerprint Authentication Server, which contains files of fingerprint, where all the fingerprints are pre-registered along with individual data, such as name, address, and date of birth. The secured Fingerprint Authentication Server, which User is accessing through a secure protocol such as HTTPS format, then sends an instruction to the Client Terminal to capture the User's finger print at the Client Terminal. In response to instructions displayed by the browser of the Client Terminal, the User puts his selected finger on the Fingerprint Sensor and the Fingerprint Capture Software residing in the Client Terminal captures a digital fingerprint, for example a pixel-based image with a 25 micron to 70 micron pitch resolution and an area of 12.5 mm to 25 mm square, and further having an 8-bit gray scale.

[0058] The Secure Fingerprint Authentication Server receives the fingerprint data along with User ID as well as Internet IP address and/or fingerprint sensor individual code (MAC address) and/or cookie and/or any unique code or other information identifying the particular Individual or terminal (for example, details from a previous conversation between Client Terminal and secured Fingerprint Authentication Server), whereupon it compares the received Fingerprint Data to a Fingerprint File, which is the pre-registered fingerprint data along with user ID, individual information such as name, address, date of birth, crime record, drivers license, social security number, etc, using Authentication Software, which may be minutiae comparison and or Fast Fourier Transform Comparison.

[0059] At the commencement of the Authentication process, the Web Server 214 for the relevant application visually or audibly instructs the User to put his finger on the Fingerprint Capture Sensor 110 and to click his mouse button or keyboard key to thereby intimate the Fingerprint Capture Software In Security

Processor 114. Then the User's captured fingerprint data is sent in encrypted format (for example, using the secure RSA encrypted transmission protocol HTTPS), to Web Server 220 of Fingerprint Authentication Server 204 via the ISO Processor 112 and Web Browser 210 of Client terminal 200. If the captured data is successfully matched to corresponding data in its Database 226, Fingerprint Authentication Server 204 then validates the User's identity to both the Client Terminal 200 and to the Application Server 202.

[0060] An exemplary preferred embodiment utilizing a Three Way Authentication Protocol and a Onetime Password as a Hash Character Encoding Sequence will now be described with reference to Fig. 3:

- Web Browser 210 of Client Terminal 200 accesses the corresponding Web Interface 214 of Application Server 202 with a request to access Application Process 216.
- Web Interface 214 of Application Server 202 responds with LOG-IN screen information and related instructions for accessing Application Process 216.
- Client Terminal 200 instructs ISO Processor 112 to activate Security Processor 114.
- ISO Processor 112 triggers Security Processor 114.
- Security Processor 114 awaits Fingerprint Data from Fingerprint Sensor 110 and when valid data is received, extracts a digital Fingerprint Pattern which is forwarded to Web Browser 210 via ISO Processor 112.
- Web Browser 210 sends an encrypted version of the extracted Fingerprint Pattern to Authentication Server 204 accompanied by (or encrypted with) Related Information about the involved Card 100' and Card Reader 208, such as User ID, IP address of Client Terminal 200, and/or hardwired ID code (MAC address) of Sensor 110.
- Web Interface 220 of Authentication Server 204, upon receiving the extracted Fingerprint Pattern along with the other information from Client Terminal 200, forwards that information to the Fingerprint Matching Processor 222.

- Under the control of Matching Software 224, Fingerprint Matching Processor 222 uses the received User ID or other User specific Related Information to retrieve a corresponding reference Fingerprint Pattern from Database 226 and compares the captured Fingerprint Pattern to the reference Fingerprint Pattern.
- The result (Matched or Unmatched) is stored in an Access History log together with the Related Information identifying the Terminal 200, User ID Card 100' and requesting Application 216, and control is returned to Authentication Server Web Interface 220.
- If the result is Matched, Authentication Server Web Interface 220 then generates a One Time Password in the form of a Challenge Character Sequence which is transmitted to Client Terminal 200, and uses that Challenge Character Sequence as a Hash code to encrypt the Related Information which it saves as the corresponding Challenge Response for possible future reference.
- Client Terminal 200 uses the received Challenge Character Sequence as a Hash code to encrypt a previously stored unencrypted copy of the submitted Related Information, which it then forwards to the Web Interface 214 of Application Server 202 as part of its response to the Application Log-In Process.
- Web Interface 214 of Application Server 202 upon receiving Hash converted Related Information, forwards it to the Application Service 216 which associates it with an on going Log-On attempt from that Client Server, and, for the purpose of confirming the Matched result, forwards the received Related Information which was Hashed by the Client Terminal using the Challenge Sequence provided by the Authentication Server as Challenge Response.
- The Web Interface 220 of Authentication Server 204, upon receiving the Challenge Response from the Application Server, forwards that Response to the Authentication Process 222 which compares it with its previously

saved reference copy of the expected Challenge Response to determine whether the User's Identity has in fact been authenticated.

- Any authenticated User Identity information resulting from that comparison is then returned to the Application Process 216 via the Authentication Server Web Interface 220 and the Validation Interface 218 of Application Server 202.
- Validation Interface 218 uses the Authentication to confirm the User's Identity as established in the original Log-On attempt has been validated.
- Once the User's Identity has been confirmed, Authentication Process 216 then proceeds to communicate directly with Web browser 210 of Client Terminal 200 via Web Interface 214 of Application Server 202.

[0061] Fig. 6 illustrates an alternative authentication process in which all matching is performed on the ISO compatible card of Fig. 4 by the Security CPU 114 and no external Authentication Server 204 is utilized. The left hand side of Fig. 6 shows the functions performed by Application Server 202, while the right hand side shows the functions performed by ISO SmartCard 100.

[0062] When a SmartCard 100 is inserted in Card Reader 208, a reset signal RST is sent from the card reader to both ISO CPU (START block 502) and Fingerprint CPU 114 (Fingerprint Verification block 504) and both receive power VCC from the Card Reader 208. ISO CPU then responds with ATR (Answer-to-Reset) message and communicates PPS (Protocol and Parameters Selection) as needed (block 506). At the same time, Fingerprint CPU goes into waiting state for receiving Fingerprint data and when data is received from sensor 110, performs the authentication process (block 504).

[0063] When an initial request command is sent by the Application 216 to ISO CPU 112 (block 508) the ISO CPU queries (block 510) Security CPU about the authentication status. If the response is positive, ISO CPU responds to the application by executing the requested command (block 512). Otherwise (either an error message or no response from Security CPU 114) it does not make any

response to the requested command but rather waits for a new first request (block 508b).

[0064] Assuming the Fingerprint was verified and the first response was received in a timely fashion and determined to be responsive by the Application 216 (block 514), the Request/Response process is continued (blocks 516, 518, 520) until a predetermined Verification Timeout has been exceeded during which no Requests were received from the Application (block 522), or the Application failed to receive an expected response (block 524).

[0065] Fig. 7 is similar to the flowchart of Fig. 6, but modified for use with the exemplary biometric verification card of Fig. 5. The far left hand side of Fig. 7 shows the functions performed by Application Server 202, the next column corresponds to Reader 208, the next column depicts ISO contacts 108, the next column shows functions performed by Security CPU 114, while the far right hand side shows the functions performed by an unmodified ISO SmartCard CPU 112.

:

- When either a SmartCard is inserted in a card reader or the application software starts operation of card reader device, a Reset Signal 550 is sent from Card Reader 208 to Security CPU 114.
- Soon after Security CPU receives Reset Signal 550, it sends a corresponding Reset Signal 552 to ISO CPU 112. Concurrently Security CPU awaits Fingerprint data from Fingerprint Sensor.
- Upon receipt of Reset Signal 552, ISO CPU makes an ATR (Answer-to-Reset) response 554 and thereafter communicates PPS (Protocol and Parameters Selection) as needed.
- As soon as Security CPU 114 receives ATR (Answer-to-Reset) from ISO CPU, it transfers it to Card Reader (block 556), including any associated PPS commands.
- In the meantime, if Security CPU receives fingerprint data, it executes the previously described authentication process. In the event the authentication test results in a PASS, the pass status is maintained for

specific time period. If the result is FAIL, Security CPU 114 awaits new fingerprint data.

- Upon the application execution, a command request 558 is sent to Security CPU, which transfers a command request 560 to ISO CPU and also transfers its correct response 562 to Card Reader only if the Security CPU is still in the previously mentioned PASS state or if the last correct response had More-data bit set (test block 564).
- Otherwise (No branch 566) Fingerprint CPU generates a dummy request 568 and transfers it to ISO CPU and also transfers the resultant ERR response 570 to Card Reader 216, thereby maintaining proper synchronization between the sequence numbers in the requests and responses.

Encryption and security

[0066] Prior to transmission over any external network, any sensitive data and/or the authentication result is preferably encrypted, possibly using DES, or Two Fish encryption. The encryption key can be based on captured or stored fingerprint data, user ID code, sensor's uniquely assigned code, memory address, adjacent data in memory, other functionally related data, a previous conversation (transaction), IP address, terminal code, or an assigned password. Alternatively, the sensitive data may be sent over the Internet using the secure HTTPS protocol.

[0067] To provide even greater security, a Virtual private gateway, such as hardware DES encryption and decryption, may be inserted between the secure Fingerprint Authentication Server and the network connection, and correspondingly between the Application Service Server and the network connection. By so using such a Virtual gateway or virtual Private Network ("VPN"), the sensitive data is additionally protected by an additional layer of encryption, for example both DES 128 (typically used in the VPN) and RSA (used by HTTPS).

[0068] For especially secure applications, all communications may wrapped with additional layers of security. In particular, message headers in a lower layer can be encrypted in an upper layer.

[0069]

Wireless Communication

[0070] Other embodiments may include a dual interface for both contact (ISO 7816) and wireless (ISO 1443 A or B) operation, and preferably incorporate a multi-interface power unit that allows interoperability among ISO 7816 contact, ISO 1443 A, ISO 1443 B, ISO 15693 and HID legacy wireless systems (among others) all on one card. Alternatively, the card may include provision for other wireless communications technologies such as Bluetooth (short range) or Cellular (medium range) or microwave (long range).

[0071] Reference should now be made to Fig. 8 which shows a smart card with on board biometric verification that can be connected to a local terminal either wireless or by means of an electrical connector. For the most part it is similar in construction and architecture to the previously described embodiment of Fig. 1, and like numbers (possibly distinguished by a single quotation mark) designate similar elements. In particular, ISO CPU 112 is shown in a different location (under rather than to one side of contacts 108), but has a similar functionality as previously described.

[0072] ISO antenna 132 comprises two loops generally located about the periphery of card 100 and provides an ISO-compatible wireless interface to ISO CPU 112 for both data and power similar to that afforded by the wired electrical interface 108. In addition, a Security antenna 134 (in the depicted example, inside antenna 132 and consisting of only one loop) provides a separate source of power to Security CPU 114 via a DC-DC power regulator 120. Because there is no direct connection for wireless data except through ISO CPU 112, the sensitive data stored within Security CPU 114 is not compromised by such a wireless interface. Alternatively, as mentioned previously with respect to the

embodiments having only wired connections to the external reader and external network, the functionality of the two processors could be combined, or the external interface could be through the Security CPU 114 rather than the ISO CPU 112, in which appropriate wireless security measures would have to be incorporated into the thus-modified architecture.

[0073] Fig. 9 is a cross section through the card of Fig. 8. Note that most of the described components are contained within a central core, 126, with only contact pads 108 extending through upper protective layer 122. The operative area of sensor 110 is accessible through an upper window in upper layer 122 and a lower window in PCB 134 that is disposed between upper layer 122 and central core 126 and which provides the required electrical connections between the various electronic components, as well as a surrounding electrostatic discharge ground contact surrounding the active region of sensor 110.

[0074] Also visible is a lower layer 124 and magnetic strip 128.

Fingerprint sensor

[0075] Fig. 10 is an exemplary schematic circuit diagram for sensor 110, in which an array 400 of sensor cells 402 is arranged in rows 404 and columns 406. As depicted, each cell 402 includes an activation gate 410 and a transducer 412. A Fingerprint is formed by the ridges and valleys of skin on a finger. Each sensor cell transducer 412 experiences a mechanical and/or electrical change when one of these ridges touches the immediate vicinity of cell 402 within array 400, which in effect provides a digital fingerprint image based on micro-pressure variations across the sensor surface caused by the ridges and valleys on the finger tip. Note that although each transducer 412 has been depicted as a single variable capacitor, there are various types of transducers that can respond to the presence of one of these ridges of human skin: In the particular example of a pressure sensitive piezo thin film transducer, the film is deformed in the vicinity the cell and generates a charge which is stored in a capacitor connected to that cell. The voltage on the capacitor is thus a function of the mechanical stress formed by the deformation of piezo material, which in turn is a function of

18

whether a mountain or a valley is above the cell. When a signal from the associated column driver 414 switches that cell's gate 410 ON and the associated row driver 416 is grounded, that voltage appears on the row's output line 418, and is converted to an 8-bit digital signal in Output driver 420. For maximizing detection of deformation of piezo material, the piezo electric material may formed on elastic material, such as polyimide or may simply be a polyimide piezo electric material. Other exemplary analog transducer technologies that can be implemented with a similar array organization include variable resistance and variable capacitance. Alternatively each cell could consist of a simple digital switch which provides only single bit of information; in that case, additional bits of information can be generated by providing more cells in the same area or by sampling each cell at a higher frequency. Such an alternate embodiment avoids the need for any A/D converters.

[0076] In an exemplary embodiment, the sensor is only 0.33 mm thin and is durable enough to be embedded in a SmartCard and is not effected by static electricity, the elements or the condition (wet, dry, hot, cold) of the user's skin. A typical unit cell size of Sensor 110 is 25 micron to 70 micron and a typical pitch is 25 micron to 70 micron. The exemplary sensor has a sensing area of 12.5 mm to 25 mm square and an 8-bit multi level of sensitivity. Such sensor can be manufactured by array of TFT (Thin Film Transistor) and Pressure sensitive capacitor, such as formed by Thin Film Piezo Material, such as Titanium Barium Oxide or Strontium Barium Oxide, and includes an upper electrode which covers and protects the entire sensing area. If mechanical stress is applied, a corresponding charge is generated and stored in the Thin Film Piezo Capacitor. Alternatively, a pressure-based sensor can be manufactured as an array of TFT (Thin Film Transistor) along with thin film capacitor, and Pressure sensitive capacitor, such as formed by sheet of pressure conductive material, such as carbon fiber dispersed rubber sheet, metal (such as Copper or Tin or silver), plated carbon fiber or glass fiber based paper, or metal, dispersed elastic material (such as silicone), and an upper electrode sheet, which covers entire sensing area.

[0077] Row and Column drivers 416, 414 which particular specified fingerprint sensor element 402 is outputting the electrical data to the Output circuitry 420 thereby converting the physical input representative of the user's fingerprint to analog electrical data. An A/D converter in the Output circuitry 420 then convert the analog electrical signal to digital electrical signal. Each thin film transistor selectively switches a shared row interconnection to the voltage on its associated capacitor, thus the voltage on each capacitor can be read and thereby each cell's deformation can be measured. An entire column of Thin film transistors is preferably switched simultaneously, and thus a number of cells (for example 8) in one selected column can be read in parallel on different row interconnections. The interconnection of multiple gates as rows and columns reduces the number of interconnections, while the parallel read out of multiple cells from different rows of the same column reduces the read time for the entire array. The output voltage from the sensor can be amplified by a differential amplifier. The output of such amplifier can be sampled and held for Analog to Digital Conversion (A/D converter).

[0078] Substrate can be glass (such as non alkaline glass), stainless steel, Aluminum, Ceramics (such as Aluminum Oxide), Paper, Glass Epoxy, but is preferably a thin sheet of Crystal Silicon. Thin film semiconductor material can be Amorphous Silicon, Polysilicon, Diamond, or any other Semiconductor Thin Film. Piezoelectric Material can be a piezoelectric ceramic, such as lead-zirconate-titanate (PZT) thin films, preferably ranging in thickness from 0.1 to 50.0 microns, or a polymer piezoelectric polyimide thin-film material. Interconnection Material may be: Ti/Ni/Cu, Al, Cr/Ni/Au, Ti/Ni/Au, Al/Au, W/Cu, W/Au, W/Au.

[0079] Fig. 11 shows a carrier assembly for a sensor formed on a thin substrate of crystalline silicon. Crystalline silicon has excellent electrical properties and facilitates integration of the sensor array with the required driver and output circuits, however a relatively large and thin sheet of silicone will flex and fracture when subject to localized surface pressure. The illustrated carrier provides a

much stiffer structure than would be provided with a sheet of silicon of the same overall thickness.

[0080] As shown, the monolithic sheet of silicon 430 is about 0.1 mm in thickness, and is surrounded by an equally thick frame 432 of glass epoxy, which is mounted on a backing plate 434 also of glass epoxy construction and about 0.05 mm in thickness. Frame 432 and backing plate 434 may be readily constructed using conventional printed circuit board (PCB) technology. In particular, the upper and lower surfaces of backing plate 434 are covered with a thin copper layer 436 separated by a glass epoxy core. Frame 432 includes a number of solder pads 440 about its outer periphery, for connection to Security Processor 114. The thin silicon chip 430 is epoxy bonded to frame 432 and plate 434, and the active regions are electrically coupled to respective electrical traces in the frame 430 by conventional wire bonding 442 at the exposed outer edge portions 444 of the silicon 430 surrounding the protective upper electrode 446.

Matching algorithms

[0081] For local on-board processing where processing power is limited and only a simple 1:1 match with a single reference sample is being attempted, the fingerprint-matching software can be based on a relatively straightforward comparison of Minutiae derived from the two patterns. For example, the gray-scale image of a fingerprint is may be reduced to two values, white and black, and 3 dimensional ridges are converted into two dimensional thin lines (vectors). The accuracy of the method is therefore subject to, among other problems, blurring, conglutination, distortion, partial lacking of line segments and other effects. Although the Minutiae method is in principle less accurate, it requires fewer computational resources and offers the possibility of compatibility with many existing databases.

[0082] For processing at a remote Authentication server where more processing power is available and more accurate discrimination may be required, for example a "POC" (Phase Only Correlation) matching algorithm. POC is an identification algorithm based on macroscopic matching of whole images. POC,

conversely, matches structural information across a wide range – from details to the total image. Hence, POC is able to provide robust accuracy against noises such as conglutination and partial hiatus. In principle, the POC method is free from the adverse effects of positional shift and differences in brightness, is fast (about 0.1 seconds for an offline match) and is highly accurate. For example, the POC software may perform a space frequency comparison of the two fingerprint patterns utilizing a two dimensional First Fourier Transform ("2DFFT"). 2DFFT converts an array of digitized data representing a physical two dimensional distribution of fingerprint, into frequency space, in other words, reverse space distribution, where higher density pattern has higher space frequency. A rotational transformation may be used to match the frequency space pattern matching. POC pattern matching has the further advantage Minutiae vector matching, because is not misled by common defects in the recorded fingerprint pattern which POC would recognize as noise but a Minutiae analysis would interpret as meaningful data.

[0083] For particularly demanding applications, a hybrid approach may offer even greater accuracy and security than either method alone. For example, a minutiae methodology can be used at the point of capture, while a POC methodology can be used at a remote server. As another example, the matching process can analyze both the minutiae and the spatial relationships to produce a combined score that takes into account the results of both.

Applications

[0084] The above-described technology provides a high level of security for multiple applications, both commercial and governmental. Depending on the requirements of each application, multiple secure applications may co-exist and operate on the same card and/or on the same authentication server. In one embodiment, a single card can contain up to 24 independent and secure applications. For example, the technology will permit/deny access (physical and/or logical), identify precise location and/or movement of personnel and/or

watch list parties while at the same time operating other secure applications, each completely and securely isolated one from the other.

[0085] Among the applications currently contemplated are the following:

- Airport ID/Access
- Building Security
- Hotel Room Access and Billing
- Hospital
- On line Gaming
- Downloaded entertainment
- Birth Certificate
- Computer Access
- Driver's License – TWIC
- Electronic Wallet
- Emergency Medical Information
- Explosives License
- Government & Military Facility Access
- HAZMAT License
- Medicare & Benefits Card
- Parking Access
- Passport
- Pilot's License
- Port ID/Access
- Proof of Insurance
- Social Security Card
- Trusted Traveler Card
- Visa or Entry/Exit pass
- Voter Registration Card
- Welfare & Food Stamp Card

[0086] For many of these applications, the card's on-board memory preferably also provides secure storage of various kinds of private personal information,

which is accessible only when the registered cardholder has proven his identity and authorized such access. Examples of such private information are:

- Administrative Information such as name, address, birth date, place of birth, nationality, religion, organizational memberships, social security number, drivers license number, passport number, and immigration information such as visa type, visa expiration, citizenship etc.
- Financial information, such as electrical wallet, Visa, MasterCard, American Express, etc. credit card information, bank information such as name of bank, balance of bank, money transfer information, IRS number, bankruptcy record, money transfer information etc.
- Physiological or health information such as: biometrics information to identify individuals such as height, weight, fingerprint, iris, retina, hand size, bone structure, voice, DNA; blood type; medical diagnostic test results; medical history; medications; insurance information; psychological and physiological responses to certain stimuli, etc.
- Event Information such as criminal record, felony, misdemeanor, infractions.
- Emergency information such as cemetery, relative and other contact information, lawyer information, religious information.
- Education, work history, including school to attend, degree, company worked related to FDD.
- Data access history (stores the data of access history in and out of card).
- ID related information such as fingerprint pattern, processed fingerprint pattern, results of fingerprint pattern.
- Passwords such as a permanent password, a temporary password, and/or a one time pass word.
- Encryption keys such as a public key, a personnel key, and/or a one time key.

[0087] An exemplary card enrollment system will now be described

[0088] The applicant: fills out an application and submits it, preferably including a photograph and fingerprint. For most applicants, an inspection of their breeder documents and an simple crosscheck of the submitted information against one or more available government and commercial databases should be sufficient to establish the individual's true identity.

[0089] After his identity has been so verified, the applicant proceeds to an issuing station where any information deemed necessary by the card issuer is loaded onto the card. The applicant puts their fingerprint on the sensor on the card. Once the fingerprint is satisfactorily placed on the sensor and loaded onto the card, the tab on the card then gets a jolt of electricity which burns out certain fuses that prevent anyone from writing to that certain area of the card ever again. Then, the little tab gets cut/guillotined off (like an umbilical cord). At that point, the card can only be read or written to through the ISO contact reader or ISO wireless system.

[0090] In the case of a networked Authentication server, some or all of the same data that is loaded onto the card is also transmitted in encrypted form to the remote server, possibly supplemented with additional data that is not normally stored on the card but that may be required for certain high security applications.

CLAIMS

1. An intelligent identification card comprising:
an on-board memory for storing reference data,
an on-board sensor for capturing live biometric data,
an on-board microprocessor for comparing the captured biometric data with
corresponding stored reference data within a predetermined threshold and
for generating a verification message only if there is a match within a
predetermined threshold, and
means for communicating the verification message to an external network.
2. The identification card of claim 1 wherein the verification message
includes at least excerpts from the stored reference data.
3. The identification card of claim 2 wherein the verification message
includes at least excerpts from the captured biometric data.
4. The identification card of claim 3 wherein the verification message is
transmitted to a remote authentication system for additional verification.
5. The identification card of claim 4 wherein the remote authentication
system includes remotely stored reference data that is different from the locally
stored reference data.
6. The identification card of claim 4 wherein the on-board microprocessor
uses a different matching algorithm than that used at the remote authentication
system.
7. The identification card of claim 2 wherein the entire matching process is
performed by the on-board processor and none of the captured biometric data is
transmitted to the network.
8. The identification card of claim 2 wherein both the originally captured
biometric data and any other "private" information stored in the on-board memory
are not made available to any external processes.

9. The identification card of claim 2 wherein the card is ISO SmartCard compatible.
10. The identification card of claim 9 further comprising an ISO SmartCard processor.
11. The identification card of claim 10 wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO SmartCard processor by a firewall.
12. The identification card of claim 10 wherein all external data to and from the security processor passes through the ISO SmartCard processor.
13. The identification card of claim 10 wherein all external data to and from the ISO SmartCard processor passes through the security processor.
14. The identification card of claim 10 wherein the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network.
15. The identification card of claim wherein the first connection is permanently disabled after the loading process has been completed.
16. The identification card of claim 10 wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO SmartCard processor by a firewall.
17. The identification card of claim 10 wherein:
the card comprises an upper magnetic stripe region and a lower embossed region;
the biometric sensor is a fingerprint sensor; and
the security processor, the ISO SmartCard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region.
18. The identification card of claim 2 wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor.

19. The identification card of claim 18 wherein real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor.
20. The identification card of claim 18 wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data.
21. The identification card of claim 18 wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate.
22. The identification card of claim 21 wherein the backing plate comprises a glass epoxy layer sandwiched between two metal layers.
23. The identification card of claim 18 wherein the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.
24. The identification card of claim 1 wherein the card further comprises means for restricting use of the card to a predetermined location. at least some of the captured
25. The identification card of claim 1 wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity prior to any grant of on-line access to an application server for processing of secure financial transactions involving that user.
26. The identification card of claim 25 wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

27. The identification card of claim 1 wherein the output from the card is used to obtain physical access into a secure area.

28. The identification card of claim 27 wherein a record of successful and unsuccessful access attempts is maintained on the card.

[Handwritten signature]

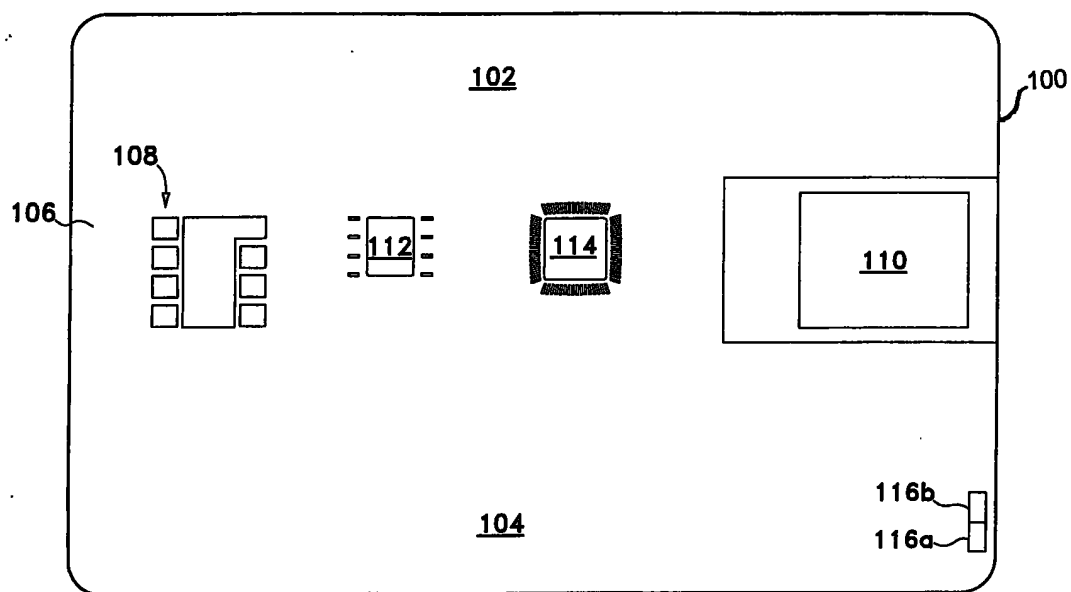
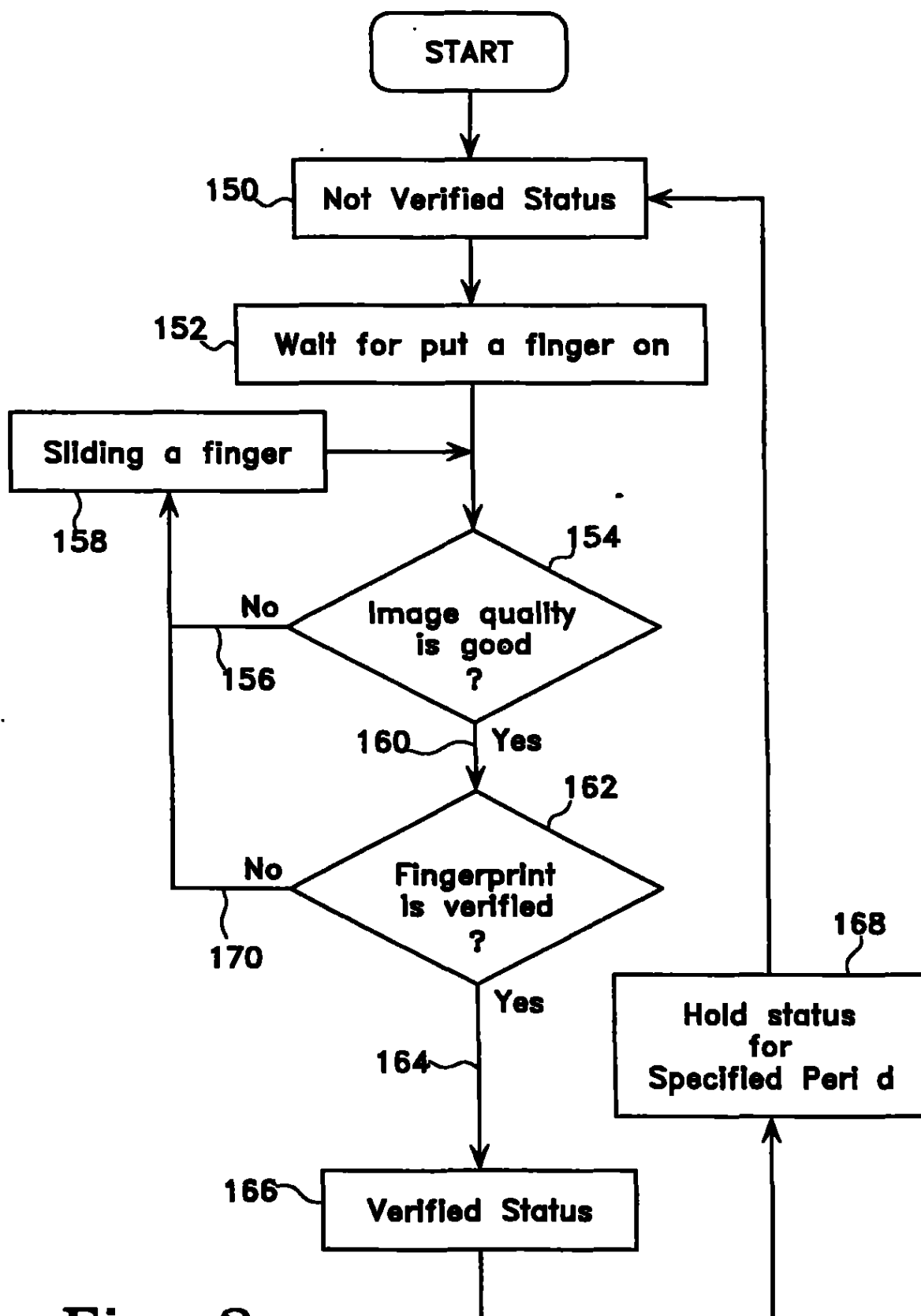


Fig. 1

**Fig. 2**

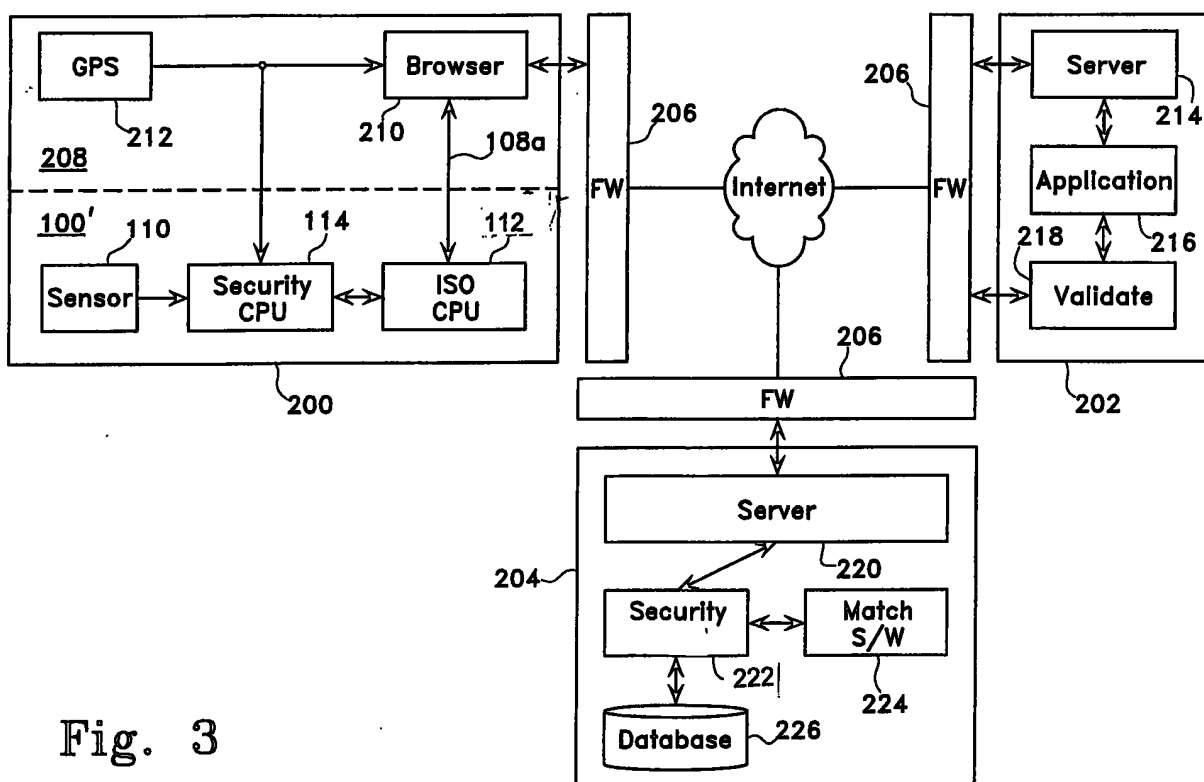


Fig. 3

[Handwritten signature]

[Handwritten signature]

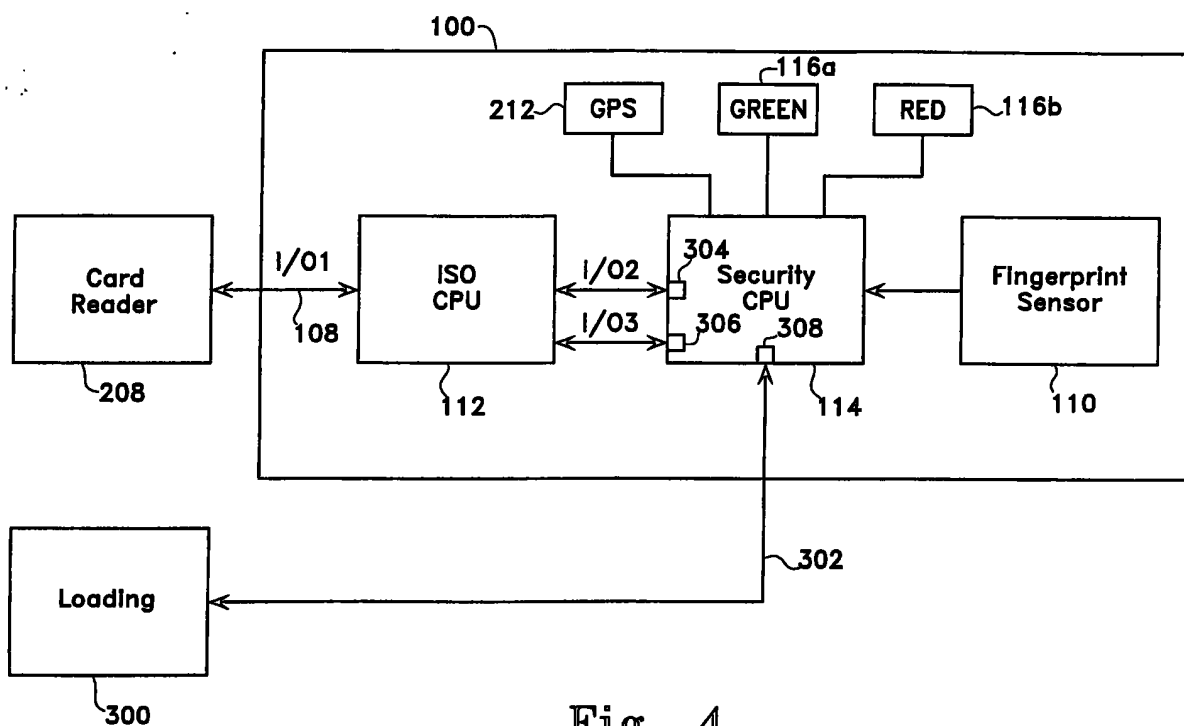


Fig. 4

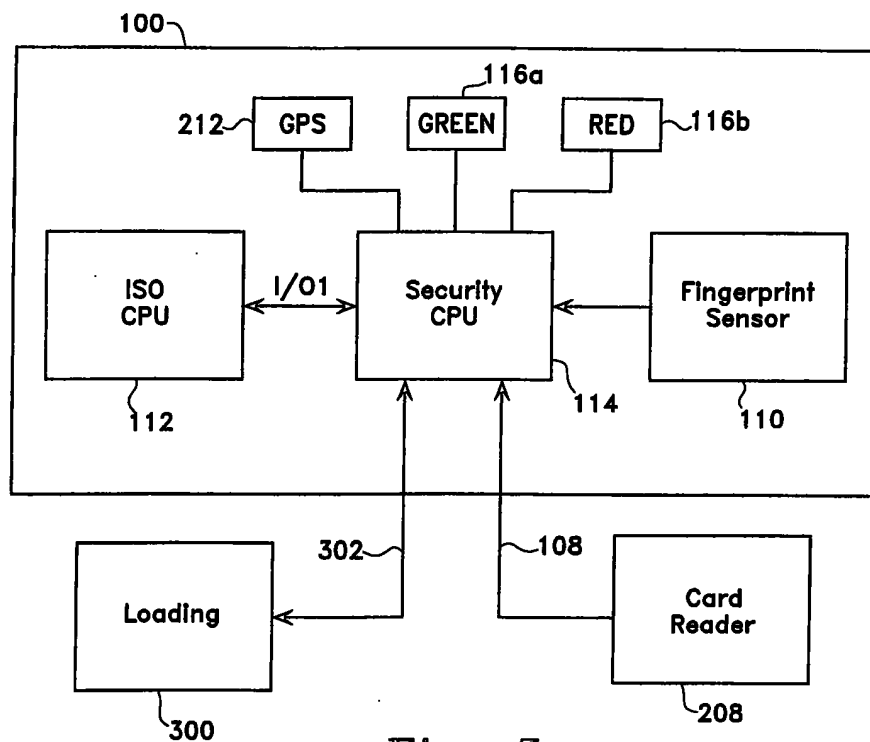


Fig. 5

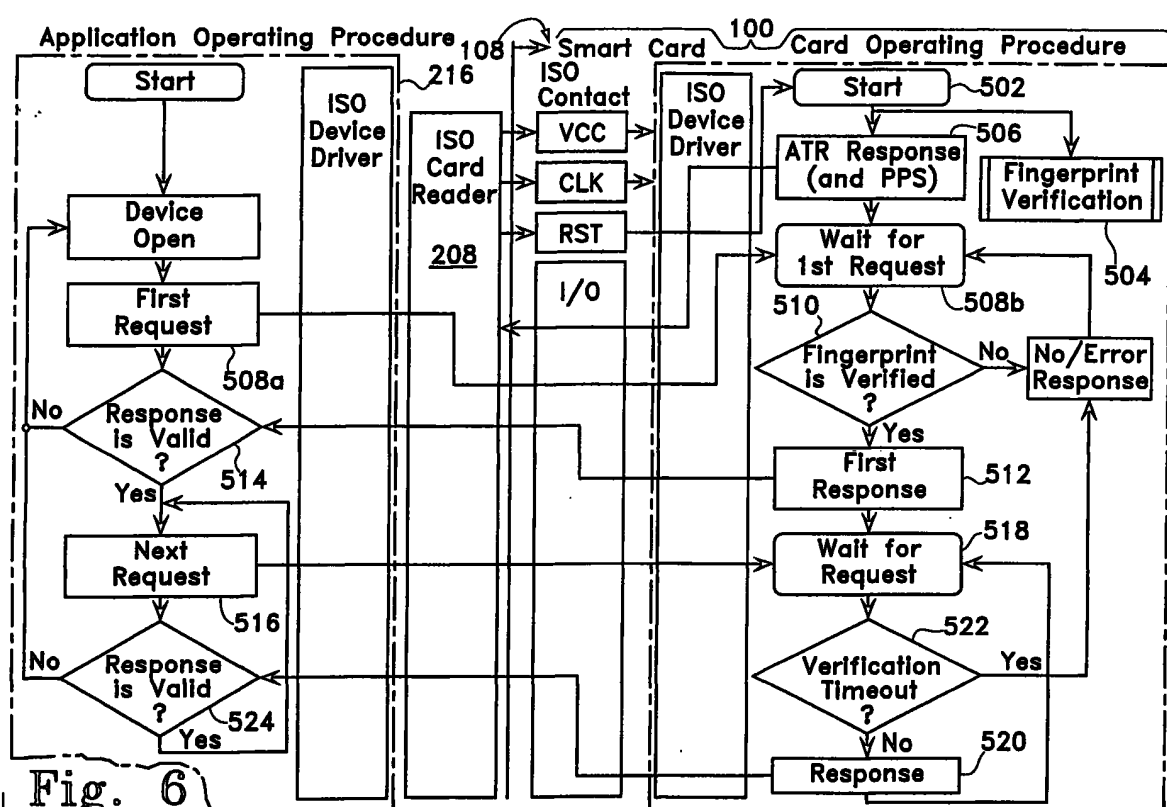
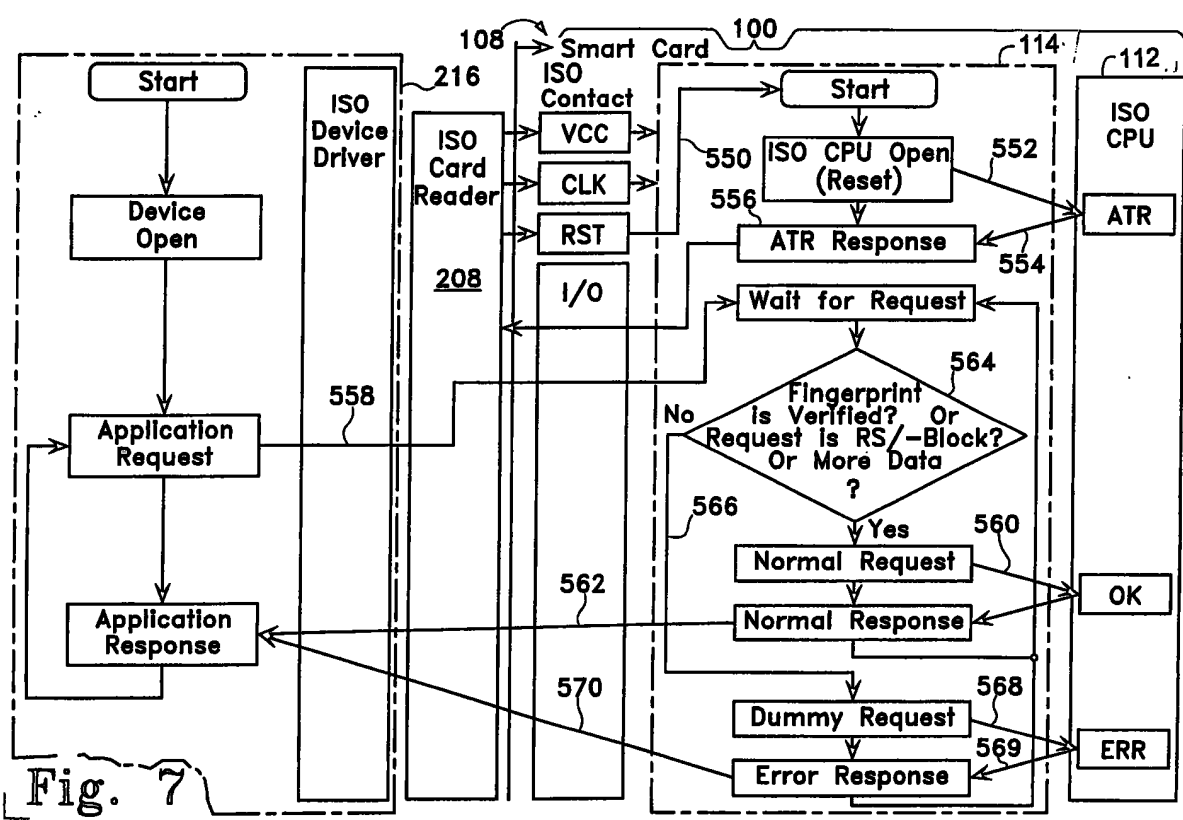


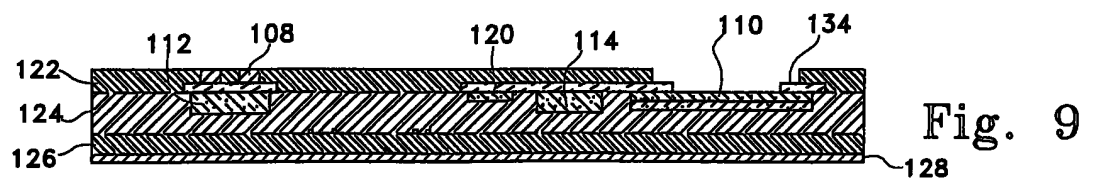
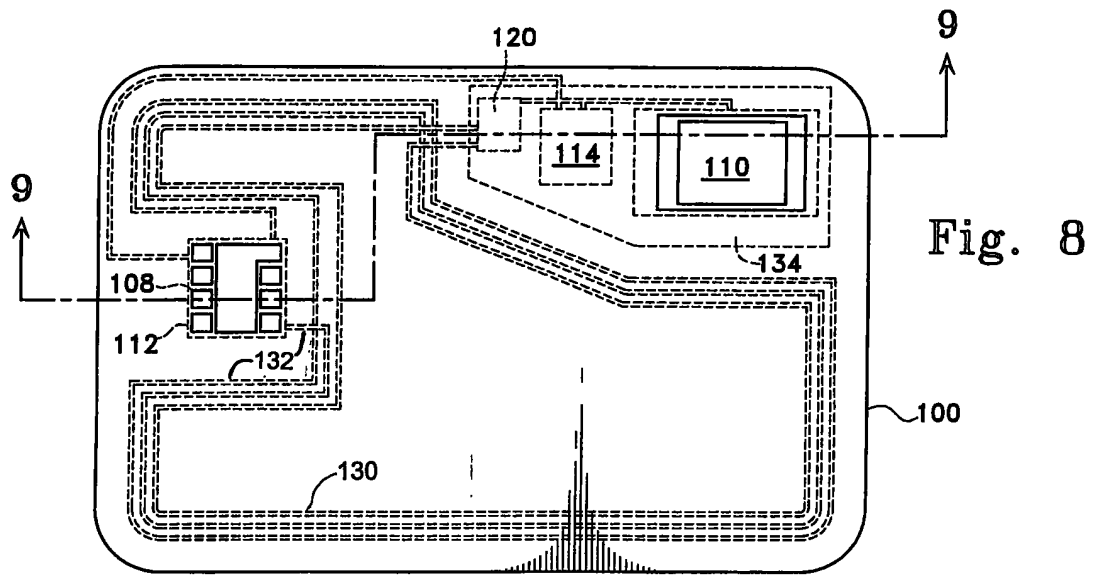
Fig. 6

29

SP



[Handwritten mark]



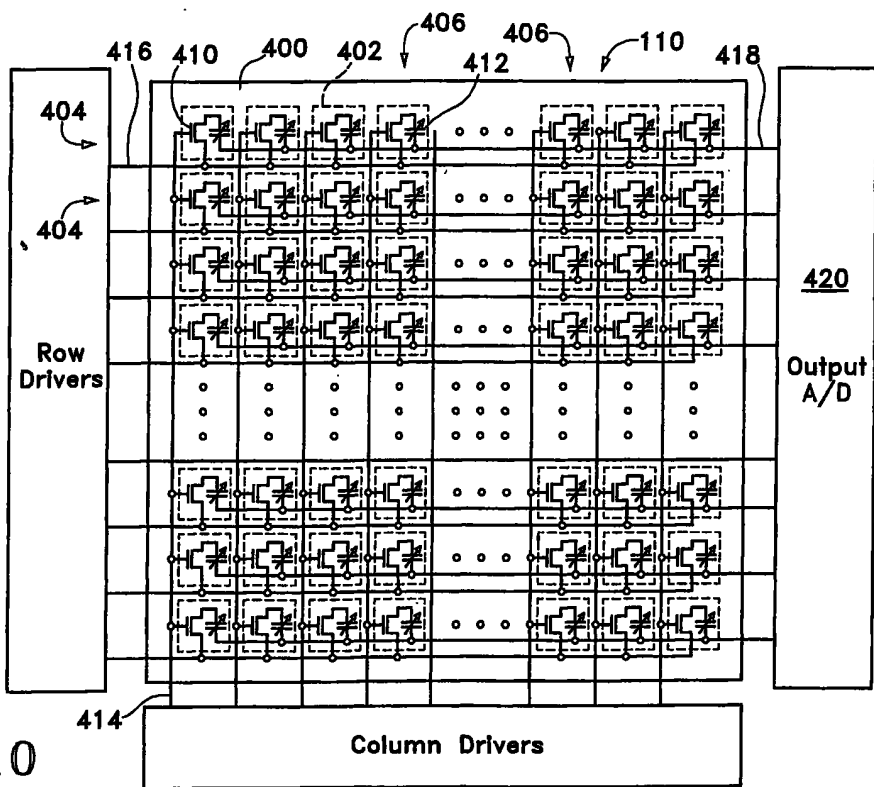


Fig. 10

88

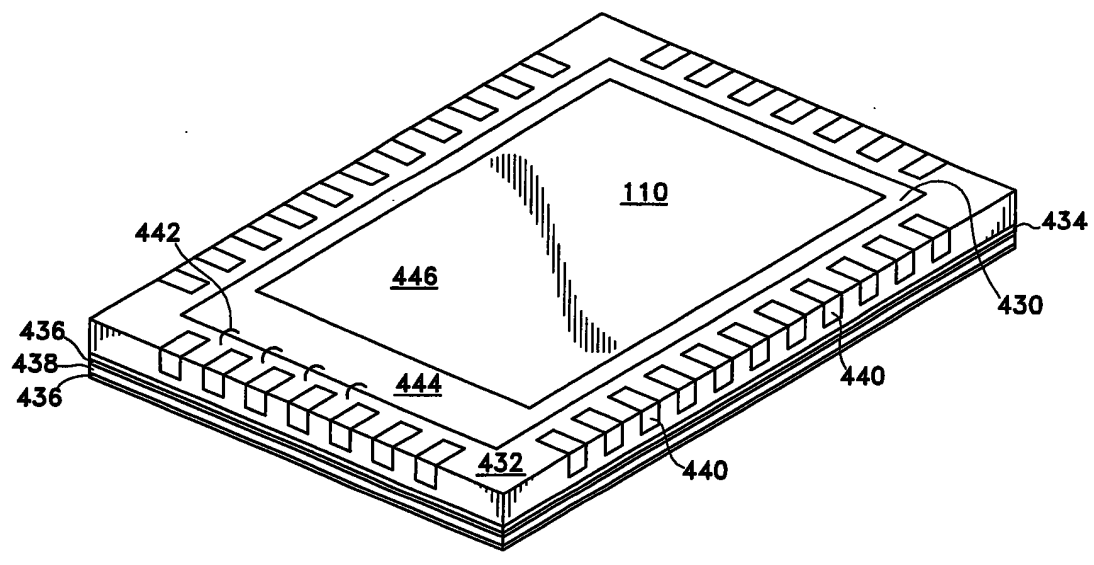


Fig. 11

INTERNATIONAL SEARCH REPORT

Application No
PCT/US 03/28602A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/077 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 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, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 074 949 A (SHEN MING SHIANG) 7 February 2001 (2001-02-07)	1,2,7,9, 10,18, 27,28
Y	column 3, line 9 - line 36; figure 1	3,19-21
Y	WO 01/18740 A (ULTRA SCAN CORP) 15 March 2001 (2001-03-15) page 6, paragraph 2 - page 7, paragraph 1	19
Y	US 5 907 627 A (BORZA STEPHEN J) 25 May 1999 (1999-05-25) column 6, line 14 - line 15; figure 4	21
Y	EP 0 457 398 A (PHILIPS ELECTRONICS UK LTD ; PHILIPS NV (NL)) 21 November 1991 (1991-11-21) column 5, line 31 - line 47	20
	-/--	

☒ 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 contact 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.

"B" document member of the same patent family

Date of the actual completion of the international search

3 May 2004

Date of mailing of the international search report

07 05 2004

Name and mailing address of the ISA

European Patent Office, P.B. 5519 Patentplan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Chiarizia, S

INTERNATIONAL SEARCH REPORT

Int'l Application No
PL 1/US 03/28602

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 006 479 A (STOCKO CONTACT GMBH & CO KG) 7 June 2000 (2000-06-07) claims 1,13	1,8 3
X	US 6 325 285 B1 (BARATELLI PAUL J) 4 December 2001 (2001-12-04) abstract; claim 1; figure 1	1,8
X	US 5 995 630 A (BORZA MICHAEL ANDREW) 30 November 1999 (1999-11-30) column 10, line 66 - column 11, line 11; figure 7	1,8 2
A	US 2002/088632 A1 (WEBER PATRICK O ET AL) 11 July 2002 (2002-07-11) abstract; figure 1	23
A	US 5 978 495 A (THOMOPOULOS STELIOS C A ET AL) 2 November 1999 (1999-11-02) column 12, line 20 - line 37	20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/28602

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 4, 5, 6, 25, 26
because they relate to subject matter not required to be searched by this Authority, namely:
Claims 4-6, 25, 26 depend on claim 1 which relates to an identification card. Therefore they can not include features (a remote system) that do not belong to the card. Since the search is defined by the device of claim 1 (an identification card), features that do not belong to said device have not been
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

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

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.1

Claims 4-6,25,26 depend on claim 1 which relates to an identification card. Therefore they can not include features (a remote system) that do not belong to the card. Since the search is defined by the device of claim 1 (an identification card), features that do not belong to said device have not been searched.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-18,24-28

Intelligent identification card comprising a biometric sensor, a ISO smart card processor and a security processor for storing and processing the biometric data, said processors being separated by a firewall.

2. claims: 1,2,18-23

Intelligent identification card comprising a fingerprint sensor and means for facilitating an optimal placement of the finger over the sensor.

INTERNATIONAL SEARCH REPORT

Int Application No
PCT/US 03/28602

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1074949	A	07-02-2001	AU 729157 B1 EP 1074949 A1 AT 242521 T DE 69908579 D1 DE 69908579 T2	25-01-2001 07-02-2001 15-06-2003 10-07-2003 29-04-2004
WO 0118740	A	15-03-2001	AU 7127900 A WO 0118740 A1	10-04-2001 15-03-2001
US 5907627	A	25-05-1999	AU 7273796 A CA 2233520 A1 WO 9717668 A1 DE 69618478 D1 DE 69618478 T2 EP 0859991 A1 JP 2000513839 T NO 982053 A	29-05-1997 15-05-1997 15-05-1997 14-02-2002 12-12-2002 26-08-1998 17-10-2000 03-07-1998
EP 0457398	A	21-11-1991	GB 2244164 A DE 69115558 D1 DE 69115558 T2 EP 0457398 A2 JP 3007714 B2 JP 4231803 A US 5325442 A	20-11-1991 01-02-1996 01-08-1996 21-11-1991 07-02-2000 20-08-1992 28-06-1994
EP 1006479	A	07-06-2000	DE 29821644 U1 EP 1006479 A2 JP 2000215296 A US 6592031 B1	18-02-1999 07-06-2000 04-08-2000 15-07-2003
US 6325285	B1	04-12-2001	NONE	
US 5995630	A	30-11-1999	WO 9838567 A1 EP 1012689 A1 CA 2198993 A1	03-09-1998 28-06-2000 07-09-1997
US 2002088632	A1	11-07-2002	AU 8340001 A AU 8496201 A EP 1352425 A2 EP 1352426 A2 WO 0215209 A2 WO 0215267 A2 US 2002081780 A1	25-02-2002 25-02-2002 15-10-2003 15-10-2003 21-02-2002 21-02-2002 27-06-2002
US 5978495	A	02-11-1999	NONE	

PATENT COOPERATION TREATY

mgl/gmm
32

From the INTERNATIONAL BUREAU

PCT

To:

MAY, John, M.
Fulbright & Jaworski L.L.P.
29th floor
885 South Figueroa
Los Angeles, CA 90017-2571
United States of America

RECEIVED

DEC 3 2003

FULBRIGHT & JAWORSKI

NOTIFICATION OF RECEIPT OF
RECORD COPY

PCT Rule 24.2(a))

Date of mailing (day/month/year)

20 November 2003 (20.11.03)

IMPORTANT NOTIFICATION

Applicant's or agent's file reference

PCT/US03/28602

International application No.

PCT/US03/28602

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

IVI SMART TECHNOLOGIES, INC. (for all designated States except US)

SAITO, Tamio et al (for US)

International filing date

: 10 September 2003 (10.09.03)

Priority date(s) claimed

: 10 September 2002 (10.09.02)

10 September 2002 (10.09.02)

27 November 2002 (27.11.02)

13 December 2002 (13.12.02)

03 July 2003 (03.07.03)

Date of receipt of the record copy
by the International Bureau

: 14 November 2003 (14.11.03)

List of designated Offices

:

AP : GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW

EA : AM, AZ, BY, KG, KZ, MD, RU, TJ, TM

EP : AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR

OA : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG

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, 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, 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

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

Facsimile No. (41-22) 338.87.20

Authorized officer:

Pascal Piriou (Fax 338-87-20)

Telephone No. (41-22) 338 8198

Continuation of Form PCT/IB/301

38

NOTIFICATION OF RECEIPT OF RECORD COPY

Date of mailing (day/month/year) 20 November 2003 (20.11.03)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference LA-7167-102.PC	International application No. PCT/US03/28602

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the International application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase - see updated Important Information (as of April 2002)
- ☐ confirmation of precautionary designations (if applicable)
- ☐ requirements regarding priority documents (if applicable)

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated on the cover sheet of this Notification by paying national fees and furnishing translations, as prescribed by Articles 22 and 39 and the applicable national laws. In addition, the applicant may also have to comply with other special requirements applicable in certain Offices. It is the applicant's responsibility to ensure the necessary steps to enter the national phase are taken in a timely fashion. Most Offices do not issue reminders to applicants in connection with the entry into the national phase.

The applicable time limit for entering the national phase will, subject to what is said in the following paragraph, be 30 MONTHS from the priority date, not only in respect of any elected Office where a demand for international preliminary examination is filed before the expiration of 18 months from the priority date (see Article 39(1)), but also in respect of any designated Office, in the absence of filing of such demand, where Article 22(1) as modified with effect from 1 April 2002 applies in respect of that designated Office. For further details, see PCT Gazette No. 44/2001 of 1 November 2001, pages 19928, 19932 and 19934, as well as the PCT Newsletter, October and November 2001 and February 2002 issues.

In practice, time limits other than the 30-month time limit will continue to apply, for various periods of time, in respect of certain designated or elected Offices. For regular updates on the applicable time limits (20, 21, 30 or 31 months, or other time limit), Office by Office, refer to the PCT Gazette ("Section IV" part published on a weekly basis), to the PCT Newsletter (on a monthly basis) and to the relevant National Chapters in Volume II of the PCT Applicant's Guide (the paper version of which is updated usually twice a year and the Internet version of which is updated usually on a weekly basis). Finally, a cumulative table of all applicable time limits for entering the national phase is available from WIPO's Internet site, via links from various pages the site including those of the Gazette, Newsletter and Guide, at <http://www.wipo.int/pct/en/index.html>.

Information about the requirements for filing a demand for international preliminary examination is set out in the PCT Applicant's Guide, Volume I/A, Chapter IX. Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination (at present, all PCT Contracting States are bound by Chapter II).

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date (this time limit may not be extended). If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. The Notice of confirmation and payment must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 18 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 18-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 18-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided 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 the time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 18-month time limit is the filing date of the earliest application whose priority is claimed.

PATENT COOPERATION TREATY

mjc/omm
70

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

MAY, John, M.
Fulbright & Jaworski L.L.P.
29th floor
885 South Figueroa
Los Angeles, CA 90017-2571
United States of America

Date of mailing (day/month/year) 20 November 2003 (20.11.03)	
Applicant's or agent's file reference LA-7167-102.PC	IMPORTANT NOTIFICATION
International application No. PCT/US03/28602	International filing date (day/month/year) 10 September 2003 (10.09.03)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 10 September 2002 (10.09.02)
Applicant IVI SMART TECHNOLOGIES, INC. et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
3. 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). In such a case, 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.
4. The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, 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.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
10 Sept 2002 (10.09.02)	60/409,716	US	06 Nove 2003 (06.11.03)
10 Sept 2002 (10.09.02)	60/409,715	US	06 Nove 2003 (06.11.03)
27 Nove 2002 (27.11.02)	60/429,919	US	06 Nove 2003 (06.11.03)
13 Dec 2002 (13.12.02)	60/433,254	US	06 Nove 2003 (06.11.03)
03 July 2003 (03.07.03)	60/484,692	US	06 Nove 2003 (06.11.03)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Pascal Piriou (Fax 338-87-20)
Facsimile No. (41-22) 338.87.20	Telephone No. (41-22) 338 8188

PATENT COOPERATION TREATY

41

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
JOHN M. MAY
FULBRIGHT & JAWORSKI LLP
865 SOUTH FIGUEROA
TWENTY-NINTH FLOOR
LOS ANGELES, CA 90017-2571

PCT

WRITTEN OPINION

(PCT Rule 66)

Applicant's or agent's file reference LA-7167-102.PC		Date of Mailing (day/month/year) 06 DEC 2004
International application No. PCT/US03/28602		REPLY DUE within 2 months/days from the above date of mailing
International filing date (day/month/year) 10 September 2003 (10.09.2003)	Priority date (day/month/year) 10 September 2002 (10.09.2002)	
International Patent Classification (IPC) or both national classification and IPC IPC(7): G06F 11/30 and US Cl.: 713/202		
Applicant IVI SMART TECHNOLOGIES, INC.		Fulbright & Jaworski LLP IPT Docketing Docketed ☒ Not required ☐ Previously ☐ Confirmation ☐

1. This written opinion is the first (first, etc.) drawn by this International Preliminary Examining Authority.
2. This opinion contains indications relating to the following items:

- | | | | |
|------|-------------------------------------|---|--|
| I | ☒ | Basis of the opinion | |
| II | ☐ | Priority | |
| III | ☐ | Non-establishment of opinion with regard to novelty, inventive step and industrial applicability | |
| IV | ☐ | Lack of unity of invention | |
| V | ☒ | Reasoned statement under Rule 66.2 (a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement | |
| VI | ☐ | Certain documents cited | |
| VII | ☒ | Certain defects in the international application | |
| VIII | ☒ | Certain observations on the international application | |

3. The applicant is hereby invited to reply to this opinion.

When? See the time limit indicated above. ~~The applicant may, before the expiration of that time limit, request this Authority to grant an extension. See rule 66.2(d).~~

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also For an additional opportunity to submit amendments, see Rule 66.4.
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis.
For an informal communication with the examiner, see Rule 66.6

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 10 January 2005 (10.01.2005)

Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer <i>Ayaz Sheikh</i> Ayaz Sheikh Telephone No. 571-272-2100
---	---

Form PCT/IPEA/408 (cover sheet)(July 1998)

Received **DEC 08 2004**
 Attorney **MSC/Jmm**
 Docket No **7167-102.W.**
 Action Req'd **BWO**
Consolidated
 Date Due **10 Jan 05**
 Initials **CS** Cross-check **CS**

WRITTEN OPINION

International app. No. 42
PCT/US03/28602

I. Basis of the opinion

1. With regard to the elements of the international application:*

- ☒ the international application as originally filed
- ☒ the description:
pages 1-31 _____, as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☒ the claims:
pages 32-35 _____, as originally filed
pages NONE _____, as amended (together with any statement) under Article 19
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☒ the drawings:
pages 1-10 _____, as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☐ the sequence listing part of the description:
pages NONE _____, as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item. These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the written opinion was drawn on the basis of the sequence listing:

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages NONE _____
- ☐ the claims, Nos. NONE _____
- ☐ the drawings, sheets/fig NONE _____

5. ☐ This opinion has been drawn as if (some of) the amendments 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)).

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed."

Y3

WRITTEN OPINION

International application No.
PCT/US03/28602

V. Reasoned statement under Rule 66.2(a)(II) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims <u>9-17, 21-23 and 26</u>	YES
	Claims <u>1-8, 18-20, 24, 25, 27 and 28</u>	NO
Inventive Step (IS)	Claims <u>NONE</u>	YES
	Claims <u>1-28</u>	NO
Industrial Applicability (IA)	Claims <u>1-28</u>	YES
	Claims <u>NONE</u>	NO

2. CITATIONS AND EXPLANATIONS
Please See Continuation Sheet

WRITTEN OPINION

International application No.

PCT/US03/28602

4x

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 11 and 16 are objected to under PCT Rule 66.2(a)(iii) as containing the following defect(s) in the form or contents thereof: both claims depend directly from claim 10 and consist of the same content.

WRITTEN OPINION

International application No.

PCT/US03/28602

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

Claims 15 and 24 are objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claims 15 and 24 are indefinite for the following reason(s): claim 15 is missing the dependent claim number, for examination purposes, the examiner treats claim 15 as being dependent upon claim 14; claim 24 misplaced "at least some of the captured" at the end of the claim, it should be "...means for restricting at least some of the captured use of the card...".

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

TIME LIMIT:

The time limit set for response to a Written Opinion may not be extended. 37 CFR 1.484(d). Any response received after the expiration of the time limit set in the Written Opinion will not be considered in preparing the International Preliminary Examination Report.

V. 2. Citations and Explanations:

Claims 1-8, 18-20, 24, 25, 27, and 28 lack novelty under PCT Article 33(2) as being anticipated by Shen (E.P. 1,074,949 A1).

Regarding claim 1, Shen teaches an intelligent identification card comprising:

- An on-board memory for storing reference data (figure 1, reference number 11),
- An on-board sensor for capturing live biometric data (figure 1, reference number 12),
- An on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold (figure 1, reference number 14), and
- Means for communicating the verification message to an external network (figure 1, reference number 13).

Regarding claim 2, Shen teaches wherein the verification message includes at least excerpts from the stored reference data (column 3, lines 31-36).

Regarding claim 3, Shen teaches wherein the verification message includes at least excerpts from the captured biometric data (column 3, lines 31-36).

Regarding claim 4, Shen teaches wherein the verification message is transmitted to a remote authentication system for additional verification (column 3, lines 31-36).

Regarding claim 5, Shen teaches wherein the remote authentication system includes remotely stored reference data that is different from the locally stored reference data (column 3, lines 28-31).

Regarding claim 6, Shen teaches wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system (column 4, lines 3-8).

Regarding claim 7, Shen teaches wherein the entire matching process is performed by the on-board processor and none of the captured biometric data is transmitted to the network (column 3, lines 31-36).

Regarding claim 8, Shen teaches wherein both the originally captured biometric data and any other "private" information stored in the on-board memory are not made available to any external processes (column 3, lines 25-31).

87

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Regarding claim 18, Shen teaches wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor (column 3, lines 9-11).

Regarding claim 19, Shen teaches wherein real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor (column 4, lines 18-23).

Regarding claim 20, Shen teaches wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data (column 3, lines 42-57).

Regarding claim 24, Shen teaches wherein the card further comprises means for restricting at least some of the captured use of the card to a predetermined location (column 1, lines 6-14).

Regarding claim 25, Shen teaches wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity prior to any grant of on-line access to an application server for processing of secure financial transactions involving that user (column 3, lines 28-36).

Regarding claim 27, Shen teaches wherein the output from the card is used to obtain physical access into a secure area (column 1, lines 9-12).

Regarding claim 28, Shen teaches wherein a record of successful and unsuccessful access attempts is maintained on the card (column 4, lines 8-17).

Claims 9, 10, 14, 15, 17, 21-23, and 28 lack an inventive step under PCT Article 33(3) as being obvious over Shen (E.P. 1,074,949) in view of DiGiorgio et al. (U.S. 6,385,729).

Regarding claims 9, 10, and 17, Shen teaches wherein the biometric sensor is a fingerprint sensor (column 3, lines 9-12); and the security processor, the ISO Smartcard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region (figure 1). However, Shen does not disclose wherein the card is ISO Smartcard compatible; further comprising an ISO Smartcard processor; and wherein the card comprises an upper magnetic stripe region and a lower embossed region.

DiGiorgio et al. discloses wherein the card is ISO Smartcard compatible; further comprising an ISO Smartcard processor (column 4, line 53 through column 5, line 12); and wherein the card comprises an upper magnetic stripe region and a lower embossed region (figure 2B, reference number 22).

Regarding claims 14 and 15, it would have been obvious to one of ordinary skill in the art that the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network and the first connection is permanently disabled after the loading process has been completed.

Regarding claims 21-23, Shen teaches all the limitations of claims 1, 2, and 18, above. However, Shen does not disclose wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate; the backing plate comprises a glass epoxy layer sandwiched between two metal layers; and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

DiGiorgio et al. discloses wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate; the backing plate comprises a glass epoxy layer sandwiched between two metal layers; and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon (column 5, lines 58-63).

Regarding claim 28, Shen teaches all the limitations of claims 1 and 25, above. However, Shen does not disclose wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

DiGiorgio et al. discloses wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid (column 10, lines 24-53).

Claims 11-13, and 18 lack an inventive step under PCT Article 33(3) as being obvious over Shen (E.P. 1,074,949) in view of DiGiorgio et al. (U.S. 6,385,729), and further in view of Goldwasser et al. (U.S. 4,826,479).

48

WRITTEN OPINION

International application No.
PCT/US03/28602

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Regarding claims 11-13, and 16, all the limitations of these claims have been taught by the rejection of claims 1, 2, 9, and 10, above. However, the combination of Shen and DiGiorgio et al. does not disclose wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall; all external data to and from the security processor passes through the ISO Smartcard processor; and all external data to and from the ISO Smartcard processor passes through the security processor.

Goldwasser et al. discloses wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall (column 33, lines 45-56); all external data to and from the security processor passes through the ISO Smartcard processor (column 33, lines 57-60); and all external data to and from the ISO Smartcard processor passes through the security processor (column 33, lines 57-60).

NEW CITATIONS

US 6,345,729 B1 (DIGIORGIO et al) 07 May 2002, see column 4, line 53 through column 5, line 12, column 5, lines 58-63, column 10, lines 24-33, and figure 2B, reference number 22.

US 4,926,479 B1 (GOLDWASSER et al) 15 May 1990, see column 33, lines 45-67.

44

The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ US

PCT

DEMAND

CHAPTER II

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty.

For International Preliminary Examining Authority use only	
Identification of IPEA	Date of receipt of DEMAND
Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION Applicant's or agent's file reference LA-7167-102.PC	
International application No. PCT/US03/28602	International filing date (day/month/year) 10 September 2003 (10.09.2003)
(Earliest) Priority date (day/month/year) 10 September 2002 (10.09.2002)	
Title of invention SECURE BIOMETRIC VERIFICATION OF IDENTITY	
Box No. II APPLICANT(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.) Telephone No.: Facsimile No.: Teleprinter No.: Applicant's registration No. with the Office	
State (that is, country) of nationality: US	State (that is, country) of residence: US
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.) SAITO, Tamio 300 Beale Street #1507 San Francisco, California 94105 United States of America	
State (that is, country) of nationality: US	State (that is, country) of residence: US
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.) AIDA, Takashi 920 Desert Isle Drive San Jose, California 95117 United States of America	
State (that is, country) of nationality: JP	State (that is, country) of residence: US
☒ Further applicants are indicated on a continuation sheet.	

Continuation of Box No. II APPLICANT(S)*If none of the following sub-boxes is used, this sheet should not be included in the demand.**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.)*

DRIZIN, Wayne
1810 Old Oakland Rd, Suite F
San Jose, California 95131
United States of America

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

*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.)**State (that is, country) of nationality:**State (that is, country) of residence:**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.)**State (that is, country) of nationality:**State (that is, country) of residence:**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.)**State (that is, country) of nationality:**State (that is, country) of residence:*☐

Further applicants are indicated on another continuation sheet.

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCEThe following person is ☒ agent ☐ common representativeand ☒ has been appointed earlier and represents the applicant(s) also for international preliminary examination.☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.☐ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.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.)*

MAY, John M.
 Fulbright & Jaworski L.L.P.
 865 South Figueroa
 Twenty-Ninth Floor
 Los Angeles, California 90017-2571
 United States of America

Telephone No.:

(213) 892-9252

Facsimile No.:

(213) 680-4518

Teleprinter No.:

Agent's registration No. with the Office

20,121

☐ 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.**Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION**

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination to start on the basis of:

☒ the international application as originally filed

the description

☒

as originally filed

☐

as amended under Article 34

the claims

☒

as originally filed

☐

as amended under Article 19 (together with any accompanying statement)

☐

as amended under Article 34

the drawings

☒

as originally filed

☐

as amended under Article 34

2. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.3. ☐ The applicant wishes the start of the international preliminary examination to be postponed until the expiration of the applicable time limit under Rule 69.1(d).4. ☐ The applicant expressly wishes the international preliminary examination to start earlier than at the expiration of the applicable time limit under Rule 54bis.1(a).

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

☒

which is the language in which the international application was filed.

☐

which is the language of a translation furnished for the purposes of international search.

☐

which is the language of publication of the international application.

☐

which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The filing of this demand constitutes the election of all Contracting States which are designated and are bound by Chapter II of the PCT.

Sheet No. 4 of 4

International application No.

PCT/US03/28602

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- | | | | |
|----|---|---|--------|
| 1. | translation of international application | : | sheets |
| 2. | amendments under Article 34 | : | sheets |
| 3. | copy (or, where required, translation) of amendments under Article 19 | : | sheets |
| 4. | copy (or, where required, translation) of statement under Article 19 | : | sheets |
| 5. | letter | : | sheets |
| 6. | other (specify): | : | sheets |

For International Preliminary Examining Authority use only

received

not received

☐☐☐☐☐☐☐☐☐☐☐☐

The demand is also accompanied by the item(s) marked below:

- | | |
|--|--|
| 1. ☒ fee calculation sheet | 5. ☐ statement explaining lack of signature |
| 2. ☐ original separate power of attorney | 6. ☐ sequence listing in computer readable form |
| 3. ☐ original general power of attorney | 7. ☐ tables in computer readable form related to a sequence listing |
| 4. ☐ copy of general power of attorney, reference number, if any: | 8. ☐ other (specify): |

Box No. VII 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 demand).


 Margaret A. Churchill, Agent for
 Applicant(s)
 FULBRIGHT & JAWORSKI L.L.P.

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:

2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):

3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply.☐ The applicant has been informed accordingly.4. ☐ The date of receipt of the demand is WITHIN the time limit of 19 months from the priority date as extended by virtue of Rule 80.5.5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.6. ☐ The date of receipt of the demand is AFTER the expiration of the time limit under Rule 54bis.1(a) and item 7 or 8, below, does not apply.7. ☐ The date of receipt of the demand is WITHIN the time limit under Rule 54bis.1(a) as extended by virtue of Rule 80.5.8. ☐ Although the date of receipt of the demand is after the expiration of the time limit under Rule 54bis.1(a), the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

Application No. (if known): PCT/US03/28802

Attorney Docket No.: LA-7187-102.PC

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV323456225US in an envelope addressed to:

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

on 9 April 2004
Date



Signature

Linda J. Werk

Typed or printed name of person signing Certificate

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

PCT Demand and Fee Calculation

TRANSMITTAL LETTER TO THE UNITED STATES RECEIVING OFFICE

Date	9 April 2004
International Application No.	PCT/US03/28602
Attorney Docket No.	LA-7167-102.PC

I. Certificate under 37 CFR 1.10 (if applicable)	
EV323458225US Express Mail mailing number	9 April 2004 Date of Deposit
I hereby certify that the application/correspondence attached hereto is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to MS PCT, Commissioner for Patents, P.O. Box 1430, Alexandria, VA 22313-1430.	
 Signature of person mailing correspondence	Linda J. Werk Typed or printed name of person mailing correspondence

II. ☐ New International Application	
TITLE	SECURE BIOMETRIC VERIFICATION OF IDENTITY
Earliest priority date (Day/Month/Year)	
SCREENING DISCLOSURE INFORMATION: In order to assist in screening the accompanying international application for purposes of determining whether a license for foreign transmittal should and could be granted and for other purposes, the following information is supplied. (Note: check as many boxes as apply):	
A. ☐ The invention disclosed was not made in the United States.	
B. ☐ There is no prior U.S. application relating to this invention.	
C. ☐ The following prior U.S. application(s) contain subject matter which is related to the invention disclosed in the attached international application. (NOTE: priority to these applications may or may not be claimed on form PCT/RO/101 (Request) and this listing does not constitute a claim for priority.)	
application no.	filed on
application no.	filed on
application no.	filed on
application no.	filed on
application no.	filed on
D. ☐ The present international application ☐ contains additional subject matter not found in the prior U.S. application(s) identified in paragraph C. above. The additional subject matter is found on pages and ☐ DOES NOT ALTER ☐ MIGHT BE CONSIDERED TO ALTER the general nature of the invention in a manner which would require the U.S. application to have been made available for inspection by the appropriate defense agencies under 35 U.S.C. 181 and 37 CFR 5.1. See 37 CFR 5.15.	

III. ☐ A Response to an Invitation from the RO/US. The following document(s) is(are) enclosed:	
A. ☐ A Request for An Extension of Time to File a Response	
B. ☐ A Power of Attorney (General or Regular)	
C. ☐ Replacement Pages	
pages	of the request PCT/RO/101
pages	of the description
pages	of the claims
D. ☐ Submission of Priority Documents	
Priority document	Priority document
E. ☐ Fees as specified on attached Fee Calculation sheet form PCT/RO/101 annex	

IV. ☐ A Request for Rectification under PCT Rule 91	☐ A Petition	☐ A Sequence Listing Diskette
--	-------------------------------------	--

V. ☒ Other (please specify): Chapter II Demand
--

The person signing this form is the:	☐ Applicant	Margaret A. Churchill
	☒ Attorney/Agent Reg. No. 39,944	Typed name of signer
	☐ Common Representative	 Signature

EV323458225US

PCT

FEE CALCULATION SHEET

Annex to the Demand

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">International application No. PCT/UB03/28602</td> <td style="width: 50%; text-align: center;">For International Preliminary Examining Authority use only</td> </tr> <tr> <td>Applicant's or agent's file reference LA-7167-102.PC</td> <td>Date stamp of the IPEA</td> </tr> </table>	International application No. PCT/UB03/28602	For International Preliminary Examining Authority use only	Applicant's or agent's file reference LA-7167-102.PC	Date stamp of the IPEA					
International application No. PCT/UB03/28602	For International Preliminary Examining Authority use only								
Applicant's or agent's file reference LA-7167-102.PC	Date stamp of the IPEA								
Applicant IVI SMART TECHNOLOGIES, INC., et al.									
CALCULATION OF PRESCRIBED FEES 1. Preliminary examination fee 750.00 P 2. Handling fee (<i>Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.</i>) 162.00 H 3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box \$ 912.00 TOTAL									
MODE OF PAYMENT <table style="width: 100%;"> <tr> <td>☒ authorization to charge deposit account with the IPEA (see below)</td> <td>☐ cash</td> </tr> <tr> <td>☐ cheque</td> <td>☐ revenue stamps</td> </tr> <tr> <td>☐ postal money order</td> <td>☐ coupons</td> </tr> <tr> <td>☐ bank draft</td> <td>☐ other (specify):</td> </tr> </table>		☒ authorization to charge deposit account with the IPEA (see below)	☐ cash	☐ cheque	☐ revenue stamps	☐ postal money order	☐ coupons	☐ bank draft	☐ other (specify):
☒ authorization to charge deposit account with the IPEA (see below)	☐ cash								
☐ cheque	☐ revenue stamps								
☐ postal money order	☐ coupons								
☐ bank draft	☐ other (specify):								
AUTHORIZATION TO CHARGE (OR CREDIT) DEPOSIT ACCOUNT (This mode of payment may not be available at all IPEAs) <table style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> ☒ Authorization to charge the total fees indicated above. ☒ This check-box may be marked only if the conditions for deposit accounts of the IPEA so permit) Authorization to charge any deficiency or credit any overpayment in the total fees indicated above. </td> <td style="width: 50%; vertical-align: top;"> IPEA/ <u>US</u> Deposit Account No.: <u>50-0337</u> Date: <u>9 April 2004</u> Name: <u>Margaret A. Churchill</u> Signature: <u>Margaret A. Churchill</u> </td> </tr> </table>		☒ Authorization to charge the total fees indicated above. ☒ This check-box may be marked only if the conditions for deposit accounts of the IPEA so permit) Authorization to charge any deficiency or credit any overpayment in the total fees indicated above.	IPEA/ <u>US</u> Deposit Account No.: <u>50-0337</u> Date: <u>9 April 2004</u> Name: <u>Margaret A. Churchill</u> Signature: <u>Margaret A. Churchill</u>						
☒ Authorization to charge the total fees indicated above. ☒ This check-box may be marked only if the conditions for deposit accounts of the IPEA so permit) Authorization to charge any deficiency or credit any overpayment in the total fees indicated above.	IPEA/ <u>US</u> Deposit Account No.: <u>50-0337</u> Date: <u>9 April 2004</u> Name: <u>Margaret A. Churchill</u> Signature: <u>Margaret A. Churchill</u>								

VERIFICACIÓN DE IDENTIDAD BIOMÉTRICA SEGURA**REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS**

[0001] Esta solicitud está basada y reivindica prioridad de las solicitudes provisionales 60/409,716 presentada en septiembre 10, 2002 (número de referencia 7167-102P1), 60/409,715 presentada en septiembre 10, 2002 (número de referencia 7167-103P), 60/429, 919 presentada en noviembre 27, 2002 (número de referencia 7167-104P), 60/433,254 presentada en diciembre 13, 2002 (número de referencia 7167-105P), y 60/484,692 presentada en julio 3, 2001 (número de referencia 7167-106P), que se incorporan aquí como referencia en su totalidad.

ANTECEDENTE

[0002] La computarización y especialmente la tecnología de Internet ha estado suministrando como nunca mayor acceso a los datos, incluyendo los datos financieros, datos médicos, datos personales, y con medios para hacer expedita las transacciones financieras y otras en las cuales los datos confidenciales se actualizan o se intercambian.

[0003] Las claves son comúnmente utilizadas para mantener la confidencialidad de tales datos; sin embargo, las claves están frecuentemente basadas en la fecha de nacimiento o el número de teléfono que es simple de adivinar y que no es de

ninguna manera seguro. Adicionalmente, a una clave complicada aleatoriamente generada puede a menudo ser fácilmente robada. Los sistemas de acceso de datos basados en la clave son así vulnerables al ataque criminal con el riesgo y daño resultante a la industria y la economía y aún a la vida de las personas. De acuerdo con esto, subsiste la necesidad de un método mejorado para asegurar los datos y proteger esos datos de acceso no autorizado.

[0004] Los datos biométricos pueden incluir detalles precisos que son difíciles de capturar pero fáciles de analizar (tales como una secuencia de la particularidad de la huella digital) o los patrones completos que son fáciles de capturar pero difíciles de analizar (tales como las características espaciales los espirales adyacentes de la huella digital).

[0005] Existen algoritmos descifrados que requieren una clave digital disponible solamente a usuarios autorizados. Sin la clave adecuada, los datos cifrados pueden ser descifrados en un formato utilizable solamente con una inversión sustancial de tiempo y de recursos de procesamiento, y aún entonces, solo si ciertas características de los datos cifrados son conocidos (o al menos son predecibles).

[0006] La Solicitud de Patente Japonesa publicada JP 60-029868 fechada en febrero 15, 1985 a nombre de Tamio SAITO

enseña un sistema de identificación individual que emplea una tarjeta de identidad con una memoria integrada para registrar los datos biométricos cifrados obtenidos del portador de la tarjeta. Los datos biométricos pueden incluir registro de voz, huella digital, apariencia física, y/o una prueba biológica. En uso, los datos en la tarjeta se leen y descifran por comparación con los datos correspondientes capturados de la persona que presenta la tarjeta. Tal sistema le permite a un individuo registrado ser positivamente identificado con un alto grado de precisión. Sin embargo, en razón a que los datos biométricos son obtenidos y procesados mediante equipo externo, es difícil de proteger la información almacenada en la tarjeta contra posible alteración y/o robo de identidad.

[0007] Una tarjeta de identificación mejorada se ha propuesto la cual incluye un chip multiprocesador para manejo de datos en la tarjeta para suministrar un cortafuegos de hardware que cifre y aisle los datos biométricos almacenados en la tarjeta, suministrando de esta manera protección sustancialmente mayor contra alteración no autorizada de los datos almacenados. Sin embargo, el proceso actual de apareamiento fue desarrollado en el mismo terminal de lectura externo que capturó los datos biométricos vivos, y era entonces así potencialmente vulnerable a la manipulación fraudulenta externa.

RESUMEN

[0008] Una primer modalidad de una tarjeta de identificación de alta seguridad incluye no solamente una memoria en la tarjeta para los datos biométricos almacenados sino también un sensor en la tarjeta para capturar los datos biométricos vivos. Un sistema de autenticación remota mantiene una base de datos segura incluyendo los datos biométricos. Un procesador a bordo de la tarjeta desarrolla una operación de apareamiento preliminar para verificar que los datos biométricos capturados coincidan con los datos biométricos localmente almacenados. Solo si existe una coincidencia local positiva, es algún dato capturado o algún dato almacenado sensible transmitido al sistema de autenticación remoto para verificación adicional y procesamiento ulterior. Como una protección ulterior contra ataque malicioso, los datos localmente almacenados son preferiblemente diferentes de los datos remotamente almacenados, y la coincidencia local y la coincidencia remota preferiblemente son conducidas utilizando diferentes algoritmos de apareamiento. Así aún si la tarjeta, los datos localmente almacenados, y/o el terminal local al cual las tarjetas están conectadas está aún comprometido, existe una alta probabilidad de que el sistema de autorización remota sea estable para detectar la intrusión intentada.

[0009] Una segunda modalidad también incluye una memoria a bordo para los datos biométricos almacenados, un sensor a

bordo para capturar los datos biométricos vivos y un procesador a bordo, sin embargo, en esa modalidad el proceso de apareamiento completo es desarrollado mediante un procesador a bordo y tanto los datos biométricos originalmente capturados como cualquiera otra información "privada" almacenada en la memoria a bordo no se hacen disponibles a ningún proceso externo. En su lugar, solamente se genera un mensaje de verificación en respuesta a una coincidencia exitosa entre los datos biométricos recientemente capturados y los datos biométricos previamente capturados. El mensaje de verificación origina que la tarjeta funcione de una manera similar a una "SmartCard" ISO convencional luego del ingreso exitoso/no exitoso de un Número de Identificación Personal (PIN), pero con la seguridad adicional lograda por medio de un proceso de verificación más seguro. En cualquiera de aquellas modalidades, los datos biométricos almacenados y cualquier algoritmo descifrado localmente almacenado asociado o clave descifrado es preferiblemente cargada en la tarjeta en el momento de la emisión original de el portador de la tarjeta de tal manera que desanime cualquier acceso externo subsecuente, mejorando adicionalmente de esta manera la integridad de los datos biométricos almacenado y el proceso de verificación completo.

[0010] En una modalidad, la "SmartCard" ISO funciona como un cortafuegos para proteger el procesador de seguridad utilizado para almacenar y procesar los datos biométricos

protegidos de ataque externo malicioso por vía de la interfaz de la SmartCard ISO. En otra modalidad, el procesador de seguridad se inserta entre la interfaz de la SmartCard ISO y un procesador SmartCard ISO no modificado y bloquea cualquier comunicación externa hasta que la huella digital del usuario ha sido comparada con una huella digital previamente registrada.

[0011] En una modalidad preferida de una tarjeta de identificación de alta seguridad con capacidades de apareamiento de huella digital a bordo, se suministra retroalimentación en tiempo real aunque el usuario esté manipulando su dedo sobre el sensor de la huella digital, facilitando de esta manera una ubicación óptima del dedo sobre el sensor. Esta retroalimentación no solo reduce la complejidad computacional sino también suministra medios adicionales para discriminar entre un usuario no experimentado un usuario fraudulento, reduciendo de esta manera adicionalmente la probabilidad de negativos falsos y/o positivos falsos. En otra modalidad preferida, el sensor de huella digital es retenido un portador que suministra rigidez adicional.

[0012] En una aplicación de ejemplo, los datos biométricos capturado y/o una indicación de la identidad del portador de la tarjeta se encripta e ingresa a una red transaccional que incluye una institución financiera y un servidor de autenticación separado antes de cualquier otorgamiento de

acceso en línea a datos confidenciales o a cualquier proceso automatizado para completar una transacción segura. En otra aplicación de ejemplo, la salida de la tarjeta es utilizada para obtener acceso físico dentro del área segura. En cualquier aplicación, el registro de los intentos de acceso exitoso y no exitoso se puede mantener en la tarjeta o en un servidor de seguridad externo, o en ambos.

DIBUJOS

[0013] La figura 1 muestra una modalidad de la tarjeta inteligente con una verificación biométrica de la identidad a bordo de la persona que presenta la tarjeta.

[0014] La figura 2 es un diagrama de flujo que muestra un proceso de ejemplo para ayudar al usuario en la ubicación óptima de un dedo sobre el sensor de la huella digital.

[0015] La figura 3 es un diagrama de bloque funcional de un sistema de verificación biométrico capaz tanto de verificación local como remota de la identidad de una persona que presenta una tarjeta de identificación segura.

[0016] La figura 4 es un diagrama de bloque funcional de una tarjeta de verificación biométrica de ejemplo o diferentes celdas de datos físicos para usar durante la carga inicial de los datos biométricos del portador de la tarjeta y

durante la verificación de la identidad del portador de la tarjeta a una aplicación remota.

[0017] La figura 5 muestra una modalidad alternativa de la tarjeta de verificación biométrica de ejemplo de la figura 4, que está destinada para uso con una CPU de SmartCard ISO no modificada.

[0018] La figura 6 es un diagrama de flujo que muestra la comunicación entre una aplicación de ejemplo y una tarjeta de verificación de ejemplo en la cual solamente se desarrolla la verificación local de la identidad del portador de la tarjeta.

[0019] La figura 7 es similar al diagrama de flujo de la figura 6, pero modificado para uso con la tarjeta de verificación biométrica de ejemplo de la figura 5.

[0020] La figura 8 muestra una segunda modalidad de una tarjeta inteligente con verificación biométrica a bordo que puede ser conectada a un terminal local bien sea inalámbricamente o por medio de un conector eléctrico.

[0021] La figura 9 es una sección transversal a través de la tarjeta de la figura 8.

[0022] La figura 10 es un diagrama de circuito de un sensor de huella digital de ejemplo.

[0023] La figura 11 muestra una modalidad de un montaje de portador para el sensor de la figura 10.

DESCRIPCIÓN DETALLADA

Tarjeta Inteligente

[0024] La frase "tarjeta inteligente" o "tarjeta inteligente" se utiliza aquí en un sentido general para referirse a cualquier objeto físico que es suficientemente pequeño para ser mantenido en la mano, portado cerca del cuello, o portado en cualquier otra parte cerca de la persona y que incluye un microprocesador que es capaz de almacenar, procesar, y comunicar información digitalmente concerniente o relacionada de alguna forma con un portador de tarjeta individual. Un ejemplo bien conocido de tal tarjeta inteligente es la SmartCard ISO (Internacional Standard Organization) que tiene el mismo tamaño y forma física de una tarjeta de crédito convencional, pero que incluye memoria flash para almacenar datos especificados del usuario y un microprocesador que puede ser programado con un algoritmo de infiltración potente que indica si el PIN (Número de Identificación Personal) recibido de un terminal de usuario coincide con el PIN cifrado almacenado en la tarjeta, suministrando de esta manera un mayor grado de seguridad de que la persona que presenta la tarjeta es el portador real de la tarjeta de lo que sería posible en un sistema de

verificación que simplemente confía en la comparación visual de firmas y/o similitudes físicas.

[0025] Ahora se debe hacer referencia de la figura 1, que muestra una modalidad de una tarjeta inteligente con una verificación biométrica a bordo. La tarjeta 100 es hecha generalmente de material plástico y tiene una apariencia total de una tarjeta de crédito convencional, de dimensiones aproximadas como se especifican en la ISO 7816 de aproximadamente 53,98 x 85,6 mm y grosor de aproximadamente 0,76 mm o más.

[0026] De manera similar a una tarjeta de crédito convencional, la tarjeta 100 incluye una región superior libre 102 que se extiende a lo largo del ancho transversal completo de la tarjeta para soportar la tira magnética (como se especifica en la ISO 7811-2 & 7811-6) sobre la superficie posterior de la tarjeta, sobre la cual se pueda almacenar convencionalmente la información alfa numérica codificada a cerca del portador de la tarjeta y cualquier cuenta asociada, permitiendo de esta manera que la tarjeta 100 sea utilizada en un lector de tira magnética convencional. Sin embargo, en razón a que cualquier dato guardado en la tira magnética puede ser fácilmente alterado, tal tira magnética pretende solo ser utilizada en ciertas aplicaciones donde la necesidad de compatibilidad con versiones anteriores con terminales basados en tira magnética más vieja es preponderante sobre la

degradación potencial de seguridad que una tira magnética trae al sistema.

[0027] La región superior 102 también se puede utilizar para soportar varias medidas de prevención de fraude, tal como una fotografía a color resistente a violación del portador y/o un logo holográfico del emisor de la tarjeta. La región inferior 104 de la tarjeta 100 se puede utilizar de forma convencional para información realzada (como se especifica por la ISO 7811-1) da como el nombre del portador, una identificador de cuenta numérica (o tarjeta), una fecha de expiración, para permitir el uso de la tarjeta 100 en una impresora de tarjeta convencional.

[0028] La región superior 102 y la región inferior 104 están separadas por una región media 106 en la cual están empotrados un conjunto de 8 tabletas de contacto SmartCard ISO 108 visible, que suministra una conexión eléctrica conveniente entre la tarjeta y los contactos correspondientes sobre un lector de tarjeta. Por este medio, no solo los datos, sino también la potencia, tiempo y señales de control se pueden intercambiar entre el lector y la tarjeta como se especifica en la ISO 7816-3.

[0029] En el lado derecho de la región 106 una tableta sensora 110 es visible, que se utiliza para capturar los datos de la huella digital del dedo del portador. La tarjeta preferiblemente es suministrada con un código ID que es único

al sensor 110 u otro componente electrónico empotrado en la tarjeta; por ejemplo, un código en el formato de una dirección IP y/o MAC convencional.

[0030] También indicada esquemáticamente en la figura 1 están varios componentes electrónicos adicionales que cooperan con la tableta de contactos 108 y el sensor 110 para suministrar mayor funcionalidad, y en particular mejor seguridad, de lo que sería de otra manera posible.

[0031] En una modalidad, el procesador compatible SmartCard ISO 112 está directamente conectado a las tabletas de contacto ISO 108 para suministrar una conexión eléctrica con un lector de tarjeta compatible ISO externo (no mostrado) para suministrar no solamente potencia a los dispositivos electrónicos a bordo, sino también unos medios para comunicar datos entre la tarjeta y cualquier software de comunicación externo, software de seguridad, software de transacción, y/u otro software de aplicación que corra sobre el lector de tarjeta o cualquiera dispositivo de cómputo asociado en red con el lector de tarjeta.

[0032] Aunque en la modalidad descrita la senda de datos entre la tarjeta 100 y el lector de tarjeta externa está en la forma de una conexión alambrada que utiliza una disposición de contacto SmartCard especificada ISO, se debe entender que en otras modalidades, otras tecnologías de transmisión también se pueden utilizar tales como conexiones

USB o RS 232C o SPI (serial) posiblemente sobre enlaces RF inalámbricos (Radio Frecuencia), de microondas y/o IR (Infra Rojo).

[0033] También, aunque la modalidad descrita recibe energía del lector de tarjeta, otras modalidades pueden tener una fuente a bordo de energía tal como una pila solar o una batería. Tal fuente de energía a bordo podría ser ventajosa, por ejemplo, si la interfaz mecánica entre la tarjeta 100 y un tipo particular de lector de tarjeta es tal que el sensor de huella digital 110 no es accesible al usuario cuando los contactos 108 están conectados a las conexiones correspondientes dentro del lector de tarjeta, y así los datos de huella digital del usuario deben ser capturados cuando la tarjeta 100 no es directamente alamburada o conectada con cable al lector de tarjeta.

Procesador de Seguridad

[0034] Como se ilustra, el procesador de seguridad 114 está conectado entre el procesador ISO 112 y el sensor 110 para suministrar procesamiento y almacenamiento seguro de los datos capturados, así como también un "cortafuego" seguro para proteger los datos y programas almacenados en su memoria dedicada desde cualquier intento de acceso impropio por vía del procesador ISO 112, como se describirá en lo sucesivo. Tal cortafuegos se puede diseñar con el paso solamente de datos cifrados utilizando una clave de cifrado que está

basada en una dirección de red únicamente asignada o que de otra manera es única a la tarjeta particular, tal como los datos extraídos de un patrón de huella digital previamente almacenada o un número de dispositivo únicamente asignado tal como el número CPU o el número de sensor de huella digital. En otra modalidad, el cortafuego solamente pasa datos que contienen datos únicos de identificación de la transmisión previa o los datos. En aún otras modalidades, el cortafuegos mantiene diferentes claves para aplicaciones diferentes, y utiliza aquellas claves para enrutar los datos a un procesador diferente respectivo o a una partición de memoria.

[0035] En otra modalidad (no ilustrada) el procesador de seguridad 114 está directamente conectado a los contactos ISO 108 y actúan como un controlador de pasarela seguro entre el procesador ISO 112 y los contactos ISO 108. Tal disposición alterna tiene la ventaja de suministrar la seguridad adicional lograda por el procesador de seguridad 114 y el sensor 110, sin ningún compromiso posible de ninguna de las características de seguridad que pueden ya ser incorporadas dentro del procesador ISO 112.

[0036] El procesador de seguridad 114 preferiblemente incluye una memoria no volátil semi-conductora o no semi-conductora, tal como la FRAM, OTP, E²PROM, MRAM, MROM, para almacenar un patrón de huella digital previamente enrolado y/o otra información biométrica personal. En otras modalidades, algunas o todas las funciones del procesador de

seguridad 114 se pueden implementar en un procesador ISO 112 y/o algunas o todas las funciones del procesador ISO 112 se pueden implementar en un procesador de seguridad 114. Tal implementación combinada podría aún mantener un cortafuegos de software entre las varias funciones, que serían especialmente ventajosas si el dispositivo fuera implementado con un proceso que no permitiera ninguna modificación subsecuente a los programas de software almacenados. Alternativamente, ambos procesadores 112, 114 pueden ser procesadores separados en un dispositivo multiprocesador simple diseñados para proteger cada proceso de alguna interferencia de otro proceso que corre en un procesador diferente. Un ejemplo de tal dispositivo multiprocesador es el DDMP (Procesador Múltiple Controlado de Datos) de Sharp de Japón.

[0037] Aunque estos varios sensores, contactos y otros componentes electrónicos, así como también circuitos impresos u otras conexiones eléctricas con las cuales ellas están interconectadas, son todas preferiblemente incorporadas completamente dentro del cuerpo de la tarjeta 100 de tal forma que ellas son protegidas de la abrasión y los contaminantes externos, en sitio preferido dentro de la región media 106 entre la región superior 102 y la región inferior 104 los protege adicionalmente de posible daño de los lectores de tira magnética convencional, realizadores, y equipo de impresión que hace interfaces mecánicamente con aquellas otras regiones.

Retroalimentación LED

[0038] Los LED 116a, 116b son controlados mediante un procesador de seguridad 114 y suministran retroalimentación visible al usuario. En la modalidad ilustrada, ellos están localizados en la región inferior 104 preferiblemente en un sitio en el borde lateral de la tarjeta distante de las tabletas de contacto 108. En cualquier evento, los LED 116a y 116b están preferiblemente localizados donde ellos no serán dañados durante el proceso de realzado y donde ellos serán visibles cuando la tarjeta se inserte en un lector SmartCard ISO convencional y/o mientras el dedo del usuario esté ubicado sobre el sensor de huella digital 110. Por ejemplo:

En Modo de Verificación:

- Centelleo ROJO: Espera del dedo
- Parada de Centelleo: Dedo ubicado en el sensor
- ROJO centellea una vez: Incapaz de coincidir, ok para mover el dedo
- VERDE centelleo largo una vez: 0 incidencia, ok para remover el dedo

En Modo de Inscripción

- Centelleo VERDE: Espera por el dedo
- Retención del centelleo: Dedo ubicado en el sensor
- ROJO centelleo una vez: Incapaz de inscripción, ok para mover el dedo
- VERDE centelleo una vez: Inscrito, objeto a remover dedo

En Modo de Borrado

- VERDE y ROJO centellean: Lista para borrar
- VERDE centellea una vez: Borrado.

[0039] Al usuario le son dadas preferiblemente múltiples oportunidades para ubicar su dedo para una coincidencia exitosa o para inscripción antes de que cualquier reporte negativo sea transmitido. En una modalidad, un reporte negativo es transmitido al Servidor de Autenticación solamente si el usuario ha removido su dedo antes de recibir la indicación ok verde, o si un límite de tiempo predeterminado se ha excedido. Tal proceso no solamente adiestra al usuario para hacer una ubicación óptima de su dedo sobre el sensor, lo cual no solamente reduce la complejidad computacional sino también permite el uso de más umbrales discriminantes. Esta retroalimentación visible también suministra una base psicológica para discriminar entre

un usuario inexperto (que típicamente mantendrá ensayando hasta que logra la ubicación adecuada) y un usuario fraudulento (quien típicamente no querrá atraer ninguna atención y saldrá antes de que sus intenciones maliciosas sean descubiertas). El resultado neto es una reducción significativa en la probabilidad de negativos falsos y/o positivos falsos.

[0040] La figura 2 ilustra un proceso de ejemplo para ayudar al usuario a ubicar su dedo en el sensor 110. En el bloque 150, el LED ROJO 116b está centelleando. Una vez que ha sido detectado el dedo (bloque 152), el LED detiene el centelleo y un ensayo hecho para la calidad de la imagen (bloque 154) (regiones alargadas definidas que corresponden a las montañas valles de la piel del dedo). Si la calidad es inadecuada (NO rama 156), un centelleo simple del LED ROJO 116b le instruye al usuario a mover su dedo a una posición diferente (bloque 158); de otra manera, SI rama 160) un segundo ensayo (bloque 162) es desarrollado para determinar si el mismo dedo ha sido ubicado en la misma posición que se utilizó para registrar el Usuario de tal forma que un algoritmo de coincidencia relativamente simple pueda verificar los datos vivos que corresponden a los datos almacenados dentro de un umbral predeterminado, verificando de esta manera que el dedo vivo es el mismo que el dedo que ha sido originalmente registrado (SI rama 164) y el LED VERDE 116a es activado (bloque 166) durante un tiempo suficiente (bloque 168) para verificar que una coincidencia exitosa ha

tenido lugar y que el usuario pueda ahora remover su dedo. Alternativamente, si el umbral de coincidencia no se cumple (No rama 170), un centelleo simple del LED ROJO 116b (bloque 158) le instruye al usuario a mover su dedo a una posición diferente y el proceso se repite.

Arquitecturas de Red de Ejemplo

[0041] Se debe hacer ahora referencia a la figura 3 que ilustra una modalidad posible de un sistema de verificación biométrico capaz de verificación tanto local como remota de la identidad de una persona que presenta una tarjeta de identificación segura. Esta incluye tres componentes principales: un terminal de cliente 200 un servidor de aplicación 202 y un servidor de autenticación 204. El terminal de cliente 200 incluye funcionalidad para la captura en vivo y el procesamiento local de una huella digital de usuario para ser cifrado de los datos localmente procesados, y para comunicación segura con el servidor de aplicación y el servidor de autenticación, preferiblemente en Internet utilizando el esquema de direccionamiento y el protocolo de transmisión IP/TCP, con protección de acceso malicioso siendo suministrada por cortafuegos IP convencionales 206. En otras modalidades los cortafuegos 206 pueden ser suministrados con Filtros y Codificador/Decodificador Descifrado que codifique los datos transmitidos después de que han sido verificados para ser datos Autorizados y que descifran o decodifican los datos recibidos antes de decidir si estos son de hecho datos

75

Autorizados, por ejemplo autorizando un algoritmo de descifrado tal como el DES 128. Por estos medios, el cortafuego 206 puede clasificar datos como Autorizados o potencialmente Maliciosos con base no solamente en el encabezado del mensaje, sino también con base en el contenido del mensaje.

[0042] El terminal de cliente 200 se puede implementar como un electrodoméstico dedicado de red, o se puede implementar en software instalado en un computador de escritorio programable, portátil o una estación de trabajo o computador personal controlado por un sistema operativo de propósito general tal como el Windows XXX, OS X, Solaris XX, Linus o BSD Libre. En el Terminal de Cliente 200 preferiblemente incluye bases de datos factorizadas "negativa" (por ejemplo identidades de tarjetas perdidas o robadas, o restricción sobre una tarjeta o un grupo de tarjetas particulares) que logran una medida adicional de seguridad.

[0043] El servidor de aplicación 202 incluye la funcionalidad para conducir la transacción o responder de otra manera a instrucciones desde el usuario remoto en el terminal de cliente 200 después de que la identidad del usuario ha sido verificada mediante el servidor de autenticación 204. El servidor de autenticación 204 incluye la funcionalidad para comunicación segura tanto con el terminal de cliente 200 como con el servidor de aplicación

202, para almacenar datos de huella digital auténticos y otra información concerniente con los usuarios previamente registrados, para comparar los datos almacenados con los datos vivos descifrados recibidos del terminal de cliente 200, y para avisarle al servidor de aplicación 202 si los datos de huella digital en vivo coinciden con los datos de huella digital almacenados especificados.

[0044] Más particularmente, el Terminal de Cliente 200 comprende adicionalmente dos componentes principales: un componente de lector de tarjeta fijo 208 que incluye un terminal con un programa de Internet 210 y una interfaz de lector de tarjeta 108a (que puede ser un cable USB simple que termina en un conjunto de contactos eléctricos para formar conexión eléctrica respectiva con las tarjetas de contacto SmartCard ISO 108) y un componente de tarjeta inteligente portátil 100'. En una modalidad, el componente portátil 100' puede ser la tarjeta inteligente previamente descrita 100 que incluye el sensor de huella digital 110, el procesador de seguridad 114 y el procesador SmartCard ISO 112.

[0045] El servidor de aplicación 202, comprende adicionalmente una interfaz de servidor de Internet que incluye un cortafuegos 206 y un programa de la relación en Internet 214, así como también un módulo de aplicación de transacción 216 y un módulo de validación 218. En el evento en que el servidor de aplicación y el módulo de aplicación 216 sean dispositivos delegados que no fueron designados para

comunicarse externamente por medio del protocolo IP/TCP. El cortafuegos 210 puede ser reemplazado con un convertidor de protocolo apropiado que incorpora el módulo de validación 218 y que tiene una dirección IP fija. El Servidor de Servicio de Aplicación puede por ejemplo ser operado por una tercer parte que está deseosa de suministrar servicio a través de Internet a un Usuario autorizado.

[0046] El Servidor de Autenticación 204 comprende además una interfaz de servidor de Internet 220, un módulo de procesamiento 222 que incluye un algoritmo de coincidencia de huella digital 224, y una base de datos 226 para almacenar la huella digital y otra información auténtica recolectada de los individuos en el momento en que aquellos individuos fueran registrados con el sistema y su identidad fuera garantizada para la satisfacción del operador de sistema. Como una mejora de seguridad adicional, los datos almacenados para un individuo particular son preferiblemente no almacenados en el Servidor de Aplicación como una secuencia simple de información sino en su lugar cada ítem sea almacenado separadamente y cualquier índice requeridos o relaciones que conectan aquellos ítems sean accesibles solamente por medio de una clave correspondiente que es mantenida como parte de los datos privados del individuo en el Servidor de Autenticación.

Localización

[0047] En ciertas modalidades, el lector fijo 208 y/o la tarjeta portátil 100' también pueden estar equipados con un receptor Satelital de Posicionamiento Global ("GPS") 212 que puede suministrar información útil a cerca de la localización habitual del lector y la tarjeta o a cerca del tiempo en que ha tenido lugar la transacción particular. En particular, los datos de localización provenientes de receptor GPS 212 se puede utilizar para deshabilitar (permanente o temporalmente) el lector y/o la tarjeta en el evento de que cualquiera sea removida a un sitio en el cual su uso no sea autorizado. La posición también puede ser automáticamente determinada por medio de dispositivos distintos a GPS, por ejemplo utilizando tecnología de localización de llamante PHS (Teléfono Celular Japonés), o sensores de localización que responden a variaciones locales en los campos electromagnéticos de la tierra. En el caso particular de la tarjeta equipada con GPS, los varios componentes GPS incluyen antena; amplificación de señal, convertidor AD y circuitos de muestra y de soporte; y procesador digital para calcular la posición son preferiblemente todos parte de un circuito integrado simple o un dispositivo discreto montado en una tarjeta de circuito simple, que es integrada con, empotrada en, o laminada al cuerpo de la tarjeta.

Arquitectura de Tarjeta para la tarjeta ISO con unas Interfaces de Procesador ISO de Coincidencia a Bordo.

[0048] La figura 4 es un diagrama de bloque funcional para una tarjeta de verificación biométrica compatible SmartCard ISO 100 0 100' con sendas de datos físicos diferentes para uso durante la carga inicial de los datos biométricos del portador y durante la verificación de la identidad del portador a una aplicación remota.

[0049] En particular, además del procesador ISO previamente descrito 112, el procesador de seguridad 114, el sensor de huella digital 110, los LED 116a, 116b y el receptor GPS opcional 212, con solamente el procesador ISO 112 estando directamente conectado al Lector de tarjeta 208 por vía de las tabletas de contacto SmartCard ISO 108, se muestra un módulo de Carga separado 300 y una conexión temporal asociada 302, que suministra comunicación directa con el Procesador de Seguridad 114 durante el Registro inicial del Usuario. Se puede anotar que el procesador ISO 112 se comunica con el Procesador de Seguridad 114 por medio de los puertos I/O 404, 306, mientras la conexión de Carga temporal 302 se conecta a un puerto I/O separado 308. El procesador de seguridad es preferiblemente programado de tal forma que cualquier dato o software relacionados con seguridad sean accesibles solamente desde el puerto 208 y no desde los puertos 304 y 306, evitando de esta manera cualquier posibilidad de acceso malicioso a estos datos sensibles después de que la conexión 302 ha sido deshabilitada.

[0050] Los procesadores ISO más comercialmente disponibles tienen al menos dos puertos I/O y algunos tienen hasta tres. Solamente uno de estos puertos (I/O 1) se designa para la conexión de datos en serie SmartCard ISO convencionales 108 al Lector de Tarjeta compatible ISO externo 208. Los uno o dos puertos extra I/O preferiblemente suministran una comunicación alámbrica dedicada entre el Procesador ISO 112 y el Procesador de Seguridad 114 que actúa como un cortafuegos de hardware para bloquear cualquier intento malicioso para reprogramar el Procesador de Seguridad 114 o para lograr acceso a cualquier información sensible que pueda haber sido previamente calculada por el sensor 110 o que pueda de alguna otra manera ser almacenada dentro del Procesador 114. En el caso particular de un Procesador ISO con más de dos líneas I/O, es posible presentar mas de dos estados de información de estado estático en la senda recomunicación dedicada entre el Procesador ISO y el Procesador de Seguridad, tal como 1) Preparado, 2) Ocupado 3) Falla, 4) Pasa aún cuando el Procesador de Seguridad está completamente apagado. Por supuesto, aún si solamente uno de los puertos y/o está disponible aquellas cuatro condiciones se pueden transmitir dinámicamente como datos en serie.

[0051] Entre los posibles comandos y datos que pueden ser transmitidos entre la ISO CPU y la CPU de Seguridad sobre las interfaces ISO I/O 2 e I/O 3 están las siguientes:

- Los comandos para capturar o autenticar un Usuario, al cual la CPU de Seguridad enviará los resultados de la captura o resultado de autenticación para almacenamiento local I/O transmisión a una aplicación remota.

- La información de huella digital como una plantilla (referencia) puede ser enviada desde la CPU de Seguridad a la ISO CPU para almacenar en la memoria SmartCard ISO para transmisión a aplicaciones remotas. Para seguridad incrementada de la información personal sensible, los datos de referencia se pueden cifrar mediante la CPU de seguridad antes de que esta sea enviada a la ISO CPU.

[0052] La conexión de carga 302 suministra una conexión directa a la CPU de seguridad 114 que puentea cualquier protección de cortafuegos lograda por la conexión ISO y los puertos I/O dedicados asociados 304 y 306, aunque posiblemente manteniendo la comunicación entre la ISO CPU 112 y el lector ISO 208 de tal forma que la potencia también estará disponible a la CPU de Seguridad 114. Esta es primariamente utilizada durante el registro inicial de la tarjeta a un usuario particular, y debe ser protegida contra acceso no autorizado.

[0053] La figura 5 muestra una modalidad alternativa a la tarjeta de verificación biométrica de ejemplo de la figura 4, que está destinada a uso con la CPU SmartCard ISO no modificada. En particular, la ISO CPU 112' ya no debe desarrollar ninguna de las funciones de puerta de enlace

entre el Lector de Tarjeta 208 y la CPU de Seguridad 114', bien sea durante el uso normal o durante la carga y así este puede ser cualquier chip aprobado ISO, no modificado de ninguna manera y utilizado solamente de manera que sea absolutamente transparente tanto para el lector de Tarjeta 208, o cualquier aplicación externa. En tal modalidad alternativa, la CPU de Seguridad 114' actúa como un cortafuego transparente entre la ISO CPU 112' y cualquier aplicación externa si la huella digital capturada coincide con la huella digital almacenada, y bloquea todas las comunicaciones si la huella digital capturada no coincide con la huella digita almacenada.

Inicialización de Tarjeta y Protección de Datos Almacenados

Guillotina

[0054] En una modalidad, la tarjeta originalmente elaborada tiene una extensión de circuito impresa sobresaliente que suministra una conexión directa a la CPU de Seguridad así como también al menos porciones de la interfaz ISO y/o cualquier memoria discreta a bordo. Esta interfaz de conexión directa es utilizada solamente para ensayar la tarjeta y los datos de huella digital cargados e incluye la señal que posibilita el proceso de cargue. Después de que se ha completado el cargue, la extensión de circuito es mecánicamente cortada de tal forma que ninguna carga adicional será posible, y la memoria CPU de Seguridad es

accesible solamente a través de la ISO CPU y el cortafuego previamente mencionado entre la ISO CPU y la CPU de Seguridad.

Fusible

[0055] En otra modalidad, la CPU de Seguridad tiene un tipo de memoria que una vez el patrón de huella digital cargado es escrito, será entonces inaccesible. Un ejemplo de tal memoria es PROM de tiempo ("OTP") que es similar en construcción a la EEPROM, pero es opaca a UV y así no puede ser borrada. Otro ejemplo es la ROM Flash que es vuelta de solo lectura después de que se ha completado el cargue, por ejemplo al aplicar suficiente corriente a una porción de la senda de señal de habilitamiento o dirección o datos para formar una ruptura física ("fusibles") en esa senda de señal.

Proceso de Autenticación de Ejemplo

[0056] En una modalidad, un proceso de autenticación de ejemplo involucra capturar la huella digital físico, por ejemplo, utilizando tecnologías ópticas de presión o conductoras o capacitivas o acústicas o elásticas o fotográficas en el Terminal de Cliente utilizados por la persona que accede a conectar al servidor de Servicio de Aplicación que es entonces enviado (preferiblemente en forma cifrada) a un Servidor de Autenticación de Huella Digital separado. El Servidor de Autenticación de Huella Digital

compara los datos de huella digital capturados con un Archivo de Huella Digital, que incluye los datos de huella digital registrados del Usuario, utilizando un Software de Autenticación, y si los datos son coincidentes el Servidor de Autenticación envía una instrucción habilitante al Servidor de Servicio de Aplicación.

[0057] En otra modalidad, el Usuario accede al programa de navegación WEB asegurado del Servidor de Autenticación de Huella Digital, que contiene archivos de huella digital, donde todas las huellas digitales son prerregistradas junto con los datos individuales, tales como el nombre, dirección, o fecha de nacimiento. EL Servidor de Autenticación de Huellas Digital asegurado, cuyo Usuario está accediendo a través de un protocolo seguro tal como el formato HTTPS, entonces envía la instrucción al terminal de cliente para capturar la huella digital del Usuario en el Terminal de Cliente. En respuesta a las instrucciones desplegadas por el programa de navegación del Terminal de Cliente, el Usuario pone su dedo seleccionado sobre el Sensor de Huella Digital y Software de Captura de Huella Digital residente en el Terminal de Cliente capturan una huella en forma digital, por ejemplo una imagen basada en píxel con 25 micrómetros a 70 micrómetros de resolución de tono y un área de un cuadrado de 12,5 mm por 25 mm, y adicionalmente tiene una escala de grises de 8 bits.

[0058] EL Servidor de Autenticación de Huella Digital segura reciben los datos de huella digital junto con el ID del usuario así como también la dirección IP de Internet y/o el código individual del sensor de huella digital (dirección MAC) y/o "cookie" y/o código único u otra información que identifica el individuo particular o terminal (por ejemplo, detalles de una conversación previa entre el terminal de Cliente y el Servidor de Autenticación de Huella Digital asegurado) por medio del cual se compara los Datos de Huella Digital recibidos con un Archivo de Huella Digital, que son los datos de huella digital pre-registrados junto con el ID del usuario, la información digital tal como nombre, dirección, fecha de nacimiento, registro de crímenes, licencia de conducción, número de seguridad social etc. utilizando Software de Autenticación, que puedan generar una comparación minuciosa y o una Comparación de Transformación Furia Rápida.

[0059] Al comienzo del proceso de Autenticación, el Servidor de Red 214 para la aplicación relevante instruye visualmente o audiblemente al Usuario a poner su dedo sobre el Sensor de Captura de Huella Digital 110 y a obturar el botón del ratón o la clave en el teclado para de esta manera indicar el Software de Captura de Huella Digital en el procesador de Seguridad 114. Entonces los datos de huella digital capturados del Usuario son enviados en formato cifrado (por ejemplo, utilizando un protocolo de transmisión cifrado RSA seguro HTTPS), al Servidor de Red 220 del

Servidor de Autenticación de Huella Digital 204 por vía del procesador ISO 112 y el Programa de Navegación de Red 210 al Terminar de Cliente 200. Si los datos capturados son exitosamente coincidentes con los datos correspondientes en su Base de Datos 226, el Servidor de Autenticación de Huella Digital 204 valida entonces la identidad del usuario tanto en el Terminal de Cliente 200 como en el Servidor de Aplicación 202.

[0060] Una modalidad preferida de ejemplo que utiliza un Protocolo de Autenticación de Tres Vías y una Contraseña de una vez como una Secuencia de Codificación de Carácter Hash será ahora descrita con referencia a la figura 3:

- Programa Navegador de Red 210 del Terminal de Cliente 200 accede a la Interfaz de Red correspondiente 214 del Servidor de Aplicación 202 con una solicitud para acceder al Proceso de Aplicación 216.

- La Interfaz de Red 214 del Servidor de Aplicación 202 responde con una información de pantalla "LOG-IN" e instrucciones relacionadas para acceder al proceso de Aplicación 216.

- El Terminal de Cliente 200 instruye a procesador ISO 112 para activar el Procesador de Seguridad 114.

- El Procesador ISO 112 dispara el Procesador de seguridad 114.

- El Procesador de Seguridad 114 espera los Datos de la Huella Digital provenientes del Sensor de Huella Digital 110 y cuando los datos validados son recibidos, extrae un Patrón de Huella Digital que es enviado al Programa Navegador de Red 210 por vía del Procesador ISO 112.

- El Programa Navegador de Red 210 envía una versión cifrada del Patrón de Huella Digital extraído al Servidor de Autenticación 204 acompañado por (o cifrado con) Información relacionada a cerca de la Tarjeta involucrada 100' y el Lector de Tarjeta 208, tal como el ID de Usuario, la dirección IP del Terminal de Cliente 200, y/o el código ID alámbrico (dirección MAC) del Sensor 110.

- La Interfaz de Red 220 del Servidor de Autenticación 204, luego de recibir el Patrón de Huella Digital extraído junto con la otra información del Terminal de Cliente 200 envía esa información al Procesador de coincidencia de Huella Digital 222.

- Bajo el control del Software de Coincidencia 224, el Procesador de Coincidencia de Huella Digital 222 utiliza el ID de Usuario recibido u otra información relacionada específica de usuario para recuperar un Patrón de Huella Digital de referencia correspondiente de la Base de Datos 226

y compara el Patrón de Huella Digital capturado con el Patrón de Huella Digital de referencia.

- El resultado (Coincidente o no Coincidente) es almacenado en un registro Histórico de Acceso junto con la información Relacionada que identifica el Terminal 200, la Tarjeta ID de Usuario 100' y la Aplicación de solicitud 216, y el control es regresado a la interfaz de Red del Servidor de Autenticación 220.

- Si el resultado es Coincidente, la Interfaz de Red del Servidor de Autenticación 200 genera entonces una contraseña de Una vez en la forma de una Secuencia de Carácter de desafío que es transmitida al Terminal de Cliente 200, y utiliza esa Secuencia de Carácter de Desafío como un código Hash para encriptar la información Relacionada que este guarda como la respuesta de Desafío correspondiente para posible futura referencia.

- El Terminal de Cliente 200 utiliza la Secuencia de Carácter de Desafío recibida como un código Hash para cifrar una copia no cifrada previamente Relacionada de la información Relacionada suministrada, que esta entonces envías a la Interfaz de Red 214 del Servidor de Aplicación 202 como parte de su respuesta al Proceso de Inicio de la sección de la aplicación.

- La Interfaz de Red 214 del Servidor de Aplicación 202 luego de recibir la Información Relacionada convertida Hash, la envía al servicio de Aplicación 216 que la asocia con un intento de inicio de sesión en Proceso del Servidor del Cliente, y, con el propósito de confirmar el resultado Coincidente, envía la Información Relacionada recibida que comprobada por el Terminal de Cliente utilizando la secuencia de Desafío suministrada por el Servidor de Autenticación como respuesta de Desafío.

- La Interfaz de Red 220 del Servidor de Autenticación 204, luego de recibir la Respuesta de Desafío del Servidor de Aplicación, envía esa Respuesta al Proceso de Autenticación 222 que lo compara con la copia de referencia Previamente guardada de la Respuesta de Desafío esperada para determinar si la identidad del usuario ha sido de hecho autenticada.

- Cualquier información de Identidad de Usuario autenticada proveniente de esa comparación es luego regresada al Proceso de Aplicación 216 por vía de la internase de Red del Servidor de Autenticación 220 y la Interfaz de Validación 218 del Servidor de aplicación 202.

- La Interfaz de validación 218 utiliza la Autenticación para confirmar la Identidad del Usuario como se estableció en el intento de conexión original ha sido validada.

- Una vez que la Identidad del Usuario ha sido confirmada, El proceso de Autenticación 216 procede entonces a comunicarse directamente con el programa Servidor de Red 210 del Terminal de Cliente 200 por vía de la Interfaz de Red 214 del Servidor de Aplicación 202.

[0061] La figura 6 ilustra un proceso de autenticación alternativo en el cual todas las coincidencias son desarrolladas sobre la tarjeta compatible ISO de la figura 4 mediante la CPU de Seguridad 114 y ningún Servidor de Autenticación externo 204 es utilizado. El lado izquierdo de la figura 6 muestra las funciones desarrolladas por el Servidor de Aplicación 202, aunque el lado derecho muestra las funciones desarrolladas por la SmartCard ISO 100.

[0062] Cuando la SmartCard 100 es insertada en Lector de Tarjeta 208, un RST de señal reestablecida es enviada desde el lector de tarjeta tanto a la ISO CPU (bloque de INICIO 502) y CPU Huella Digital 114 (bloque de Verificación de Huella Digital 504) y ambos reciben energía VCC del Lector de Tarjeta 208. La ISO CPU responde entonces con un mensaje ATR (Respuesta a Reinicio) y comunica un PPS (Selección de Protocolo y Parámetros) según sea necesario (bloque 506). Al mismo tiempo, la CPU de Huella digital da hacia el estado de espera para recibir los datos de Huella Digital y cuando los datos son recibidos del sensor 110, desarrolla el proceso de autenticación (bloque 504).

[0063] Cuando un comando de solicitud iniciales enviado mediante la Aplicación 216 a la ISO CPU 112 (bloque 508) la ISO CPU consulta (bloque 510) la CPU de seguridad a cerca del estado de autenticación. Si la respuesta es positiva, la ISO CPU responde la aplicación al ejecutar el comando solicitado (bloque 512). De otra manera (un mensaje de error o ninguna respuesta de la CPU de Seguridad 114) ésta no genera ninguna respuesta del comando solicitado sino en su lugar espera para una nueva primera solicitud (bloque 508b).

[0064] Asumiendo que la Huella Digital fue verificada y la primer respuesta fue recibida a tiempo y se determinó como una respuesta de la Aplicación 216 (bloque 514), el proceso de Solicitud/Respuesta continua (bloques 516, 518, 520) hasta que un tiempo de expiración de verificación predeterminado ha sido excedido durante el cual ninguna solicitudes fueron recibidas de Aplicación (bloque 522), o la Aplicación falló en recibir una respuesta esperada (bloque 524).

[0065] La figura 7 es similar al diagrama de flujo de la figura 6, pero modificada para uso con la tarjeta de verificación biométrica de ejemplo de la figura 5. El lado izquierdo lejano de la figura muestra las funciones desarrolladas por el Servidor de Aplicación 202, la siguiente columna corresponde al Lector 208, la siguiente columna describe los contactos ISO 108, la siguiente columna muestra las funciones desarrolladas por la CPU de Seguridad 114,

aunque el lado derecho lejano muestra las funciones desarrolladas por una CPU SmartCard ISO modificada 112.

- Cuando una SmartCard es insertada en un lector de tarjeta o un software de aplicación inicia la operación del dispositivo lector de tarjeta, una Señal de Restablecimiento 550 es enviada desde el Lector de Tarjeta 208 a la CPU de Seguridad 114.

- Tan pronto después de que la CPU de Seguridad recibe La Señal de Restablecimiento 550, ésta envía una Señal de Restablecimiento correspondiente 552 a la ISO CPU 112. Concurrentemente la CPU de Seguridad espera los datos de Huella Digital del Sensor de Huella Digital.

- Luego de recibir la Señal de Restablecimiento 552, la ISO CPU elabora una respuesta ATR (Respuesta a Restablecimiento) 554 y posteriormente comunica el PPS (Selección de Protocolo y Parámetro) según sea necesario.

- Tan pronto como la CPU DE seguridad 114 recibe el ATR (Respuesta a Restablecimiento) de la ISO CPU, la transfiere al Lector de Tarjeta (bloque 556), que incluye cualquiera de los comandos asociados PPS.

- Mientras tanto, si la CPU de Seguridad recibe los datos de huella digital, ésta ejecuta el proceso de autenticación previamente descrito. En el evento en que el

ensayo de autenticación resulte en un PASO, este estado de paso es mantenido durante un periodo de tiempo específico. Si el resultado FALLA, la CPU de Seguridad 114 espera nuevos datos de huella digital.

- Luego de la ejecución de la aplicación, una solicitud de comando 558 es enviada a la CPU de Seguridad para transferir también su respuesta correcta 560 ISO CPU y también transferir su respuesta correcta 562 al Lector de Tarjeta solamente si la CPU de seguridad está aún en el estado de PASO previamente mencionado o si la última respuesta correcta tiene un conjunto de bit de más datos (bloque de prueba 564).

- De otra manera (no rama 566) la CPU de Huella Digital genera una solicitud ficticia 568 y la transfiere a la ISO CPU y también transfiere la respuesta ERR resultante 570 al Lector de Tarjeta 216, manteniendo de esta manera una sincronización adecuada entre los números de secuencia entre las solicitudes y las respuestas.

Cifrado y Seguridad

[0066] Antes de la transmisión sobre cualquier red externa, cualquiera de los datos sensibles y/o el resultado de autenticación es preferiblemente cifrado, posiblemente utilizando DES, o un cifrado de "Two Fish". La clave de cifrado puede estar basada en datos de huella digital

capturados o almacenados, un código ID de usuario, un código únicamente asignado de sensor, una dirección de memoria, unos datos adyacentes en la memoria, otros datos relacionados de funcionalidad, una conversión previa (transacción), una dirección IP, un código de terminal, o una contraseña asignada. Alternativamente, los datos sensibles pueden ser enviados por Internet utilizando un protocolo HTTPS seguro.

[0067] Para suministrar aún mayor seguridad, una puerta de enlace privada Virtual, tal como el cifrado y descifrado DES de hardware, pueden ser insertados entre el Servidor de Autenticación de Huella Digital Seguro y la conexión de red, y correspondientemente entre el Servidor de Servicio de Aplicación y la conexión de red. De esta manera utilizando tal puerta de enlace Virtual o Red Privada Virtual ("VPN"), los datos sensibles son adicionalmente protegidos mediante una capa adicional de cifrado, por ejemplo tanto de DES 128 (típicamente utilizado en el VPN) como RSA (utilizado por el HTTPS).

[0068] Para aplicaciones especialmente seguras, todas las comunicaciones fueron envueltas con capas adicionales de seguridad. En particular, los encabezamientos de mensajes en una capa inferior pueden ser cifrados en una capa superior.

[0069]

Comunicación Inalámbrica

[0070] Otras modalidades pueden incluir una Interfaz doble tanto para contacto (ISO 7816) y operación inalámbrica (ISO 1443 A o B), y preferiblemente incorporan una unidad de energía multi-interfaz que permite la interoperabilidad entre el contacto ISO 7816, ISO 1443 A, ISO 1443 B, ISO 15693 y los sistemas inalámbricos de legado HID (entre otros) TODOS EN UNA TARJETA. Alternativamente, la tarjeta puede incluir el suministro de otras tecnologías de comunicaciones inalámbricas tales como la Bluetooth (de rango corto) o celular (rango medio) o microondas (rango largo).

[0071] Se hace ahora referencia la figura 8 que muestra una tarjeta inteligente con una verificación biométrica a bordo que puede ser conectada a un terminal local bien sea inalámbricamente o por medio de un conector eléctrico. Para la mayor parte es similar en construcción y arquitectura a la modalidad previamente descrita de la figura 1, y los números similares (posiblemente distinguidos por unas "simple") designan elementos similares. En particular, la ISO CPU 112 es mostrada en una localización diferente (inferior en lugar de un lado de contactos 108), pero que tiene una funcionalidad similar como se describió previamente.

[0072] La antena ISO 132 comprende dos bucles generalmente localizados alrededor de la periferia de la tarjeta 100 y suministran una interfaz inalámbrica compatible con ISO a la

ISO CPU 112 tanto para datos como energía similar a la lograda por la interfaz eléctrica alámbrica 108. Además, la antena de seguridad 134 (en el ejemplo descrito, la antena interna 132 y consistentemente de solamente un bucle) suministran una fuente separada de energía a la CPU de Seguridad 114 por vía del regulador de energía DC-DC 120. En razón a que no existe una conexión directa para datos inalámbricos excepto a través de la ISO CPU 112, los datos sensibles almacenados dentro de la CPU de Seguridad 114 no están comprometidos por tal interfaz inalámbrica. Alternativamente, como se mencionó previamente con respecto a las modalidades que solo tienen conexiones alámbricas al lector externo y la red externa, la funcionalidad de dos procesadores puede ser combinada, o la interfaz externa puede ser a través de la CPU de Seguridad 114 en lugar de la ISO CPU 112, en la cual medidas de seguridad inalámbricas apropiada tendrían que ser incorporadas dentro de la arquitectura así modificada.

[0073] La figura 9 es una sección transversal a través de la tarjeta de la figura 8, Nótese que la mayoría de los componentes descritos están contenidos dentro del núcleo central, 126, con solo tabletas de contacto 108 que se extienden a través de la capa protectora superior 122. El área operativa de sensor 110 es accesible a través de la ventana superior en la capa superior 122 y una ventana inferior en la PCB 134 que está dispuesta entre la capa superior 122 y el núcleo central 126 y que suministran las

conexiones eléctricas requeridas entre los varios componentes electrónicos, así como también un contacto de tierra de descarga electrostática circundante que circunda en la región activa del sensor 110.

[0074] También es visible una capa inferior 124 y una tira magnética 128.

Sensor de Huella Digital

[0075] La figura 10 es un diagrama de un circuito esquemático de ejemplo para el sensor 110, en la cual está dispuesta una disposición 400 de las celdas del sensor 402 en filas 404 y columnas 406. Como se describió, cada celda 402 incluye una puerta de activación 410 y un transductor 412. Una Huella Digital se transforma entre las crestas y valles de la piel sobre un dedo. Cada transductor de celda de sensor 412 experimenta un cambio mecánico y/o eléctrico cuando una de estas crestas toca la vecindad inmediata de la celda 402 dentro de la disposición 400, que el efecto suministra una imagen de huella digital en forma digital con base en las variaciones de micro-presión a través de la superficie del sensor originada por las crestas y los valles en la punta del dedo. Nótese que aunque cada transductor 412 ha sido descrito como un capacitor de variable simple, existen varios tipos de transductores que puedan responder a la presencia de una de estas crestas de la piel humana: en el ejemplo particular de un transductor de película delgada piezo sensible de presión,

la película es deformada en la vecindad de la celda y genera una carga que es almacenada en un capacitor conectado a esa celda. El voltaje en el capacitor es así una función de la tensión mecánica formada por la deformación del material piezo, que a su vez es una función de si una montaña o un valle está próximo a la celda. Cuando una señal de un manejador de columna asociado 414 ENCIENDE la puerta de la celda 410 y el manejador de hilera asociado 416 es puesto en tierra, ese voltaje aparece en la línea de salida de la hilera 418, y es convertido a una señal digital de 8 bits en el manejador de Salida 420. Para maximizar la detección de la deformación del material piezo, el material eléctrico piezo puede ser conformado de un material elástico, tal como poliimida o puede ser simplemente un material eléctrico piezo de poliimida. Otras analogías de transductor análogo d ejemplo que pueden ser implementadas con una organización de disposición similar incluyen resistencia variable y capacitancia variable. Alternativamente cada celda podría consistir de un interruptor digital simple que suministra solamente un bit simple de información, en ese caso, los bits adicionales de información pueden ser generados al suministrar más celdas en la misma área o al muestrear cada celda a una frecuencia mayor. Tal modalidad alternativa evita la necesidad de cualquier convertidor A/D.

[0076] En una modalidad de ejemplo, el sensor es solamente de 0,33 mm de grueso y suficientemente durable para ser empotrado en una SmartCard y no se afecta por la electricidad

estática, los elementos o la condición (húmedo, seco, caliente, frío) de la piel de usuario. Un tamaño de celda unitario típico del Sensor 110 es de 25 micrómetros a 70 micrómetros y un tono típico es de 25 micrómetros a 70 micrómetros. Un sensor de ejemplo tiene un área sensible de un cuadrado de 12,5 mm a 25 mm y un multinivel de 8 bits de sensibilidad. Tal sensor puede ser elaborado mediante una disposición de un capacitor sensible TFT (Transistor de Película Delgada) y Presión, tal como el formado por el Material Piezo de Película Delgada, tal como el Óxido de Titanio Bario o el Oxido de Estroncio Bario, e incluye un electrodo superior que cubre y protege el área sensible y completa. Si se aplica tensión mecánica, una carga correspondiente se genera y se almacena en el Capacitor Piezo de Película Delgada. Alternativamente, el sensor basado en presión puede ser elaborado como una disposición de TFT (Transistor de Película Delgada) junto con un capacitor de película delgada, y el capacitor sensible a Presión, tal como el formado por la lámina de material conductor de presión, tal como la lámina de caucho dispersada de fibra de carbono, metal (tal como cobre o estaño o plata), fibra de carbono plateada o papel basado en fibra de vidrio, o metal, o un material elástico dispersado (tal como silicona), o una lámina de electrodo superior, que cubre el área sensible completa.

[0077] Los manejadores de fila y columna 416, 414 cuyo elemento sensor de huella digital especificado particular 402

está sacando los datos eléctricos al circuito de salida 420 convierten de esta manera la entrada física representativa de la huella digital del usuario a datos eléctricos análogos. Un convertidos A/D en el circuito de SALIDA 420 convierte entonces la señal eléctrica análoga a una señal eléctrica digital. Cada transistor de película delgada cambia selectivamente una interconexión de hilera compartida al voltaje sobre su capacitor asociado, así el voltaje en cada capacitor puede ser leído y de esta manera cada información de celda puede ser leída. Una columna completa de transistores de película delgada es preferiblemente conmutado simultáneamente y así un número de celdas (por ejemplo 8) en una columna seleccionada pueden ser leídos en paralelo sobre diferentes interconexiones de hilera. La interconexión de múltiples puertas como hileras y columnas reduce el número de interconexiones, aunque la lectura paralela de múltiples celdas provenientes de diferentes hileras de la misma columna reduce el tiempo de lectura para la disposición completa. El voltaje de salida del sensor puede ser amplificado por un amplificador diferencial. La salida de tal amplificador puede ser muestreada y mantenida para una Conversión Análoga a Digital (convertidor A/D).

[0078] El sustrato puede ser vidrio (tal como un vidrio no alcalino), acero inoxidable, Aluminio, Cerámicas (tal como Óxido de Aluminio), Papel, Epoxi de Vidrio, pero es preferiblemente una lámina delgada de Silicio de Cristal. El material semiconductor de película delgada puede ser Silicio

Morfo, Polisilicio, Diamante, o cualquier otra película delgada semiconductor. El Material Piezo eléctrico puede ser una cerámica piezo eléctrica, tal como películas delgadas de plomo-Zirconato -titanato (PZT), que varían preferiblemente en el grosor de 0,1 a 50,0 micrómetros, o un material de película delgada de poliimida piezo eléctrico polimérico. El material de interconexión puede ser: Ti/Ni/Cu, Al, Cr/Ni/Au, Ti/Ni/Au, Al/Au, W/Cu, W/Au, W/Au.

[0079] La figura 11 muestra un montaje de portadora para un sensor formado sobre un sustrato delgado de silicio cristalino. El silicio cristalino tiene excelentes propiedades eléctricas y facilita la integración de la disposición del sensor con el manejador requerido y los circuitos de salida. Sin embargo, una lámina relativamente grande y delgada de silicio se flexionará y se fracturará cuando es sometida a una presión de superficie localizada. El portador ilustrado suministra una estructura mucho más rígida que la que se suministraría con la lámina de silicio del mismo grosor total.

[0080] Como se muestra, la lámina monolítica de silicio 430 es de aproximadamente 0,1 mm de grosor, y está circundada por una estructura igualmente gruesa 432 de epoxy de vidrio, que está montada en el plato de respaldo 434 también de construcción de epoxi de vidrio y aproximadamente 0,05 mm de grosor. La estructura 432 y el plato de respaldo 434 pueden ser fácilmente contruidos utilizando una tecnología de

tarjeta de circuito impresa convencional (PCB). En particular, la superficie superior e inferior del plato de respaldo 434 están cubiertas con una capa de cobre delgada 436 separada por un núcleo epoxi de vidrio. La estructura 432 incluye un número de tabletas soldadas 440 alrededor de su periferia, para conexión al Procesador de Seguridad 114. El chip de silicio delgado 430 es unido con epoxi a la estructura 432 y al plato 434, y las regiones activas están eléctricamente acopladas a las trazas eléctricas respectivas en la estructura 430 mediante una unión con alambre convencional 442 en las porciones de borde exterior expuestas 444 del silicio 430 que circunda el electrodo superior protector 446.

Algoritmos de Coincidencia

[0081] Para el procesamiento a bordo local donde la energía de procesamiento está limitada y solamente una coincidencia simple 1:1 con una muestra de referencia simple está siendo intentada, el software de coincidencia de huella digital puede estar basado en una comparación relativamente directa de minucias derivadas de los dos patrones. Por ejemplo, las imágenes de escala de grises de una huella digital puede ser reducida a dos valores blanco y negro, crestas tridimensionales son convertidas en líneas delgadas bidimensionales (vectores). La predicción del método está por lo tanto sometida a, entre otros problemas, nitidez, aglutinación, distorsión, seguro parcial de los segmentos de

línea y otros efectos. Aunque el método de minucias es en principio menos preciso, este requiere menores recursos computacionales y ofrece la posibilidad de compatibilidad con muchas bases de datos existentes.

[0082] Para procesar en un servidor de autenticación remoto donde más energía de procesamiento está disponible y más discriminación precisa se puede requerir, por ejemplo un algoritmo de coincidencia "POC" (Correlación de Solo Fase). La POC es un algoritmo de identificación basado en coincidencia macroscópica de imágenes completas. El POC al contrario, hace coincidir información estructural en un rango amplio -desde detalles a la imagen total. De esta manera, el POC es capaz de suministrar precisión robusta contra ruidos tales como aglutinación y actos parciales. En principio, el método POC está libre de defectos adversos de cambios posicionales y diferencias en brillo, es rápido (aproximadamente 0,1 segundo de una coincidencia fuera de línea) y altamente preciso. Por ejemplo, el software POC puede desarrollar una comparación de frecuencia de espacio de los dos patrones de huella digital que utilizan una Transformación de Primer Furier dimensional ("2DFFT"). El 2DFFT convierte una disposición de datos digitalizados que representan una distribución bidimensional física de huella digital en espacio de frecuencia, en otras palabras, la distribución de espacio inverso, donde el patrón de mayor densidad tiene mayor frecuencia de espacio. Una transformación rotacional se puede utilizar para hacer

coincidir la coincidencia de patrón de espacio de frecuencia. El patrón POC que coincide tiene la coincidencia de vector de Minucias de ventaja adicional, por que este no es engañado por defectos comunes en el patrón de huella digital registrado cuyo POC reconocería como ruido pero un análisis de Minucia interpretaría como dato significativo.

[0083] Para aplicaciones particularmente demandantes, una aproximación híbrida puede ofrecer aún mayor precisión y seguridad que cualquier método solo. Por ejemplo, una metodología de minucias se puede utilizar en el punto de captura, aunque la metodología POC se puede utilizar en un servidor remoto. Como otro ejemplo, el proceso de coincidencia puede analizar tanto las donaciones de minucias como la espacial para producir una calificación combinada que tenga en cuenta los resultados de ambos.

Aplicaciones

[0084] La tecnología anteriormente descrita suministra un alto nivel de seguridad para aplicaciones múltiples, tanto comerciales como gubernamentales. Dependiendo de los requisitos de cada aplicación, las aplicaciones seguras múltiples pueden coexistir y operar en la misma tarjeta y/o en el mismo servidor de autenticación. En una modalidad, una tarjeta siempre puede contener hasta 24 aplicaciones independientes y seguras. Por ejemplo, la terminología permitirá/denegará acceso (físico y/o lógico), identificará

sitio preciso y/o movimiento de personal y/o revisará partes de lista aunque al mismo tiempo operando otras aplicaciones seguras, cada una completa y seguramente aislada de la otra.

[0085] Entre las aplicaciones habitualmente contempladas están las siguientes:

- ID/acceso aeropuerto
- Seguridad de construcción
- Acceso y cuentas Habitaciones de Hotel
- Hospital
- Juegos en Línea
- Entretenimiento descargado
- Certificados de nacimiento
- Acceso a computadora
- Licencia de conducción- TWIC
- Billetera electrónica
- Información médica de emergencia
- Licencia de explosivos
- Acceso a Instalaciones Gubernamentales Militares
- Licencia HAZMAT
- Tarjeta de cuidados médicos y beneficios
- acceso a parqueadero,
- pasaporte
- licencia de piloto
- ID/acceso a puerto
- prueba de seguro,
- Tarjeta de seguridad social,

- Tarjeta de viajero confiable,
- pases de visa o de entrada/salida
- Tarjeta de Registro de votante
- Tarjetas con estampilla.

[0086] Para muchas de estas aplicaciones, la memoria a bordo de la tarjeta preferiblemente también suministra almacenamiento seguro de varias clases de información personal privada, que es accesible solamente cuando el portador registrado a probado su identidad y autorizado tal acceso. Ejemplos de tal información privada son:

- Información administrativa tal como nombre, dirección, fecha de nacimiento, lugar de nacimiento, nacionalidad, religión, membresías organizacionales, números de seguridad social, números de licencia de conducción, número de pasaporte, información de inmigración tales como tipo de visa, expiración de la visa, ciudadanía, etc.

- Información financiera, tal como billetera eléctrica, Visa, MasterCard, American Express, etc. Información de tarjeta de crédito, información bancaria tal como nombre del banco, balance del banco, información de transferencia de dinero, número IRS, record de quiebras, información y transferencia de dinero, etc.

- Información fisiológica o de salud tal como: información biométrica para identificar individuos tales como

altura, peso, huellas digitales, iris, retina, tamaño de la mano, estructura de los huesos, voz, ADN; tipo de sangre; resultados de prueba de diagnóstico médico; historia médica; medicaciones; información de seguros; respuestas psicológicas y fisiológicas a ciertos estímulos, etc.

- Información de eventos tales como registro criminal, felonía, mala conducta, infracciones.

- Información de de emergencia tal como cementerio, familiares y otra información de contacto, información de abogado, información religiosa, educación, historia de trabajo, incluyendo escuela a la que se asiste, grado, compañía con la que se trabaja relacionada con FDD.

- Historia de acceso de datos (almacena los datos de historia de acceso a entrada y salida de tarjetas).

- Información relacionada con ID tal como patrón de huella digital, patrón de huella digital procesada, resultados de patrón de huella digital.

- Contraseñas tales como contraseña permanente, o una contraseña temporal, y/o una contraseña de una vez.

- Claves de cifrado tales como una clave pública, una clave personal, y/o una clave de una vez.

[0087] Un ejemplo de un sistema de tarjeta sería descrito ahora.

[0088] El solicitante: llena una solicitud y la entrega, preferiblemente incluyendo una fotografía y huella digital. Para la mayoría de los solicitantes, una inspección de sus documentos de nacimiento y una revisión simple de la información suministrada contra una o más bases de datos gubernamentales o comerciales disponibles debe ser suficiente para establecer la identidad cierta del individuo.

[0089] Después que su identidad ha sido así verificada, el solicitante procede a una estación de emisión donde cualquier información que se considere necesaria por el emisor de la tarjeta es cargada en la tarjeta. El solicitante pone su huella digital en el sensor sobre la tarjeta. Una vez que la huella digital es satisfactoriamente ubicada en el sensor y cargada en la tarjeta, la lengüeta en la tarjeta entonces un golpe de electricidad que quema ciertos fusibles que evitan que cualquiera escriba en cierta área de la tarjeta de nuevo. Entonces, las pequeñas lengüetas se cortan/guillotinan (como un cordón umbilical). En ese momento, la tarjeta puede ser solamente leída o escrita a través de un lector de contacto ISO o un sistema inalámbrico ISO.

[0090] En el caso de un servidor de Autenticación en red, algunos o todos los mismos datos que sean cargados en la tarjeta son también transmitidos en forma encriptada al

servidor remoto, posiblemente suplementado con datos adicionales que no son normalmente almacenados en la tarjeta pero que pueden ser solicitados por ciertas aplicaciones de alta seguridad.

REIVINDICACIONES

1. Una tarjeta de identificación inteligente que comprende:

Una memoria a bordo para almacenar datos de referencia,
Un sensor a bordo para capturar los datos biométricos vivos,
Un microprocesador a bordo para comparar los datos biométricos capturados con los datos de referencia correspondientes almacenados dentro de un umbral predeterminado y para generar un mensaje de verificación solamente si hay una coincidencia en un umbral predeterminado, y
Medios para comunicar el mensaje de verificación a una red externa.

2. La tarjeta de identificación de la reivindicación 1 donde el mensaje de verificación incluye al menos extracción de los datos de referencia almacenados.
3. La tarjeta de identificación de la reivindicación 2 en donde el mensaje de verificación incluye al menos extracciones de los datos biométricos capturados.
4. La tarjeta de identificación de la reivindicación 3 en donde el mensaje de verificación es transmitido a

un sistema de autenticación remoto para verificación adicional.

5. La tarjeta de identificación de la reivindicación 4 en donde el sistema de autenticación remoto incluye datos de referencia remotamente almacenados que son diferentes de los datos de referencia localmente almacenados.
6. La tarjeta de identificación de la reivindicación 4 en donde el micro procesador a bordo utiliza un algoritmo de coincidencia diferente a aquel utilizado por el sistema de autenticación remoto.
7. La tarjeta de identificación de la reivindicación 2 en donde el proceso de coincidencia completo es desarrollado por el procesador a bordo y ninguno de los datos biométricos capturados es transmitido en la red.
8. La tarjeta de identificación de la reivindicación 2 en donde tanto los datos biométricos originalmente capturados como cualquier otra información "privada" almacenada en la memoria a bordo no están disponibles a ninguno de los procesos externos.

9. La tarjeta de identificación de la reivindicación 2 donde la tarjeta es compatible con una SmartCard ISO.
10. La tarjeta de identificación de la reivindicación 9 que comprende además un procesador SmartCard ISO.
11. La tarjeta de identificación de la reivindicación 10 en donde el procesador de seguridad utilizado para almacenar y procesar los datos biométricos protegidos está funcionalmente separado del procesador SmartCard ISO por un cortafuego.
12. La tarjeta de identificación de la reivindicación 10 en donde los datos externos a y desde el procesador de seguridad pasan a través de un procesador SmartCard ISO.
13. La tarjeta de identificación de la reivindicación 10 en donde todos los datos externos a y desde el procesador de las SmartCard ISO pasan a través del procesador de seguridad.
14. La tarjeta de identificación de la reivindicación 10 en donde el procesador de seguridad tiene una primer conexión utilizada para cargar datos durante el proceso de carga a una segunda conexión conectada a una red externa.

15. La tarjeta de identificación de la reivindicación en donde la primer conexión es permanentemente deshabilitada después de que el proceso de carga se ha completado.

16. La tarjeta de identificación de la reivindicación 10 en donde el procesador de seguridad utilizado para almacenar y procesar los datos biométricos protegidos está funcionalmente separado del procesador SmartCard ISO por un cortafuego.

17. La tarjeta de identificación de la reivindicación 10 en donde:

La tarjeta comprende una región de tira magnética superior y una región realzada inferior;

El sensor biométrico es un sensor de huella digital; y

El procesador de seguridad, el procesador de SmartCard ISO y el sensor de huella digital están todos localizados en la región media entre la región superior y la región inferior.

18. La tarjeta de identificación de la reivindicación 2 en donde los datos biométricos incluyen datos de huella digital y el sensor es un sensor de huella digital que captura datos de un dedo de usuario ubicado en el sensor.

19. La tarjeta de identificación de la reivindicación 18 e donde la retroalimentación en tiempo real es suministrada mientras el usuario está manipulando su dedo sobre el sensor de huella digital, facilitando de esta manera una ubicación óptima del dedo sobre el sensor.

20. La tarjeta de identificación de la reivindicación 18 en donde el proceso de coincidencia utiliza un algoritmo de coincidencia híbrido que tiene en cuenta tanto las relaciones de minucias como espaciales totales en los datos biométricos capturados.

21. La tarjeta de identificación de la reivindicación 18 en donde el sensor de huella digital comprende una lámina de silicio cristalina soportada por un plato de respaldo.

22. La tarjeta de identificación de la reivindicación 21 en donde el plato de respaldo comprende una capa epoxi de vidrio en sándwich o entre dos capas de metal.

23. La tarjeta de identificación de la reivindicación 18 en donde el plato de respaldo es reforzado por una

estructura portadora que circunda la lámina de silicio.

24. La tarjeta de identificación de la reivindicación 1 en donde la tarjeta comprende además medios para restringir el uso de la tarjeta a un sitio predeterminado, al menos algunos de los capturaos.

25. La tarjeta de identificación de la reivindicación 1 en donde al menos algunos de los datos biométricos capturados y los datos de referencia son transmitidos a un servidor de autenticación separado para asegurar la verificación de la identidad del usuario antes de que sea otorgado acceso en línea a un servidor de aplicación para procesar transacciones financieras seguras que involucran ese usuario.

26. La tarjeta de identificación de la reivindicación 25 en donde en respuesta a una solicitud de coincidencia que relaciona un intento de acceso particular a un servidor de aplicación particular que produce una coincidencia positiva en el servidor de autenticación, un protocolo de autenticación de tres vías seguro es ejecutado en el cual la frecuencia de carácter de desafío es enviada del servidor de autenticación a la tarjeta de identificación como, o en la medida en que la

tarjeta de identificación entonces utiliza la secuencia del carácter de desafío y la coincidencia solicita generar una respuesta de desafío que esta entonces envía al servidor de aplicación, el servidor de aplicación entonces envía la respuesta de desafío al servidor de autenticación, que entonces verifica si la respuesta de desafío es válida.

27. La tarjeta de identificación de la reivindicación 1 en donde la salida de la tarjeta es utilizada para obtener acceso físico a un área segura.

28. La tarjeta de identificación de la reivindicación 27 en donde un registro de intentos de acceso exitosos y no exitosos es mantenido en la tarjeta.

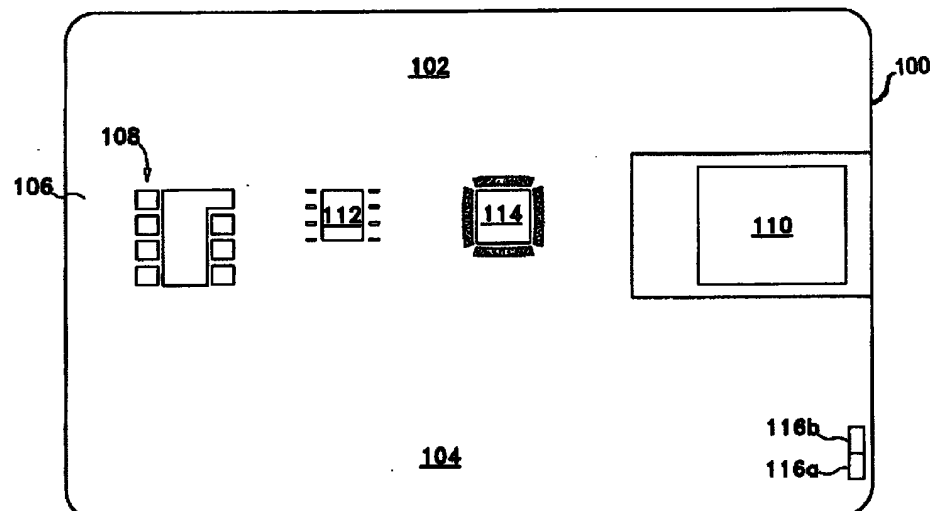


Fig. 1

[Handwritten signature]

118

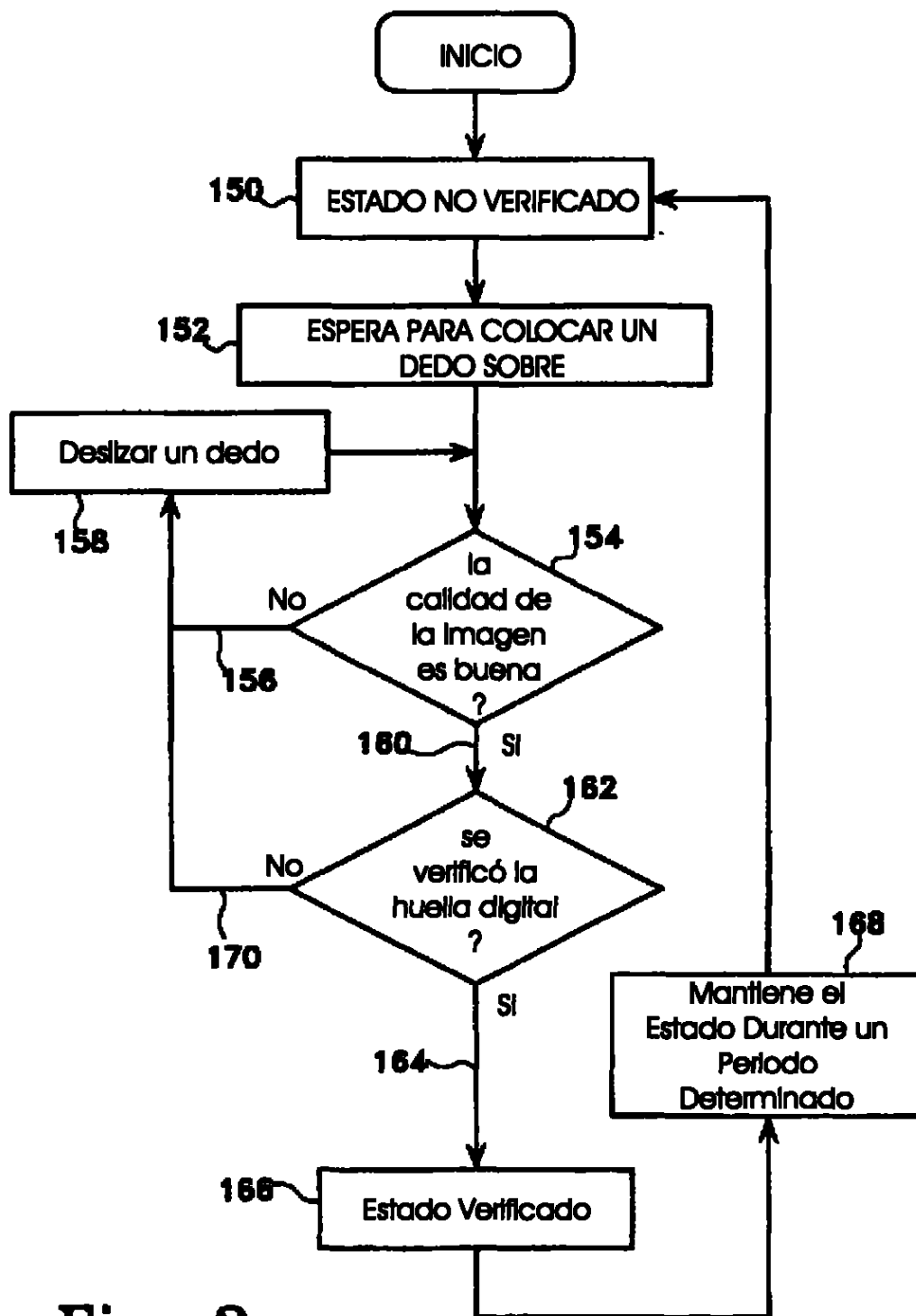


Fig. 2

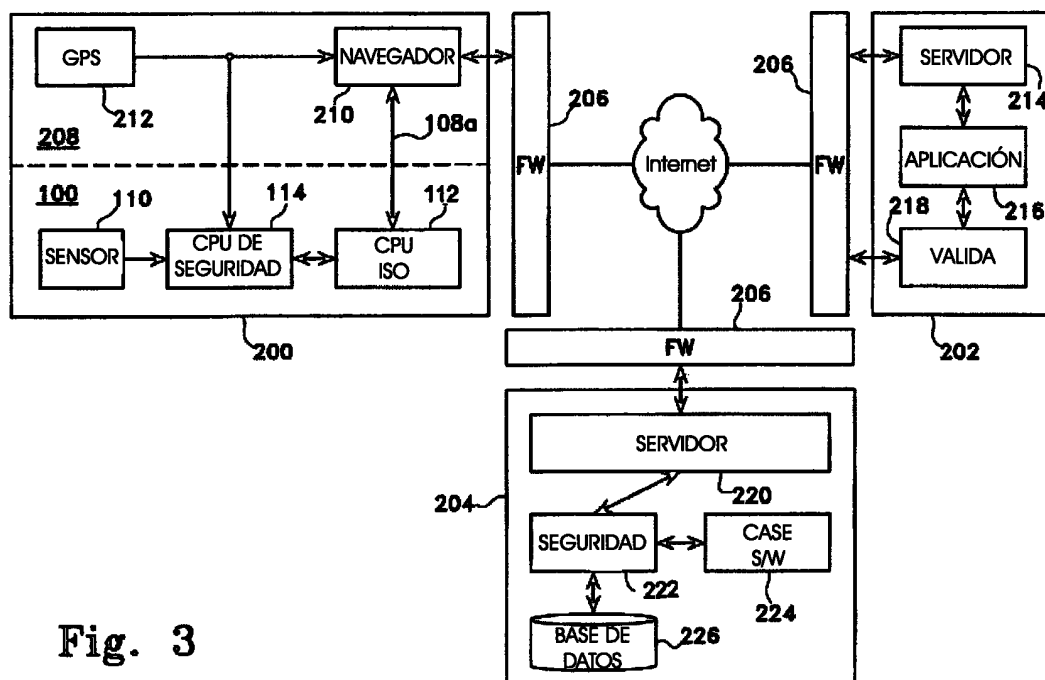


Fig. 3

Handwritten signature or mark.

120

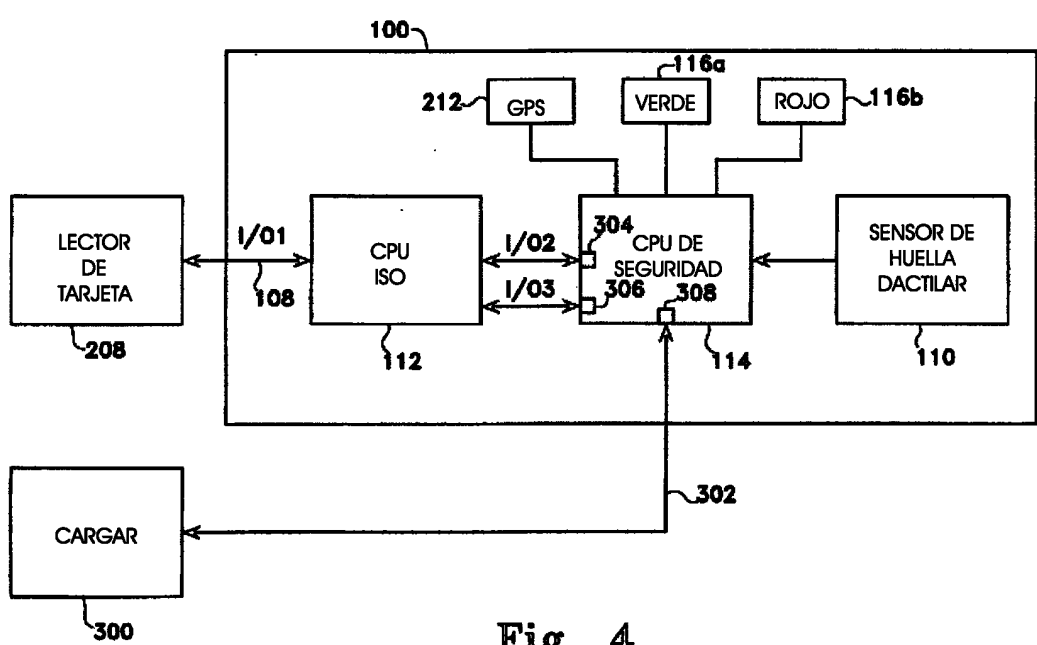


Fig. 4

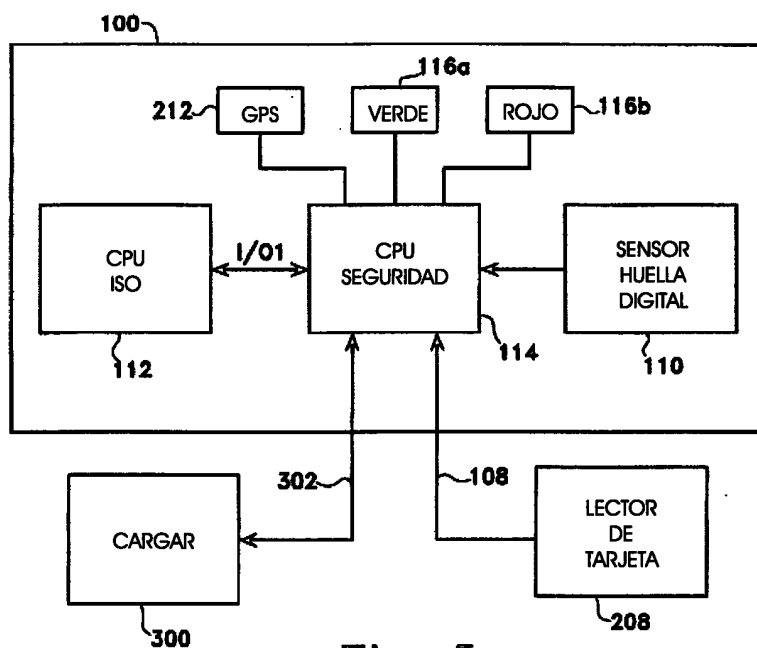
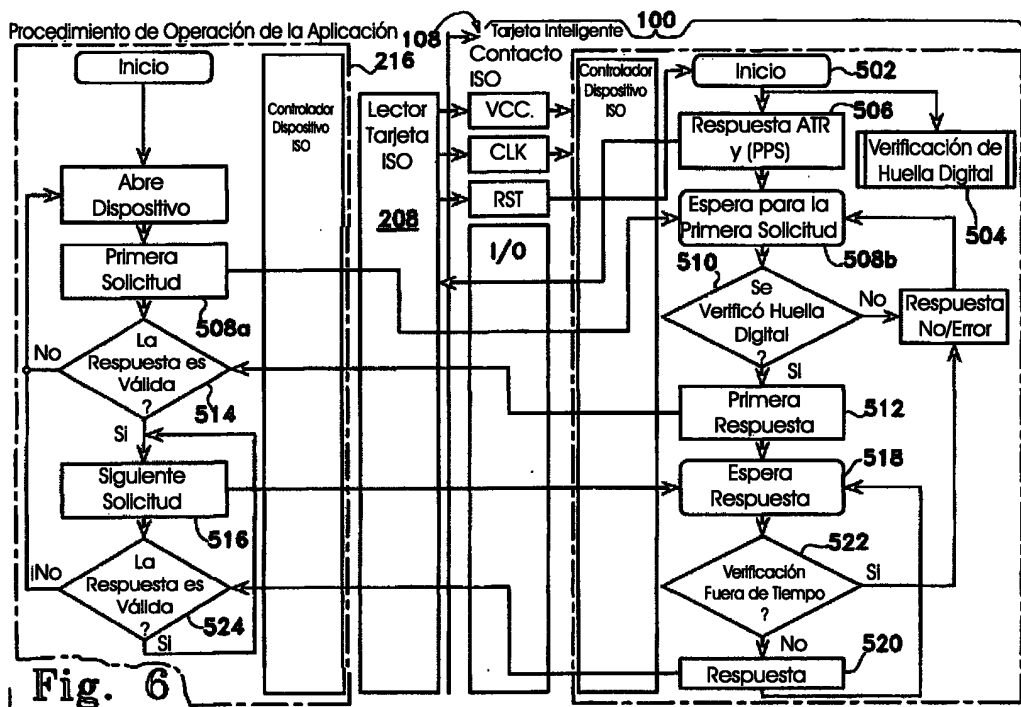
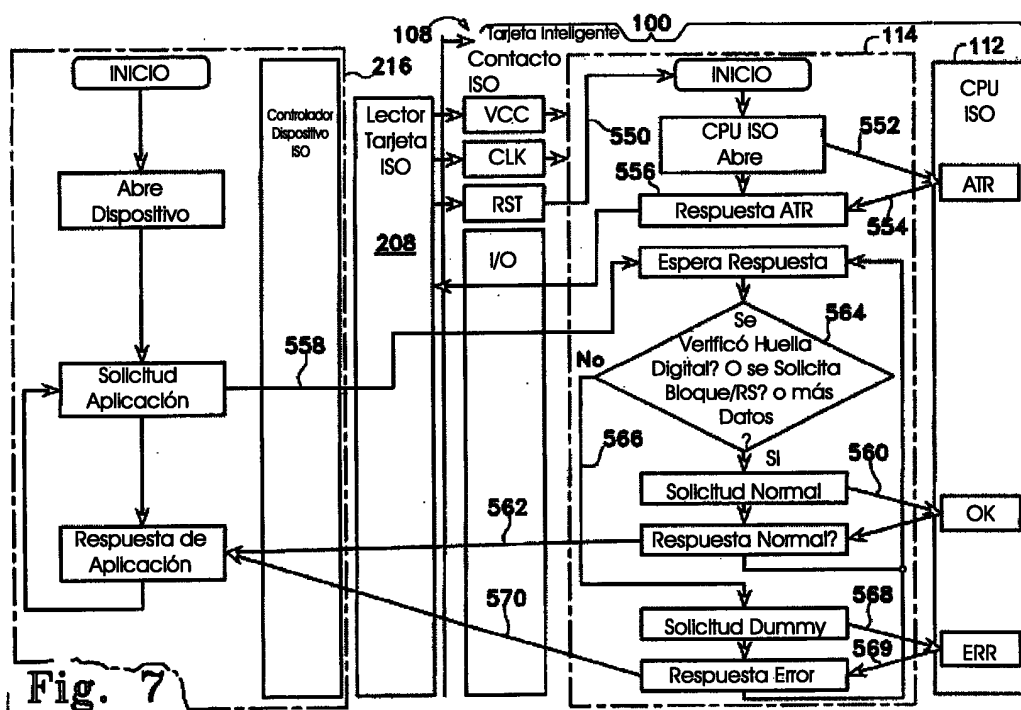


Fig. 5

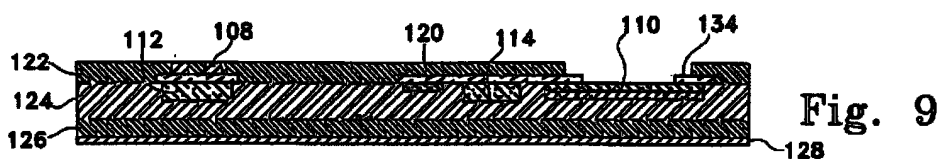
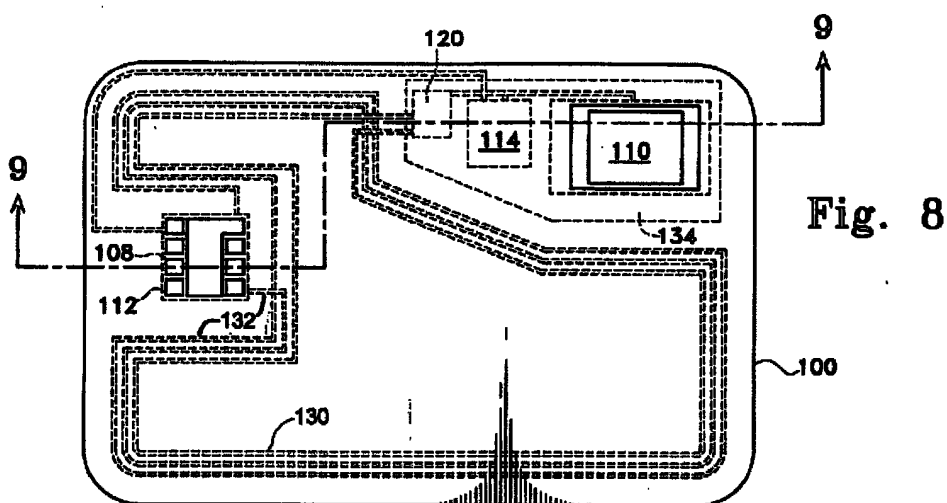
124



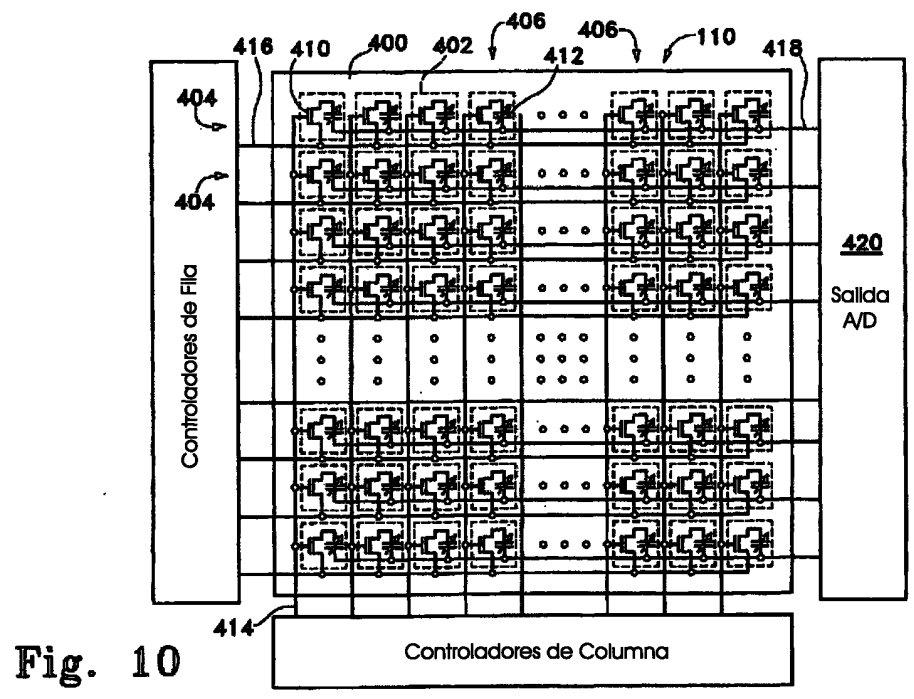
122



123



125



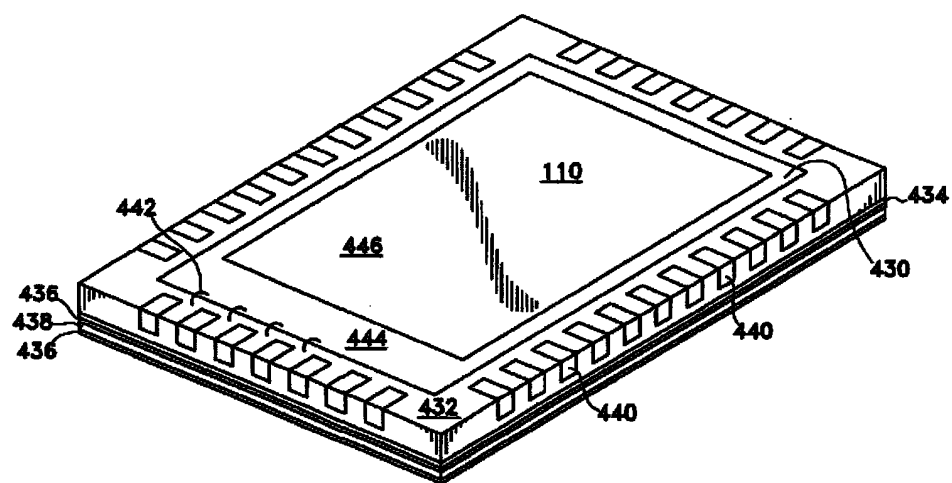


Fig. 11

[Handwritten signature]

127

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800174089-2

RECIBO OFICIAL DE CAJA : 05 - 19,198
FECHA : MARZO 14 DE 2005

SUPERINDUSTRIA Y COMERCIO
Radicación : 05031213 00000000 Folios: 127
Fecha (AMD): 2005-04-07 17:40:49
Trámite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
CAVELIER ABOGADOS	CONSIGNACION	BANCO POPULAR	050-00110-6	41376756	14/03/2005	30,080,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	
1		TRANITES DE SOL. DE PATENTE DE IN	443,000.00
		TOTAL :	\$ 443,000.00

SON: CUATROCIENTOS CUARENTA Y TRES MIL PESOS

RESPONSABLE :



RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

06 14732-841-001-3

128

SUPERINDUSTRIA Y COMERCIO
Radición 6º B de 00000006 Folio 127
Fecha (AMU) 2608 84-07 17 48 49
Trámite 011 PFT-PATENT 379 FASE NACI 411 PRESENTA
Dependencia 020 DIVISION DE NUEVAS CREACIONES

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRAMITE

	USUARIO	RADICADOR
PATENTE DE INVENCION ☒	()	()
Indicación de que se solicita la concesión de una patente	()	()
Datos de identificación del solicitante o de la persona que se presenta la solicitud	()	()
Descripción de la invención	()	()
Dibujos de ser estos pertinentes	()	()
Comprobante de Pago de las tasas establecidas	()	()
COMPLETA ()		
INCOMPLETA ()		
DISEÑO INDUSTRIAL ()		
Indicación de que se solicita el registro de Diseño Industrial	()	()
Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
Representación gráfica o fotografica del Diseño Industrial o muestra del Material que incorpora el diseño	()	()
Comprobante de pago de las tasas establecidas	()	()
COMPLETA ()		
INCOMPLETA ()		
ESQUEMA DE TRAZADO ()		
Indicación de que solicita el registro de un Esquema de trazado	()	()
Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
Representación gráfica del esquema de trazado	()	()
Comprobante de pago de las tasas establecidas	()	()
COMPLETA ()		
INCOMPLETA ()		

Firma Responsable

Claudia M Nueva

Fecha

2020
Bogotá, D.C.,

D ictora:
EMILIO FERRERO
IVI SMART TECHNOLOGIES, INC.
Solicitante

Oficio N°

12776

ASUNTO:	Radicación N°	05-31213
	Solicitud internacional	PCT/US2003/028602
	Fecha limite inicio fase nacional	11/04/2005
	Trámite	011
	Evento	379
	Actuación	430
	Folios	001

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

- Si fuere el caso, el solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT).
- La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486).
- La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.



DORIS ELENA POLO CORDOBA
Jefe de la División de Nuevas Creaciones. (E)

El anterior requerimiento fue notificado por fijación en lista de fecha, 13 MAYO 2005

202030

13 MAY 2004