PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8548927	B2	2013-10-01	Beenau et al.	
	2	8401539	B2	2013-03-19	Beenau et al.	
	3	8126449	B2	2012-02-28	Beenau et al.	
	4	8041815	B2	2011-10-18	Bahl et al.	
	5	8004410	B2	2011-08-23	Martinez de Velasco Cortina et al.	
	6	7980378	B2	2011-07-19	Jones et al.	
	7	7844505	B1	2010-11-30	Arneson et al.	
	8	7671746	B2	2010-03-02	Martinez de Velasco Cortina et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	9	7533809	B1	2009-05-19	Robinson et al.	
	10	7487538	B2	2009-02-03	Mok	
	11	7310734	B2	2007-12-18	Boate et al.	
	12	7225337	B2	2007-05-29	Baessler	
	13	7080819	B2	2006-07-25	Tojo	
	14	7031946	B1	2006-04-18	Tamai et al.	
	15	6975834	B1	2005-12-13	Forster	
	16	6950013	B2	2005-09-27	Scaman et al.	
	17	6894615	B2	2005-05-17	Look	
	18	6850147	B2	2005-02-01	Prokoski	
	19	6793134	B2	2004-09-21	Clark	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	20	6758405	B2	2004-07-06	Look	
	21	6753759	B2	2004-06-22	Stegmaier et al.	
	22	6698653	B1	2004-03-02	Diamond et al.	
	23	6617961	B1	2003-09-09	Janssen et al.	
	24	6570487	B1	2003-05-27	Steeves	
	25	6427504	B1	2002-08-06	Janssen et al.	
	26	6388579	B1	2002-05-14	Adcox et al.	
	27	6360208	B1	2002-03-19	Ohanian et al.	
	28	6340116	B1	2002-01-22	Cecil et al.	
	29	6334059	B1	2001-12-25	Stilp et al.	
	30	6276607	B1	2001-08-21	Sato	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	31	6275157	B1	2001-08-14	Mays et al.	
	32	6269292	B1	2001-07-31	Kokubu et al.	
	33	6268796	B1	2001-07-31	Gnadinger et al.	
	34	6211790	B1	2001-04-03	Radomsky et al.	
	35	6203952	B1	2001-03-20	O'Brien et al.	
	36					
	37					
	38	6182894	B2	2001-02-06	Hackett et al.	
	39	6175922	B1	2001-01-16	Wang	
	40	6167333	A	2000-12-26	GEHLOT; NARAYAN L. et al.	
	41	6157333	A	2000-12-05	Louagie et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	42	6140941	A	2000-10-31	Dwyer et al.	
	43	6111506	A	2000-08-29	YAP; CHAS HOCK ENG et al.	
	44	6104281	A	2000-08-15	HEINRICH; HARLEY KENT et al.	
	45	6098879	A	2000-08-08	TERRANOVA; STEVEN N. et al.	
	46	6073840	A	2000-06-13	MARION; KENNETH O. et al.	
	47	6052068	A	2000-04-18	PRICE R et al.	
	48	6025784	A	2000-02-15	Mish	
	49	6025780	A	2000-02-15	BOWERS; JOHN H. et al.	
	50	5974500	A	1999-10-26	MALETSKY; KERRY D. et al.	
	51	5874896	A	1999-02-23	Lowe et al.	
	52	5864580	A	1999-01-26	Lowe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	53	5787174	A	1998-07-28	TUTTLE JOHN R	
	54	5742618	A	1998-04-21	Lowe	
	55	5657008	A	1997-08-12	Bantli	
	56	5552789	A	1996-09-03	Schuermann	
	57	4529870	A	1985-07-16	CHAUM DAVID	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100095130	A1	2010-04-15	Bertran et al.	
	2	20100094754	A1	2010-04-15	Bertran et al.	
	3	20050149764	A1	2005-07-07	Bahl et al.	
	4	20030200227	A1	2003-10-23	Ressler	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	5	20030074317	A1	2003-04-17	Hofi	
	6	20020109580	A1	2002-08-15	Shreve	
	7	20020089434	A1	2002-07-11	Ghazarian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004006165	WO	A1	2004-01-15	BNC IP SWITZERLAND GMBH		☐
	2	2002042076	JP	A	2002-02-08	DAINIPPON PRINTING CO LTD		☒
	3	19608757	DE	A1	1997-09-11	BROSOW, JOERGEN		☒
	4	10042805	DE	A1	2002-03-14	BUNDESDRUCKEREI GMBH		☒
	5	9843104	WO	A2	1998-10-01	PRICE, Frederick, J., R-W.		☐
	6	0993999	EP	A2	2000-04-19	FORD MOTOR CO		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

	7	0977145	EP	A2	2000-02-02	KABUSHIKI KAISHA TOSHIBA		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Atmel Corporation, Silicon solutions making smart cards smarter, 2000, 12 pages.	☐
	2	Extended European Search Report received in European patent application no. 10182033.0, dated January 13, 2012, 7 pages.	☐
	3	FANCHER, CAROL HOVENGA, In your pocket smartcards, February 1997, 7 pages.	☐
	4	RAKERS ET AL., Secure contactless smartcard ASIC with DPA protection, March 2001, 7 pages.	☐
	5	Japanese Office Action received in Japanese patent application no. 2004-519130, dated May 12, 2009, 3 pages (including partial English translation).	☒
	6	Anonymous, Read/write RFID offers standalone advantages, Security, August 1996, 1 page.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/li zhang/	Date (YYYY-MM-DD)	2015-03-16
Name/Print	Li Zhang	Registration Number	70902

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006165 A1

(51) International Patent Classification[7]: G06K 7/00, 19/07, 19/10

(21) International Application Number: PCT/IB2003/003702

(22) International Filing Date: 9 July 2003 (09.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/394,241 9 July 2002 (09.07.2002) US

(71) Applicant: BNC IP SWITZERLAND GMBH (CH/CH); Saegestrasse 5, CH-9230 Flawil (CH).

(72) Inventors: CORTINA, Francisco, Martinez de Velasco; Sierra Amatapec #213, Lomas de Chapultepec, D.F.11000 (MX). RIETZLER, Manfred; Am Alserberg 10, 87616 Marktoberdorf (DE).

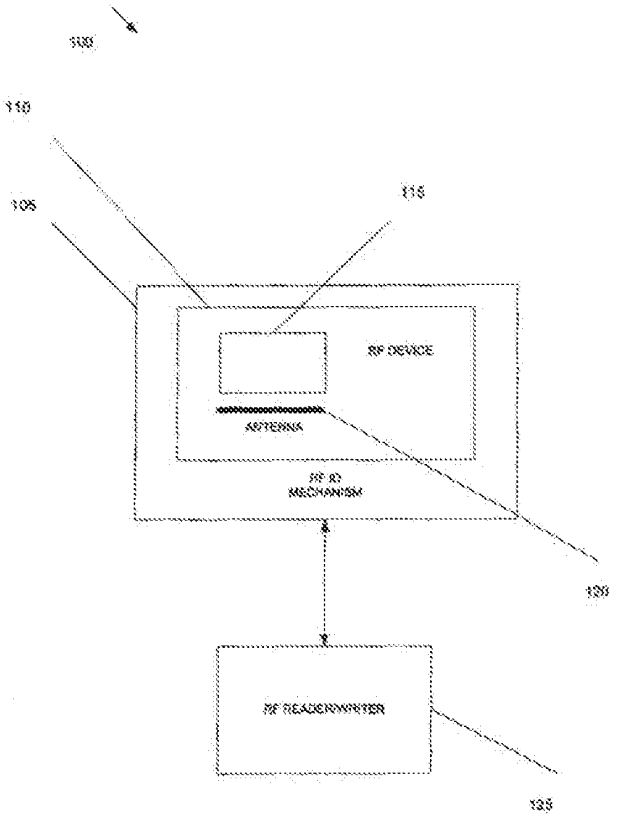
(74) Agent: MIDGLEY, Jonathan, Lee; Marks & Clerk, 57-60 Lincolns Inn Fields, London, WC2A 3LS (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, 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, 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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS



(57) Abstract: The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader.

WO 2004/006165 A1

Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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

TITLE OF THE INVENTION

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

This application claims priority to provisional application 60/394,241, filed July 9, 2002. This application also incorporates by reference U.S. Patent Application S.N. 10/118,092 filed 09 April 2002; PCT Patent Application PCT/IB02/01439, filed 30 April 2002; German Patent Application No. 10121126.0 filed 30 April 2001; and Mexican Patent Applications No. 010967 filed 26 October 2001, No. 010968 filed 26 October 2001, No. 010969 filed 26 October 2001, No. 010971 filed 26 October 2001, No. 003141 filed 25 March 2002, and No. 003202 filed 26 March 2002.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention generally relates to a system and method for providing secure identification solutions, and specifically to a system and method for verifying and tracking identification information.

SUMMARY OF THE INVENTION

The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification

mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to:

- An RF Registration Item (e.g., License Plate) and Method of Use.
- An RF Identification Mechanism (e.g., Passport) and Method of Use.
- An RF Communications Device (e.g., Cellular Telephone) and Method of Use.
- A System and Method of Border Crossing Control.
- A System and Method for Limiting Software Downloads to Authorized Users.
- A System and Method for Airport Security.

The embodiments of the present invention are discussed below. Those experienced in the art will see that multiple features of certain embodiments described below can be incorporated into other embodiments both described and not described below.

The present invention is not limited to the above embodiments. Additional advantages and novel features of the invention will be set forth in part in the Description that follows, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

BRIEF DESCRIPTION OF THE FIGURES

Figures 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention.

Figures 5-8 illustrate the RF registered item and method of use, in an embodiment of the present invention.

Figures 9-11 illustrate the RF passport and method of use, in an embodiment of the present invention.

Figures 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention.

Figures 15-18 illustrate a system and method for border crossing control, in an embodiment of the present invention.

Figures 3A-3B and 19-21 illustrate a system and method for limiting software downloads to authorized users, in an embodiment of the present invention.

Figures 22-23 illustrate a description of the system and method for airport security, in an embodiment of the present invention.

DESCRIPTION OF THE INVENTION

I. GENERAL RF IDENTIFICATION SYSTEM AND METHOD OF USE

Figure 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120.

A. RF Device

Figure 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF

device allows electronic identification via the reading of data stored in the chip in a contactless mode.

Figure 5 illustrates a dual frequency RF device 110, according to one embodiment of the present invention. Those experienced in the art will see that a one frequency or multiple (more than two) frequency RF device can also be used. The RF device includes the following components: A modulator 215 is a device that receives baseband signals from a antenna. An AC/DC converter 220 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 225 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 245 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 250 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 230 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 255 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 210 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 205 stores data. Information can be read and written from or to this device.

A more detailed description of an RF device can be found in U.S. Patent Application S.N. 10/118,092 filed 09 April 2002; PCT Patent Application PCT/IB02/01439, filed 30 April 2002, which are herein incorporated by reference. Additional information on the RF device can be found in the accompanying documents.

B. RF Identification Mechanism

Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA).

There are a variety of ways to make identification cards that are resistant to fraud and counterfeiting. In one embodiment, the present invention incorporates numerous security features, as explained below.

C. Features of Secure Identification Mechanisms

The present invention offers a variety of solutions for making secure and durable identification mechanisms resistant to fraud and counterfeiting. The following features help make the identification card more secure. These features are only examples, and those experienced in the art will see that the present invention is not limited to these features and that many other features can be incorporated.

In one embodiment of the present invention, at least one of the following features is incorporated: visible features, machine readable features, and proprietary substrate based features. Visible features require only the human eye to detect the security features. Machine readable features require special hardware

(e.g., an ultraviolet light source, magnetic reader) to detect the security features. Proprietary substrate based features are security features incorporated within a plastic substrate.

In one embodiment of the present invention, at least one of the following characteristics are present relative to the identification mechanism: it is extremely difficult to duplicate; it is tamper proof; it is recognizable either visually or utilizing a machine readable device; it is durable enough to withstand harsh environments; it is produced by specialized, difficult to obtain production equipment; it can be machine readable; and cost savings are realized by volume production of the identification mechanism.

Security features curb petty, semiprofessional and professional counterfeiters by creating features that are highly difficult to reproduce. For example, the ready accessibility of dye sublimation card printers, color scanners, color printers, heat sources (e.g., hair dryers), and color photo copiers makes it relatively easy to reproduce ordinary photo identification cards. In one embodiment, the present invention, therefore, utilize images and text that cannot be scanned or photocopied without noticeable distortion, or cannot be recreated without highly sophisticated and expensive equipment.

Security Features. In one embodiment, the present invention can incorporate at least one of the following security features:

- *Tamper Proof Material.* This material consists of metalized polyester treated with a chemical that will not allow an auto adhesive hologram to be transferred from one document to another one. It will self-destruct by any attempt at transfer.

- *Bidi-Tri-Dimensional at Three Levels.* This material must be created in an optical table by a qualified holographer and with a combination of design and dot-matrix effects created by precise digital means allow identification of the document's authenticity.
- *Hidden Images.* A hologram can contain a hidden image that cannot be detected with a naked eye. The hidden image can be identified by shooting a laser at 45 degrees. The reflection shows a spectrum of a text shield or design. A special lens to protect the eye from laser damage can be used.
- *Dot-Matrix.* A dot-matrix 1,000 dots per inch (DPI) effect is created in a computer and comprises engraving dots with a laser in an specific angle which a minimum density of 1200 to 2000 DPI's. It allows printing of micro text contained within a hologram with great precision and creates very precise 2D and 3D effects.
- *Hot Stamping.* Hot stamping places a hologram on a document by thermal transfer. This hologram will interlace with a paper substrate and will not allow a hologram to be transferred from one document to another.
- *Moiré Pattern.* The moiré pattern is a design-based pattern which superimposes two patterns with non-identical spatial frequencies. The effect is visually detected after utilizing a normal photocopier to reproduce the original pattern. The reproduced pattern induces a "moiré" or aliasing which immediately suggests the reproduced image is counterfeit. The original is produced utilizing digital image technology which differs from normal photocopy technology. This effectively "tricks" the photocopier and reveals the moiré in the reproduced pattern.

* *Hot Stamp Metalized Hologram.* This feature is a visual/substrate-based feature which can also be machine readable. It uses a special metalized hologram (e.g., as found on various currencies) or a holographic hot stamp (e.g., that is non-machine readable). This feature comprises special stripes placed within the card laminations and visible to the eye. These holograms can be proprietary in order to limit the availability to counterfeiters. The metalized holograms can also be machine readable to verify authenticity. The security of this feature is high because to duplicate it, a counterfeiter must have access to both the card manufacturing equipment and the source of materials, which are both difficult to obtain.

* *Microprint: Offset Printed, Visual/Machine-Readable Text of Particular Size.* The text is indecipherable without the use of a reading lens, and is usually incorporated as a single line. This feature is used to print misspelled words to fool counterfeiters who often assume complete and correctly spelled microprint. The offset printed text is located under a translucent lamination to protect it from abrasion. This feature is difficult to produce with clarity and resolution using a photocopier, scanner, or dye sublimation printer.

* *Microprint: Visual/Machine-Readable Text of Particular Size.* This text is indecipherable without the use of a reading lens, and is usually incorporated to appear as a single line. This feature is used to print misspelled words to fool counterfeiters who often assume complete and correctly spelled microprint. This feature is difficult to produce with clarity and resolution using a photocopier, scanner, or dye sublimation printer.

- *Ultraviolet Fluorescence: Offset Printed, Visual/Machine-Readable Art or Text which Produces Light When Activated by an Ultraviolet Light Source.* This feature is normally undetectable to the naked eye and can be overlooked by the casual counterfeiter. This feature is difficult to produce with easily obtained equipment. Special fluorescent colors are available for added security.
- *Light Pipe.* This is a substrate based, machine readable feature requiring a light source to detect. This feature is produced using optical techniques which direct light to specific locations of the card (e.g., the edge). The effect is a brilliant light at a location different from where the light source is pointed, and usually in a specific color. Since this feature involves specific translucent materials and optical design of substrates, counterfeiters may never detect this feature. It is also almost impossible to recreate such a feature.
- *Laser Engraving.* This visual substrate-based feature can be either tactile or subsurface depending upon the types of plastics employed. The feature can be either graphic or alphanumeric. Using a laser, a pattern or alpha-numeric text is ablated into the sub-layers of a plastic card. Depending on the parameters of the laser system and the materials of card substrate, a tactile or subsurface mark appears. This feature is particularly effective in the serialization of cards to reduce the risk of lost or stolen cards. The mark cannot be "scraped off" without noticeable damage to the card surface. A tactile surface is helpful in quick recognition of authenticity. Laser systems of such complexity are expensive and difficult to obtain.

- *Metalized Stripe*. This stripe is a visual substrate-based feature which can also be machine readable. This feature uses a special metalized stripe (e.g., found commonly inside various currencies) or a holographic stripe (e.g., non-machine readable). These special stripes are placed within the card laminations and are visible to the naked eye. The special stripes can be proprietary in order to limit the availability to counterfeiters. The metalized stripes can be machine readable to verify authenticity. This level of security feature is high because counterfeiters need access to both card manufacturing equipment and the source of materials. These are both difficult to obtain.
- *Guilloche Pattern*. This feature is an intricate pattern of curvilinear fine lines which were originally created by "engine turning," commonly used in currency design. This visual feature is design-based and commonly produced using offset printing onto plastic. It is normally contained under a translucent lamination which acts as protection from abrasion. The fine lines are difficult to reproduce with full clarity and resolution on a copier, dye sublimation card printer, or scanner/personal computer/inkjet system because the dye sublimation printer can print only onto the surface of the card.
- *Rainbow Guilloche*. This feature is similar to the guilloche pattern above and is used in conjunction with a color spectrum which gradually changes from color to color achieving a continuous effect across the surface of the card. The level of security is slightly greater since use of a sophisticated color copier is required to duplicate the pattern effectively.

- *Cameo Effect.* This feature is the result of cropping the background of an image with software to print only a silhouette of the person which makes it more difficult to replace than a square image. This effect is combined and interlaced with other security features, such as hidden infrared on the background of the picture, or interlacing a photo with guilloche patterns on the back.
- *Ghost Image.* This feature provides the ability to print a second photo of a person, which is degraded by software, and it is printed on a faded gray or color scale over the personal data of the person to protect this information from tampering or altering. This effect is also achieved by software.

Types of Holograms. Many different types of holograms with unique visual effects are utilized for commercial and security applications, as well as promotional products. In one embodiment, the present invention includes at least one of the following holograms:

- *Two Dimensional (2D) Hologram.* This hologram lies on one single layer, which projects vivacity of color. With this technique, we convert standard color line artwork or photography into an array of holographic colors.
- *Three Dimensional (3D) Hologram.* This hologram is created from a solid model or sculpture. The product's third dimension is captured. The design becomes a 3D image after the depth of the image is captured through the use of a sculpture. A logo or product will be seen without the need of special glasses or lenses.
- *Two/Three Dimensional (2D/3D).* This hologram combines a superficial layer with other dimensional layers, which can be a combination of both

technologies, as mentioned previously. One image produces multi-color levels because of the positioning of the various layers. This system adds a third dimension to pictures.

- *Line Artwork & Photographs.* One embodiment of the present invention uses line artwork, photographs, or a combination of both, to create several layers of images separated by specific distances in order to give the illusion of depth. In general, two layers are enough, but if necessary, five different layers of images can be used.
- *Colorgrams.* Also known as true color holograms, colorgrams usually use someone's photo. It is made up of photographic quality art-work. These holograms are surprisingly capable of displaying true colors of the object, like true human skin tones or the original colors of a flag. If a counterfeiter can't get the original photo, they can't duplicate the label. It's a good way to prevent counterfeiting. The colorgram system is similar to the 2D/3D system. Full-color photographs are reproduced in their true, original colors at a specific angle, usually at a 45 degree viewing angle. The system can combine photographs with line artwork at different layer levels.
- *Stereograms.* Stereograms involve the latest in advanced technology. They are the result of a complex system that gathers full images, volume, movement, color and total animation. Total animation gives the sensation of the movement of a live recording.
- *Holomatrix™ from 50 DPI to 2000 DPI.* This feature comprises microtext, optical variable effects, and computer-generated optical devices. Graphic images for this type of hologram are created with microdots. Each

dot is an individual embossment made with a laser beam. This feature creates holograms through the use of sophisticated computer technology. The laser beam individually embosses each dot, creating a luminous image with a fascinating presentation of colorful optical effects. This technique prints small dots and is similar to a laser printer or inkjet system. These dots are holographic gratings that act like small prisms that sparkle intensely. With this system, optical patterns can be built of images in such a way that the images can be viewed at a 360 degree angle, and have multiple images in the same hologram. Because of the difficulty of reproducing these images, this feature is excellent for security applications.

- *Diffractive Optical Variable Image Devices.* All the products classified as DOVIDs (Diffractive Optical Variable Image Devices) present an image which changes colors when tilted in various angles. This essential characteristic makes the images impossible to copy or imitate by traditional printing and graphics software.
- *Optical Variable Devices.* An optical variable device (OVD) is a way of printing an image in such a way that certain characteristics vary when viewed or illuminated from different angles.
- *Combined Holograms.* These holograms combine two or more of the above mentioned types of holograms. Combining Holomatrix™ with any of the above types makes the hologram more complex and ideal for security applications.

Optional Tests. In one embodiment of the present invention, the identification mechanism is tested in multiple ways. Laboratory test are used to

demonstrate durability, tamper proof, temperature and humidity stability, abrasion resistance, adhesiveness and light stability to ensure durability of the identification mechanism and to ensure that the dyes will not fade or degrade before at least 5 years of extensive use. In addition, dual lamination can be performed.

One embodiment of the present invention can include at least one of the following tests.

* *Static Bending Test.* In this test, a composite card is tested to exceed 100,000 bending cycles without breaking or losing its integrity.
* *Heat Test.* In this test, a composite card is exposed for an extended period of time to intense sunlight, boiling water, and a temperature of up to 220 degrees Fahrenheit without twisting or bending.
* *Rigidity Test.* In this test, multiple layers are applied to a composite card to give it rigidity so that when it is laminated it will not lose its flat shape, guaranteeing that the bar code is readable.
* *Durability Test.* In this test, a card is placed in a steam pressure chamber at 160 degrees Fahrenheit for four days to test that the card will not warp or break, and that the over lamination will not come off.
* *Abrasion Test.* In this test, a card is placed in an agitator containing a water and sand solution and subjected to 30 minutes of agitation.

Required Security Levels. Multiple security levels exist and are explained below.

First Level Security Features. First-level security features are clearly visible so that any attempts to modify the text data, photo image, or other personalized information is evident at a simple glance.

In one embodiment, the first-level security features include a complex hologram with multiple security features, combining a complex hologram structure with micro printing. The printer and the hologram is transfer through a holographic registration and a fiber optic sensor to assure very high accuracy. The holographic pattern is always transferred in the same position.

In one embodiment of the present invention, the hologram includes at least one of the following general features:

- A highly integrated technology and expensive machinery is required for mass production. Only manufacturers with sophisticated know-how can maintain its quality.
- The hologram makes the object visibly distinguished from other printing materials or those color copied.
- Some types of hologram (e.g., Kaleidogram, Finegram) ensure more satisfying security features than of the flat types, since the most advanced equipment is necessary in the process of production.

In one embodiment of the present invention, reproduction features include:

- A Transparent Kaleidogram with protective OP layer that is heat transferred on to the card book. It covers the entire printed area.
- Attempts to remove the hologram layer will damage the composition of hologram. Thus it can not be re-used, or tampered.
- Combined with micro-letter printing, the reproduction by color copy or photomechanical process is not feasible, as the 0.26 mm size characters is ruined when reproduced.

Additional first-level security features can be integrated with the RF identification mechanism (e.g., card) in the future. An example of such security features would be icons, symbols, or guilloches that could be printed in special solvent sensitive inks. These features can be printed directly onto the intermediate transfer layer. These security features could be employed at some time in the future if a solvent tampering technique is identified.

Overall, the proposed first-level security features provide the document with excellent protection against altering and falsification, as well as acts of counterfeiting. The features are readily visible and any attempts to modify the underlying information is evident at a glance.

Second Level Security Features. Second-level security features can also be included. These second-level security features are invisible to the eye under normal viewing conditions, and are evident only when using a proper detection device. In one embodiment of the present invention, at least one of the following features is included:

- *Invisible Ultraviolet-Fluorescent Features.* The visible portion of the energy spectrum extends from deep blue at, for example, 400 nm to deep red at, for example, 700 nm. Long wavelength ultraviolet energy in the region of the spectrum for example, between 350 nm and 400 nm, such as 380 nm, is used to excite an embedded ultraviolet-fluorescent material. These high-energy ultraviolet photons are absorbed by the fluorescent material that happens to be invisible or transparent in the 400 nm to 700 nm region of the spectrum. The ultraviolet photons pump the absorbing material to an excited energy states. The material in the excited states

quickly relaxes back and releases the absorbed energy again in the form of photons. Because some of the energy is lost in this transition, the emitted photons have less energy than the absorbed photons. The visible portion of the energy spectrum is positioned at the lower energy photon levels. Consequently, the process results in visible light being emitted from the material when it is illuminated by ultraviolet light. In a darkened room, the eye detects the glow being emitted by the ultraviolet-fluorescent material but not the ultraviolet light that is used to excite the material.

* *Two-Dimensional Bar Code.* The card solution can include a PDF-417 format barcode (two-dimensional barcode) that is printed onto the card. The PDF-417 barcode can hold several types of data (e.g., fingerprint minutiae, personal information).

RF Device. An RF device can complement all the previously mentioned security features, as it has a unique identifier (e.g., a unique 64 bit serial number), and the information contained on it is protected by sundry cryptographic methods. The capacity of the device will allow a great deal of information about the holder to be stored on the device (e.g., fingerprint minutiae or other biometric template, the holder's biographical information, statistical information). Those experienced in the art will see that an RF device allows data to be written to and read from the device via an antenna without the holder having to present the document for verification through traditional methods such as visual inspection, or other method of machine reading.

Third level Security Features. Two optional security features can be changed every eighteen months: special IR-activated security taggant material and

proprietary security taggant material.

Special Infrared-Activated Security Taggant Material. A special ceramic compound (e.g., such as a product named Taggant, provided by Secure Products) is mixed with a clear ink media in very small concentrations. (The ceramic compound is referred to as Taggant, but those experienced in the art will recognize that other ceramic compounds or equivalent product can be used.) This mixture is printed on the intermediate transfer material surface. After being ground to small particles that are approximately 2 - 3 μm in diameter, the special ceramic compound appears to be a very fine white-colored powder. The combination of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye.

A low-power, eye-safe near-infrared laser can be used to activate the special IR-activated taggant material. The input wavelength of the laser must be tuned within a 3--5 nm bandwidth in order to activate the material. The input energy is pumped into the material with the lower energy photons of the laser. The combination of the long lifetimes for the excited energy states and the high concentration of photons from the near infrared laser result in a second transition upward in energy level. In other words, two photons are absorbed by the material to increase the available excitation energy. These high excitation energy states relax releasing photons in the visible portion of the spectrum as well as the near-infrared portion.

This process of effectively adding two lower energy photons together to release a higher energy photon is called "up-conversion". The special IR-activated security taggant material has three separate emissions or security features. When

an appropriate infrared laser, which is invisible to the eye, is focused on the special taggant material, three features are emitted simultaneously. These three features are a visible green spot at the point of focus, a visible blue spot at the point of focus, and an invisible infrared point at a higher energy level in the near-infrared portion of the spectrum. When viewed by the eye, the green and blue spots blend together to create a vivid turquoise color. However, all three features can be detected automatically and separately with the proper equipment.

Proprietary Security Taggant Material. A proprietary security taggant material can also be included in the card design. A special ceramic taggant material (e.g., such as the one produced by Secure Products) exhibits multiple security features and is in part based on the "up-conversion" concept. The white powder is ground into particles that are 2 – 3 μm in diameter and is mixed into a clear ink media in very small concentrations. Again, as before, the combination of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye. However, this special material can be activated by several wavelengths and each activation wavelength results in a different response.

One characteristic and security feature is activated by a special low-power, eye-safe near-infrared laser. The activation bandwidth is approximately 3 nm and is located on the longer wavelength side of the activation energy required for the second-level feature. Laser devices are far less common in this area of the spectrum. When the special taggant is excited by a laser specially tuned to this excitation frequency and bandwidth, two separate emissions are observed. One emission is in the visible portion of the spectrum and can be observed as a green

spot at the point of incidence. The second emission is in the near-infrared portion of the spectrum near the excitation wavelength of the first optional security feature.

A second characteristic and security feature is observed by using a second low-power, eye-safe near-infrared laser at about the same excitation energy as the similar second-level feature. At this excitation wavelength, a green spot can be observed at the point of incidence due to the "up-conversion" process.

Finally, a third characteristic and security feature can be observed by applying energy in a wider bandwidth in the upper portions of the visible energy spectrum. This wavelength of energy is absorbed and re-emitted as longer wavelength infrared energy. In one embodiment, the initial implementation activities will focus on a verification process that utilizes a single excitation wavelength and a single observation wavelength. The implementation of the other embedded security characteristics can be phased into the program as new features are required to maintain the overall security of the card documents. Since these untapped security features and benefits will have existed in the documents from the initial issuance, the implementation of the new features will minimize the impact to the overall system.

In addition, new security features can be integrated into the present invention should the need arise.

D. Method of Using the General RF Identification System

Figure 4 illustrates method of using the RF identification system 400, according to one embodiment of the present invention.

In 405, the identification information (e.g., fingerprint, picture) is written to

a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity.

II. RF REGISTERED ITEM AND METHOD OF USE

One embodiment of the present invention allows authorities to track information regarding a registered item (e.g., a vehicle), identify the item, and determine whether a driver of the item has the right to operate the vehicle. The present invention is described using the illustration of a license plate, but those experienced in the art will recognize that multiple other embodiments are possible, including, but not limited to: a sticker (e.g., a self-adhesive decal that can be placed on an automobile window, windshield or license plate), an RF embedded license plate (e.g., if the license plate is to be manufactured with some non-conductive material, the RF device can be embedded directly into the license plate), an encapsulated RF device (e.g., in the housing of a rear-view mirror, headlights or taillights, the vehicle's front or rear bumpers, or in any non conductive component of the vehicle; the device can be encapsulated in such a way that it will resist normal use and exposure to the elements, or embedded directly into the materials comprising the aforementioned placement media).

The present invention can be used, for example, for vehicle identification, border crossing solutions, traffic violations, insurance programs, pollution control,

vehicle access control, traffic logistics planning and engineering, toll booths, and other vehicle control applications. The present invention takes centrally stored information and makes it accessible to the field (e.g., to police or other authorities). It also extends and expands the verification of individual and item (e.g., vehicle) information.

A. RF Registered Item

Figure 5 illustrates an RF registered item 500, according to one embodiment of the present invention. The registered item 500 includes the following components: A modulator 515 is a device that receives baseband signals from a antenna. An AC/DC converter 520 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 525 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 545 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 550 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 530 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 555 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 510 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 505 stores data. Information can be read and written from or to this device.

B. Method of Using RF Registered Item

Figure 6 illustrates method of using RF registered item 600, according to one embodiment of the present invention. In 605, individual identification information (e.g., fingerprint, picture) and/or vehicle identification information (e.g., registered vehicle, license number) are collected and written to an RF device (i.e., a chip with an RF antenna). In 610, the RF device is embedded onto an identification mechanism, a license plate. In 615, an authority wishing to check a vehicle uses an RF reader/writer to read the chip data. In 620, the authority takes and compares the individual identification information (e.g., user's fingerprint, check user's face) and/or vehicle identification information (e.g., check make and model of vehicle, check vehicle license number) and to the chip data to verify an individual's identity and whether the individual has the authority to possess and operate the vehicle.

In one embodiment, a selective metalizing procedure is used to selectively metalize the areas which will not carry the RF device. This can be done by using a mask, as illustrated in Figure 7.

C. Method of Making RF Registered Item

In one embodiment, the identification mechanism (e.g., license plate) comprises a material that allows visual validation of the registration, even at night. The material can be a retro-reflective materials, holographic foil, or another substrate with a high metal content.

Figure 8 illustrates method of making RF registered item 800, according to one embodiment of the present invention. In 805, antennas are produced on a

demetalized or selective metalizing process. In 810, after demetalizing, resistance is decreased and conductivity is increased by applying inks containing silver or copper (e.g., conductive inks). In 815, an adhesive layer is applied to the antenna in a Web environment or with automatic label capabilities.

In one embodiment of the present invention, at least one of the following is tracked:

- *Vehicle Identification Number (VIN).* The VIN is the vehicle's international registration number and is the "fingerprint" of the car. Vehicle identification is performed by visually reading the car's VIN, and using the software to validate the VIN. This software allows a user to determine if the vehicle has been modified, altered, and/or stolen.
- *Owner Identification.* Owner identification is made using photographic information (e.g., a photograph) and/or biometric information (e.g., a fingerprint, iris pattern) stored in the RF device.
- *Tracking information.* The RF device is used to read the VIN number and the owner's information. This can be used to identify a vehicle or individual reliably without having to connect to a central database.
- *Central Data Base.* The central data base validates the identity information for increased security (e.g., tracking who and where the device was produced and who it belongs to).

B. Optional Security Features

In one embodiment of the present invention, at least one of the following security features is included:

* *Secure Device.* In one embodiment, the device has: numerous (e.g., five) visual inspection security features visible only to the naked eye; numerous (e.g., three) non-visual forensic security features that require a special device for detection; and at least one security feature requiring a special detection device that is proprietary (i.e., it was manufactured specifically for a particular client).

* *Secure Identification.* This feature requires information contained in the device to be unalterable without a determination of who wishes to alter the information and for what purpose. Highly secure chips with a hardware programmable cryptographic block with credit and debit exchange keys is used in one embodiment of the present invention. In addition, the individual information of the vehicle (e.g., the VIN) and the personal information (e.g., biometrics) contained in the device must be protected.

* *Secure Transaction.* This feature protects the device from the equipment that reads and writes from the device. This equipment must be initialized using the same encryption keys as the RF device.

* *Secure Data Base.* This feature protects information in the central data base and the transaction log indicating where and for whom the device was produced. Central data base security is possible using encryption. This technology allows centrally-stored information to be taken to the field (e.g., to track the inspections for stolen vehicles). It also extends and expands the verification of both individual and vehicle identity.

III. RF IDENTIFICATION MECHANISM AND METHOD OF USE

The present invention includes an RF identification mechanism, such as a passport, and a method of using the same. The present invention will be described in the context of a passport. However, those experienced in the art will recognize that the RF identification mechanism is not limited to a passport, and multiple other embodiments are available, including, but not limited to: a license, credit card, cell phone, etc.

A. RF Identification Mechanism

Figure 9 illustrates an RF registered item 900, according to one embodiment of the present invention. The registered item 900 includes the following components, as described earlier: a modulator 915, an AC/DC converter 920, an encoder 925, a power control 930, an instruction sequencer 940, a cryptographic block 910, a decoder 945, a security management unit 955, a memory 905, and an antenna 935.

B. Method of Using an RF Identification Mechanism

Figure 10 illustrates a method of using the RF passport, according to one embodiment of the present invention.

In 1005, identification information (e.g., a biometric template, photography, social security number, personal identification number) is collected and written to the chip on the RF device. In 1010, the RF device is embedded on a passport. In 1015, the user enters an area where a passport must be presented and an RF reader/writer reads the identification information from the RF device on the

passport. In 1020, an authority collects second identification information from the user (e.g., takes the user's fingerprint, looks at the user's face) and the information is compared to the RF device data to verify the user's identity.

C. Method of Making an RF Identification Mechanism

Figure 11 illustrates how an RF passport is made, according to one embodiment of the present invention. In 1105, the passport inlay is produced on a PVC substrate. A copper wire and chip are embedded into the passport inlay. In 1110, the passport inlay is embedded into the passport document. In 1115, the passport is printed using a holographic retransfer film and dye sublimation inverse printing. In 1120, the RF passport identification information is matched to the person who owns the passport. In 1125, the passport is initialized, and personal information and/or biometrics are encoded on the passport to the RF device. This is done after the passport is personalized for security reasons. The RF passports are of no utility if they are stolen, as they need to be initialized with proper encryption keys and personalized.

IV. RF COMMUNICATION DEVICE AND METHOD OF USE

One embodiment of the RF communication device creates a communication through a network to a point of sale ("POS"). This is performed, for example, by a wireless RF device that stores a person's identification information, and can thus become a person's identification "document." This is discussed in the context of an RF cellular telephone, but those experienced in the

art will recognize that any communication device, including but not limited to a personal digital assistant or a pager, can be used.

As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone. The user is then asked to enter authentication information (e.g., a fingerprint). If the user wishes to complete a transaction, the user enters the authentication information. An exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information.

The present invention, referred to in one embodiment as a RF cellular telephone, creates a communication through a network of cells to a point of sale (POS). This is performed by combining Global System for Mobile Communication (GSM) technology with a wireless RF device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). GSM technology includes a compact chip located on the back of the telephone. The compact chip has an operating system. The GSM telephones identify the telephones to a network carrier to avoid, for example, telephone cloning.

The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card or other card (e.g., mileage cards). Multiple types of information can be carried and stored on the RF cellular telephone. The following uses are examples of how the RF cellular telephone can be used: an RF cellular telephone can be used as a substitute for

credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities; an RF cellular telephone can be a personal identification or a Portable Data File (PDF); an RF cellular telephone can be integrated with a Global Positioning System (GPS) receiver; an RF cellular telephone can be integrated with hand held devices to provide Internet access, and access to business and personal information (e.g., email); and an RF cellular telephone could be a boarding pass (e.g., e-ticket) and/or could track a user going through security with authentication by fingerprint at a gate or other local area. Those experienced in the art will recognize that there are multiple other examples and uses of the RF cellular telephone.

One embodiment of the present invention provides at least one of the following benefits: assists in avoiding current credit card fraud, through clonation, substitution of identity, or counterfeit documents; reduces or eliminates the need to carry credit cards, documents (e.g., a boarding pass) or other information; reduces or eliminates the need for an entity to issue or update credit cards or identification documents (e.g., tickets), with associated fees (e.g., mailing costs); and reduces or eliminates the need to stand in line or wait for services.

The present invention is discussed in the context of using a fingerprint for identification, as this is a widely recognized identification tool. However, those skilled in the art will recognize that any type of identification information (e.g., Personal Identification Number (PIN)) or any other biometric identifier (e.g., a voice print, iris recognition, facial recognition) could be used.

A. RF Communications Device System

Figure 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

The POS 1210 can include an RF reader/writer 31 and a fingerprint digital scanning device 1232. One-to-one verification ensure that the information on the RF cellular telephone matches the holder of the RF cellular telephone.

The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact.

One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in Figure 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements aren't met, a user cannot access the memory of the chip. The chip includes an AC-DC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device

that receives baseband signals from a antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 1347 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device.

In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security.

B. Method of Using an RF Communications System

Figure 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device

obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone.

According to Figure 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information).

In 1410, the customer purchases a service or product and is prompted to enter authentication information (e.g., a fingerprint). In 1415, if the user wishes to complete the transaction, the user enters authentication information (e.g., imprints a fingerprint into a fingerprint scanner) and it is loaded to the RF device.

In 1420, the RF reader/writer and RF cellular telephone are used to verify the authentication information (e.g., the fingerprint scanner works with the RF reader/writer and the RF cellular telephone and/or other devices to ensure the customer's fingerprint matches the fingerprint stored on the RF cellular telephone) and this information is presented to a point of sale or access control device to retrieve purchase information.

Although the present invention has been described in the context of a POS, those skilled in the art will recognize that a user could use the RF cellular telephone without a POS. For example, a user could call a telephone number to buy a ticket to access a stadium, using identity verification and other transmitted information. As another example, a user could load a boarding pass or ticket to an event on an RF cellular telephone, and the boarding pass or ticket would be confirmed at an access control device around the perimeter of an airport lounge or stadium.

Additional information related to the present invention can be found in U.S. Patent Application 10/118,092, filed April 2, 2002, and PCT. Patent Application IB0201439, filed April 30, 2002, which are herein incorporated by reference.

V. SYSTEM AND METHOD FOR BORDER CROSSING CONTROL

One embodiment of the present invention provides a border crossing control mechanism using RF technology. This technology helps provide a flexible, efficient, and effective border crossing security system to meet the needs of rapidly changing security conditions. The present invention provides heightened security while at the same time efficiently and quickly moving vehicles and people across

borders and through customs. In this embodiment, an identification mechanism (e.g., a laser card) is integrated with a vehicle decal that registers and matches any shipping components (e.g., drivers, vehicles, containers). The shipping components will be pre-registered in the decal at a point of origin. A fingerprint biometric of the driver is written into the identification card and the decal at the factory. An RF antenna embedded into the decals allows tracking of, for example, the driver, cab and trailer, and validation of these components at strategic checkpoints. It also provides for designated routing through the port for inspection and clearance prior to departing the port.

The present invention can be used in a closed system or open system. In a closed system, all information resides on the RF laser card and RF decals. In an open system, information is passed from the point of original to country A's custom's inspectors, and from country A's customs inspectors to Country B's customs inspectors using a network (e.g., the Internet). This makes integration and implementation easier.

A. Border Crossing Control System

Figure 15 illustrates border crossing control system 1500, according to one embodiment of the present invention.

The system 1500 includes at least one client 1505, application server 1510, database 1515, RF identification mechanism 1520, RF device 1525, RF reader/writer 1530, connected by a network 1520.

Client. According to one embodiment of the present invention, clients are any computers (e.g., PC, PDA, cellular phone) connected to a network (e.g., LAN

(Local Area Network), WAN (Wide Area Network), VPN tunnel (Virtual Private Network Tunnel), Internet).

Application Server. According to one embodiment of the present invention, an application server is used (e.g., an Oracle9iAS integrated into a J2EE application server). The application server can support web application software, wireless, web page caching, business intelligence features, and offer complete integration in a single product. The application server can also offer scalability, reliability, and security features. It can also include advanced clustering features to keep critical applications up and running 24x7; offers zero downtime and planned downtime through a fast start fault recovery architecture; and recover from incidents quickly and gracefully.

In the example embodiment of an Oracle9i application server, the high availability infrastructure includes Oracle9iAS Web Cache clusters, Oracle HTTP Server (Apache), and Oracle9iAS Containers for J2EE. In addition, database applications hosted on Oracle9i Application Server can take advantage of Oracle9i Real Application Clusters (RAC) to make them more available. Oracle9i Application Server is the middle-tier deployment platform for all applications developed using Oracle9i Developer Suite. All applications can be deployed on the same middle-tier. Oracle9i Developer Suite is a complete and standards-based set of development tools. The suite includes Oracle9i JDeveloper, Oracle's flagship J2EE and XML development environment that supports the full development life cycle of J2EE applications and Web services. It also includes Oracle9i Forms Developer for easily and quickly construct sophisticated database

forms and business logic delivered through any Internet browser as a high performance, rich Java client.

Database. In one embodiment, the present invention uses a database with real application clusters (RAC) that can transparently scale and protect packaged applications with no changes necessary for the application (e.g., Oracle9i). RAC can scale all applications and also provides superior data protection with hot failover in less than 30 seconds.

According to one embodiment, the database provides a unique combination of scalability and availability in the same clustered database solution. With RAC, efficient scaling can be accomplished by simply adding servers to the overall cluster as the demand grows. Since RAC databases can grow flexibly, applications are protected from having to purchase excess computing power at a premium price. A RAC database can have costs significantly lower than the same solution implemented on an SMP (Symmetric Multi Processing) machine.

The database may include security and manageability features. The security features include: a Virtual Private Database (VPD); fine-grained auditing; data encryption;

The VPD technology provides programmatic row-level security and is enabled by associating tables or views with centrally defined access control policies. VPD addresses the application bypass problem and ensures that the same access control policy is enforced whether a user gains access to data through an application, ad hoc tool or SQL*Plus. As a result, multiple communities of users can securely share data within the same database.

Fine-grained auditing allows businesses to audit database activity by statement, system privilege, object or user. Its enhanced fine-grained auditing functionality enables organizations to centrally define specific audit policies that alert administrators to data access misuse. Audit records, stored within the database, capture the user statement's exact SQL text and can be easily viewed through ad hoc queries.

Data encryption is the ability to natively encrypt data in the database, enabling applications to guard sensitive data. Server-based encryption supports industry-standard Data Encryption Standard (DES) and Triple-DES (3DES), in both two and three key modes for any organizations who require the strongest level of encryption. Encryption can also support the MD5 secure cryptographic hash to ensure data integrity and a Federal Information Processing Standard (FIPS) 140-certified random number generator for generating secure encryption keys.

The manageability features include intelligent self-managing and tuning. The database can enhance database manageability by automating routine tasks, reducing complexity of administration and making the database more self-tuning and self-managing. Features can be added to streamline space, memory, and resource management as well as other day-to-day database administrative tasks.

RF Identification Mechanism, RF Device, and RF reader/writer. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing an Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer.

Multiple Chip Background Information. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequence can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See Figure 16.)

In one embodiment of the present invention, instead of, or in addition to incorporating the chip on the RF identification mechanism (e.g., RF smart laser card or RF decal), a chip can be embedded on a car windshield for smart windshield applications for vehicle registration, manufacturing, distribution of traffic violations, or any operation that requires contact with certain authorities. In this embodiment, the RF antenna can be used as radio antennas embedded on glass with copper wire during the manufacturing process, and connected to a module or embedded in the glass itself.

The resonant frequency of the antenna circuit in the RF device can be given by solving this equation:

$$f = \frac{1}{2\pi\sqrt{LC}}$$

$f = frequency(Hz)$
$L = inductance(H)$
$C = capacitance(F)$

The frequencies at the poles are parallel resonant frequencies, and depending on the technology can be:

$$f_1 = 13.56\,MHz$$
$$f_2 = 915\,MHz$$
$$L = \frac{N^2 \mu_0 A}{l}$$

N = number of windings around inductor
μ_0 = permeability of free space $(H \cdot m^{-1})$
A = cross-sectional area of inductor (m^2)
l = length of inductor (m)

The inductance " L " depends on the number of turns of the coil, of the area perpendicular to the coil and of the permeability of free spaces and length of the coil. Therefore:

$$L = \frac{1}{f^2 4\pi^2 C} \Rightarrow$$
$$\frac{N^2 \mu_0 A}{l} = \frac{1}{f^2 4\pi^2 C} \Rightarrow$$
$$l = f^2 4\pi^2 N^2 \mu_0 A$$

For substitution, the following values are used:

$$L_1 = 2.93 \text{K} 10^8\,H$$
$$L_2 = 6.437 \text{K} 10^{12}\,H$$

The data signal between the antenna and the tag is modulated by amplitude and coded by a Manchester encoding. Thus, manchester data = NRZ data ^ (NRZ clock).

Multiple RF Chip Overview

Figure 17 illustrates an overview of the chip, according to one embodiment of the present invention. As described in detail above, the chip includes: an AC/DC converter (915 MHz) 1705 and accompanying power supply control unit

1715; a modular 1710; a codifier 1720; an AC/DC converter (13.56 MHz) 1745 and accompanying power supply control unit 1750; a decoder 1740; a security administrator 1755; an instruction sequencer 1730; a cryptographic block 1725, and memory 1735.

B. Method of Using a RF Border Crossing Control System

Figure 18 illustrates method for using an RF border crossing control system 1800, according to one embodiment of the present invention. In 1805, an RF decal is issued at the point of origin for each shipping component (e.g., tractor/cab; trailer/bed; containers). In 1810, data is written to the embedded chip using a computer (e.g., a PC) located at the point of origin. Electronic forms can be used to ensure consistency, accuracy and completeness in the information gathering and decal issuance process. Information includes: specific details for identification and verification of the tractor, trailer, and containers; specific information on the driver including photo and biometric information (e.g., fingerprint); time stamp of when the driver, tractor, trailer, and containers leave the point of origin.

In 1815, a certified official (e.g., company official, customs agent) applies the RF decal to the shipping components (e.g., cab, trailer, containers) at the point of origin or other appropriate place. In 1820, the driver's personal data and shipment information are written to the driver's RF identification mechanism (e.g., laser card) at the point of origin or other appropriate place.

In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs

area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals.

In 1840, as an additional option, at the conclusion of the customs inspection process, and after all approval data is written to the RF decals, a final check is conducted at the port exit or other appropriate place. As the vehicle approaches the exit point, the RF decals are read for the final check to ensure all have matching data. This will be proof that the vehicle passed through all required checkpoints, inspections, and processing. As with the point of entry, each RF decal is read in sequence and the information is displayed to the custom agent's display screen. If any RF decal information does not match, the display will indicate a stop and the vehicle will be stopped for additional inspection or validation.

VI. SYSTEM AND METHOD FOR LIMITING SOFTWARE DOWNLOADS

One embodiment of the present invention relates to a de-metalizing edging process, and various resultant combinations of embedded processor chip, antenna, metallic hologram, integrated circuit, and substrate form factors to produce an end product (e.g., smart card or smart label). This enables RF communication within a

networked system configured for various identification and verification applications. These security RF smart labels can be adapted to the identification and data capture requirements associated with unique software media or packaging of any software publisher, ISV or manufacturer.

A. System for Limiting Software Downloads

Figure 19 illustrates system for limiting software downloads, according to one embodiment of the present invention. The system includes a RF read/write device, an RF smart label with a chip and RF antenna, and the software.

The software media (e.g., a CD) and/or package carries an RF smart label, containing an RF antenna providing a link to a chip 1900. The chip has encryption and read/write capabilities. Access is controlled through a certificate of authenticity 1910. Working in combination with an RF reader/writer, the present invention will capture any available unique digital central processing unit (CPU) or processor number and read/write to an original certificate of authenticity. The system locks the certificate to the CPU or processor, and will not allow this unique software to be installed on any machine other than the one on which it was initially authorized to be loaded. This highly secure encrypted solution can also be used to control access to customer support, debugs, updates and other services via the network (e.g., Internet) for authentic paid software licenses only. As described above, the chip includes a modulator 1905, encoder 1965, decoder 1940, instruction sequencer 1915, cryptographic block 1920, converter 1920, power control 1945, security management 1950, memory 1955, and antenna 1960.

VPN Tunnel Mode. The present invention can be incorporated into a network, such as a Virtual Private Network (VPN). A VPN is a private data network that makes use of the public telecommunication network or Internet infrastructure, maintaining privacy through the use of security and authentication procedures. A VPN is the emulation of a virtual private Wide Area Network (WAN) facility using Internet Protocol (IP) facilities. The VPN may use many aspects of networking, such as IP addressing, advertising reach ability, Quality of Service (QoS), data security and access control.

Figure 20 illustrates a VPN tunnel mode solution, according to one embodiment of the present invention. A database 2005 is connected to a security gateway 2015, which is connected to an application server 2010, connected to the client 2025 through a network 2020. Tunnel mode is used when one or more IP clients need to communicate to a main computer or server computer. The tunnel mode utilizes data encryption and key management. The VPN end points monitor the operation of the VPN tunnels (VPN clients) to ensure the connectivity has not been lost, and take appropriate action if there has been a failure. This is very important because all applications are dependent.

The present invention utilizes features that provide high-quality, interoperable cryptographic base security for access central information. For example, two traffic protocols are used: an Authentication Header (AH) that provides data integrity; and an Encapsulation Security Payload (ESP) that provides confidentiality (e.g., encryption of data), data integrity, and thought use of cryptographic-key management procedures. ESP is known as an Internet Key

Exchange (IKE) protocol. This protocol negotiates the security association between two end points and exchanges keys between them.

There exist two operation modes for both AH and ESP: transport mode and tunnel mode. Transport mode is used to authenticate information transmitted between nodes or machines (e.g., computers, servers) on a WAN/LAN network. Tunnel mode is used for communication between two or more end points that pass through a public network (e.g., the Internet). Tunnel mode is used to provide more security for information accessed by remote users or applications.

Figure 3A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in Figure 3B.

B. Method of Limiting Software Downloads

Figure 21 illustrates method for limiting software downloads to authorized users 2100, according to one embodiment of the present invention. In 2105, a software license is issued with an RF device (including a chip with an RF antenna) to an authorized user for one computer. In 2110, when the user installs the software on a computer (e.g., computer #1), the RF device reads the computer's serial number from computer #1. In 2115, if the chip information on the RF device matches the information on computer #1, the software is installed. In 2120, as the software license in this case is for only one computer, the software will not be able to be installed on other computers until the software is removed from computer #1, when the serial number from computer #1 is erased. In an alternate embodiment, where a license is granted for X number of users, only X number of computer serial

numbers will be able to be checked by the RF device, and thus only X users can download the software.

In additional embodiments, use of other unique identifying characteristics associated with other computer components (e.g., mouse, motherboard or central processing unit cabinet), can be utilized. In a further embodiment, the present invention is used for multi-license and corporate environments. In these cases, where an authorized corporate licensing entity with a registered billing address has access to software through a network (e.g., the Internet), the RF device limits the download of software to the number of users or units authorized under the license agreement. The present invention can control downloads to any computer, including central servers or individual PCs. This simple, yet highly secure kit locks the number of each CPU or processor for the central server and the PCs to the authorized number of users for each version of software, thus providing a seamless, secure upgrade capability. In an additional embodiment, the present invention provides an adapted PDA to provide additional support for software distribution and inventory control, as well as instant legal software authentication for law enforcement and industry piracy control.

VII. SYSTEM AND METHOD FOR AIRPORT SECURITY

The present invention is a scalable, end-to-end RF identification system for airport and air transport security and addresses, for example, the following issues: establishes the actual identity of a passenger; runs a hot file fingerprint search against the INS, CIA, INTERPOL, FBI databases; links passenger to boarding pass and checked/handheld baggage; cross-verifies passenger identification at strategic

points within the airport environment; cross-verifies stowed baggage with boarded passengers; track individuals within the airport; highly secure, cost effective, and non-intrusive; enables speedy and accurate passenger processing. In a security system that ultimately extends to existing airline and government computer systems and databases, the present invention is the "final link" that allows designated security personnel to track and validate on the spot the status of persons or items throughout the airport environment.

While the invention is described in the context of airport security, those experienced in the art will see that any facility (e.g., train station, ship, company campus, university campus) with a need for security can use the present invention, and the present invention is not limited to use in an airport facility.

A. Airport Security System

Figure 22 illustrates a chip of an airport security system, according to one embodiment of the present invention. The present invention includes: an RF reader/writer; and an RF identification mechanism (e.g., RF boarding pass, RF luggage tags, RF identification cards) including an RF device. Alternatively, AFIS verification scanners, security and control software, and distributed databases can be included.

The RF reader/writer can comprise computer system components (e.g., remote readers/writers, verification scanners, client/server or thin client systems and networks, and application software and databases).

The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz.

The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts.

As described above, the chip has a memory 2205 (e.g., 2k), an option hardware wired cryptographic block 2210 (with 4 exchange encrypted keys with up to 256 bits), a modulator 2215, a converter 2220, an encoder 2225, a power control 2230, an instruction sequencer 2260, a decoder 2245, a security management unit 2255, an memory 2205.

B. Method of Airport Security

Figure 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics

are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card.

In 2310, a passenger presents the RF air travel identification card or other RF identification mechanism to the airline authority when traveling. In 2315, The agent scans the RF air travel identification card. In 2320, the RF boarding pass and RF baggage tags are printed for the passenger. The boarding card now contains all data and tracking mechanisms required for secure passenger access to the gate and the matching aircraft, as well as boarding verification. In an alternative embodiment, instead of issuing an RF boarding pass, the RF air travel identification card can also contain e-ticket information. In parallel to the issuance of the boarding pass, identity information is captured by the system and digitally copied, together with the relevant travel route and destination data onto the RF baggage tags. The RF baggage tags are printed through systems and printers enhanced with an RF identification write device. The RF baggage tag now contains all data and tracking mechanisms required to link passenger, bag, and flight, thus enabling verifiable passenger/baggage/flight cross-referencing to the matching aircraft.

CONCLUSION

Additional advantages and novel features of the invention will be set forth in part in the Attachments that follow, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

WHAT IS CLAIMED IS:

1. A system of verifying information, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

a radio frequency identification mechanism incorporating the radio frequency device; and

a radio frequency reader to read information from the radio frequency device.

2. A method of verifying information, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto a radio frequency identification mechanism;

reading first identification information with a radio frequency reader; and

comparing the first identification information with second identification information to determine if a match exists.

3. A system of verifying registration information of an item, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

an item incorporating the radio frequency device; and

a radio frequency reader to read information from the radio frequency device.

4. A method of verifying registration information of an item, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto the item;

reading the first identification information from the item with a radio frequency reader; and

comparing the first identification information with second identification information obtained from a user to determine if a match exists.

5. A system of verifying registration information of a vehicle, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip; and

a license plate incorporating the radio frequency device.

6. A method of verifying registration information of a vehicle, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto a license plate attached to the vehicle;

reading the first identification information from the license plate with a radio frequency reader; and

comparing the first identification information with second identification information obtained from a user to determine if a match exists.

7. The system of Claim 3, wherein the first and second identification information comprises at least one of:

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

8. The method of Claim 4, wherein the first and second identification information comprises at least one of:

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

9. A system of verifying identification information of an individual, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

an identification mechanism incorporating the radio frequency device; and

a radio frequency reader to read information from the radio frequency device.

10. A method of verifying identification information of an individual, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto an identification mechanism;

reading the first identification information from the identification mechanism with a radio frequency reader; and

comparing the first identification information with second identification information obtained from the individual to determine if a match exists.

11. The system of Claim 9, wherein the first and second identification information comprises at least one of:

physical characteristics of an individual authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of an individual authorized to drive a vehicle.

12. The method of Claim 10, wherein the first and second identification information comprises at least one of:

physical characteristics of an individual authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of an individual authorized to drive a vehicle.

13. The system of Claim 9, wherein the identification mechanism is at least one of:

a passport;

a driver's license; and

an identification card.

14. The method of Claim 10, wherein the identification mechanism is at least one of:

a passport;

a driver's license; and

an identification card.

15. A system of verifying identification information of an individual, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

a communication device incorporating the radio frequency device; and

a radio frequency reader to read information from the radio frequency device.

16. A method of verifying identification information of an individual, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto a communications device;

reading the first identification information from the communications device with a radio frequency reader; and

comparing the first identification information with second identification information obtained from the individual to determine if a match exists.

17. The system of Claim 15, wherein the first and second identification information comprises at least one of:

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

18. The method of Claim 16, wherein the first and second identification information comprises at least one of:

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

19. The system of Claim 15 wherein the communications device comprises:

a cellular phone;

a personal digital assistant;

a pager;

a personal communications device

20. A system of verifying border crossing control information, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

a radio frequency decal incorporating the radio frequency device attached to at least one item;

a radio frequency card incorporating the radio frequency device tied to an individual connected to the at least one item; and

a radio frequency reader to read information from the radio frequency decal and the radio frequency card.

21. A method of verifying border crossing control information, comprising:

storing identification information on a chip with a radio frequency antenna;

incorporating the chip onto a radio frequency decal attached to at least one item;

incorporating the chip onto a radio frequency card tied to an individual connected to the at least one item;

reading the identification information from the radio frequency decal and the radio frequency card with a radio frequency reader; and

comparing the identification information from the radio frequency decal and the radio frequency card to determine if a match exists.

22. The system of Claim 20, wherein the identification information comprises at least one of:

physical characteristics of the individual;

physical characteristics of a vehicle driven by the individual; and

biometric information of the individual;

physical characteristics of the at least one item; and

personal knowledge of the individual.

23. The method of Claim 21, wherein the identification information comprises at least one of:

physical characteristics of the individual;

physical characteristics of a vehicle driven by the individual; and

biometric information of the individual;

physical characteristics of the at least one item; and

personal knowledge of the individual.

24. A system of verifying identification information of an individual at an airport, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

at least one airport identification mechanism incorporating the radio frequency device; and

a radio frequency reader to read information from the radio frequency device.

25. A method of verifying identification information of an individual at an airport, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto at least one airport identification mechanism;

reading the first identification information from the at least one identification mechanism with a radio frequency reader; and

comparing the first identification information with second identification information obtained from the individual to determine if a match exists.

26. The system of Claim 24, wherein the first and second identification information comprises at least one of:

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

27. The method of Claim 25, wherein the first and second identification information comprises at least one of:

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

28. A method of verifying a user is authorized to download a software application, comprising:

storing first identification information on a chip, wherein a radio frequency antenna is embedded on the chip;

incorporating the chip into at least one identification device;

reading the first identification information from the at least one identification device with a radio frequency reader;

accepting second identification information from the user;

comparing the first identification information to the second identification information obtained from the user to verify the identification of the user.

29. A system of verifying registration information of a vehicle, comprising;

a radio frequency device comprising a radio frequency antenna embedded on a chip;

a identification mechanism incorporating the radio frequency device; and

a radio frequency reader to obtain information from the radio frequency device.

30. The system of Claim 29, wherein the identification mechanism is a sticker.

31. The system of Claim 29, wherein the identification mechanism is a window sticker.

32. The system of Claim 29, wherein the radio frequency device further comprises:

information storage capabilities; and

transmission capabilities.

33. The system of Claim 29, wherein the identification mechanism is a retroreflective article.

34. The system of Claim 29, wherein the chip is an integrated circuit.

35. A method of verifying registration information of a vehicle, comprising:

storing first identification information on a chip with a radio frequency antenna;

incorporating the chip onto an identification mechanism attached to the vehicle;

reading the first identification information from the identification mechanism with a radio frequency reader; and

comparing the first identification information with second identification information obtained from a user to determine if a match exists.

36. The method of Claim 35, wherein the identification mechanism is a sticker.

37. The method of Claim 35, wherein the identification mechanism is a window sticker.

38. The method of Claim 35, wherein the radio frequency device further comprises:

information storage capabilities; and

transmission capabilities.

39. The method of Claim 35, wherein the identification mechanism is a retroreflective article.

40. The method of Claim 35, wherein the first and second identification information comprises at least one of:

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

41. The method of claim 35, wherein the chip is an integrated circuit.

42. A system of verifying information, comprising;

a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type; and

a radio frequency reader to read information from the retroreflective integrated circuit product.

43. A system of verifying information, comprising;

a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in integrated circuit, a light retroreflective element, and a carrying layer; and

a radio frequency reader to read information from the retroreflective integrated circuit product.

44. The system of Claim 42, wherein the communication antenna is formed on the reflecting surface of a retroreflective element.

45. A method of verifying information, comprising:

storing first identification information on a retroreflective integrated circuit-sealed product comprising an integrated circuit module with a built-in radio frequency identification type integrated circuit and a communication antenna connected to the radio frequency identification type;

reading first identification information from the retroreflective integrated circuit-sealed product; and

comparing the first identification information with second identification information to determine if a match exists.

46. The method of Claim 45, wherein the first and second identification information comprises at least one of:

physical characteristics of an individual;

biometric information of an individual;

personal knowledge of an individual; and

physical characteristics of an item.

47. The method of Claim 45, wherein the communication antenna is formed on the reflecting surface of a retroreflective element.

48. A method of verifying information, comprising:

storing first identification information on a retroreflective integrated circuit-sealed product comprising a built-in integrated circuit, a light retroreflective element, and a carrying layer;

reading first identification information from the retroreflective integrated circuit-sealed product; and

comparing the first identification information with second identification information to determine if a match exists.

49. The system of Claim 1, wherein the radio frequency identification mechanism includes at least one of:

tamper-proof material;

a bidi-tri-dimensional feature;

a hidden image;

a dot-matrix;

hot stamping;

a moire pattern;

a hot stamped metalized hologram;

microprint;

ultraviolet fluorescence;

light piping;

laser engraving;

metalized striping;

a guilloche pattern;

a cameo effect;

ghost imaging;

a multidimensional hologram;

line artwork;

a photograph;

a colorgram;

a stereogram;

a holomatrix;

an optical variable device;

a combined hologram;

multi-dimensional bar codes; and

security taggant material.

50. The system of Claim 1, wherein the radio frequency identification mechanism is subject to at least one of:

a static bending test;

a heat test;

a rigidity test;

a durability test; and

an abrasion test.

51. The method of Claim 2, wherein the radio frequency identification mechanism includes at least one of:

tamper-proof material;

a bidi-tri-dimensional feature;

a hidden image;

a dot-matrix;

hot stamping;

a moire pattern;

a hot stamped metalized hologram;

microprint;

ultraviolet fluorescence;

light piping;

laser engraving;

metalized striping;

a guilloche pattern;

a cameo effect;

ghost imaging;

a multidimensional hologram;

line artwork;

a photograph;

a colorgram;

a stereogram;

a holomatrix;

an optical variable device;

a combined hologram;

multi-dimensional bar codes; and

security taggant material.

52. The method of Claim 2, wherein the radio frequency identification mechanism is subject to at least one of:

a static bending test;

a heat test;

a rigidity test;

a durability test; and

an abrasion test.

FIGURE 1

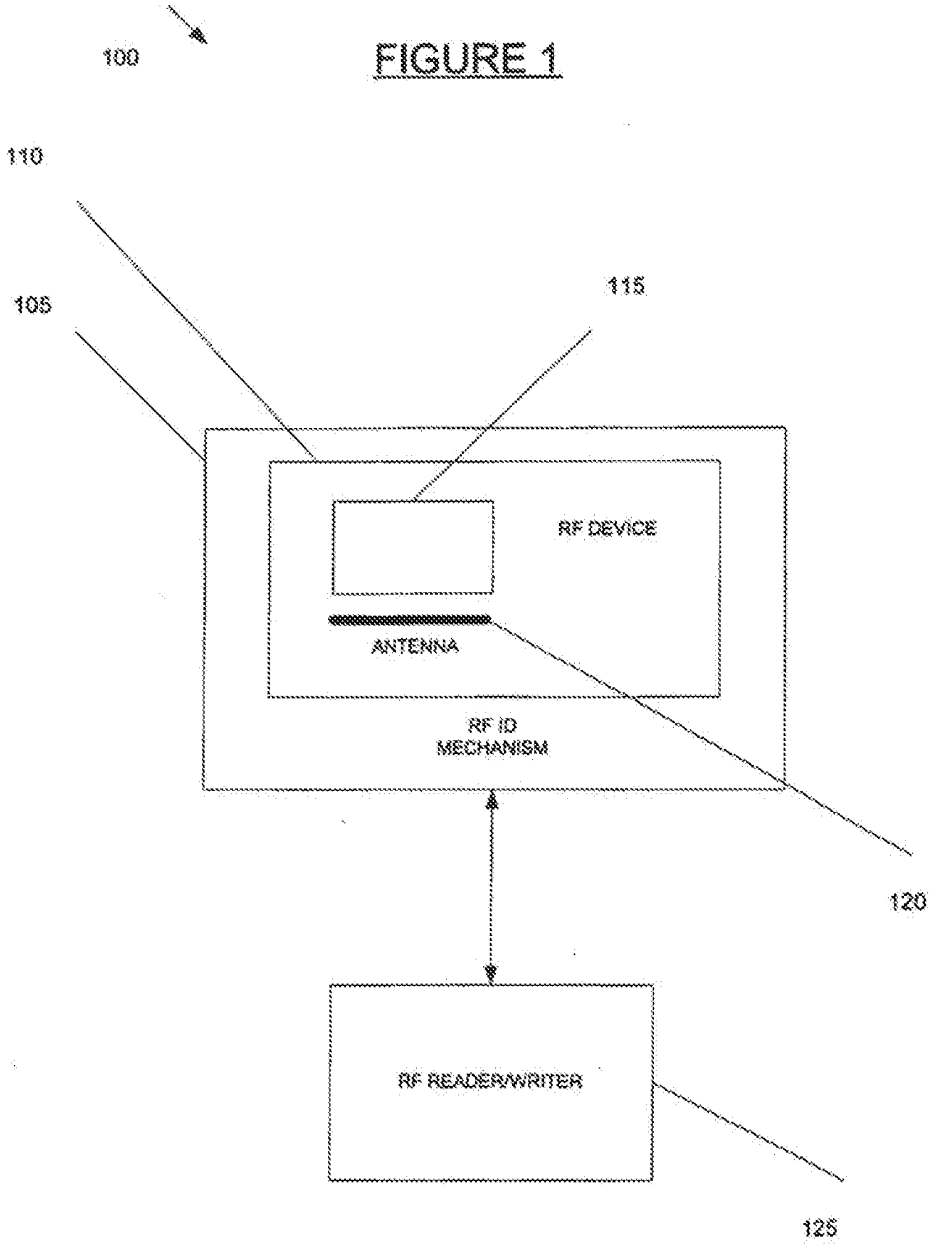

100
110
105
115
RF DEVICE
ANTENNA
RF ID
MECHANISM
120
RF READER/WRITER
125

FIGURE 2

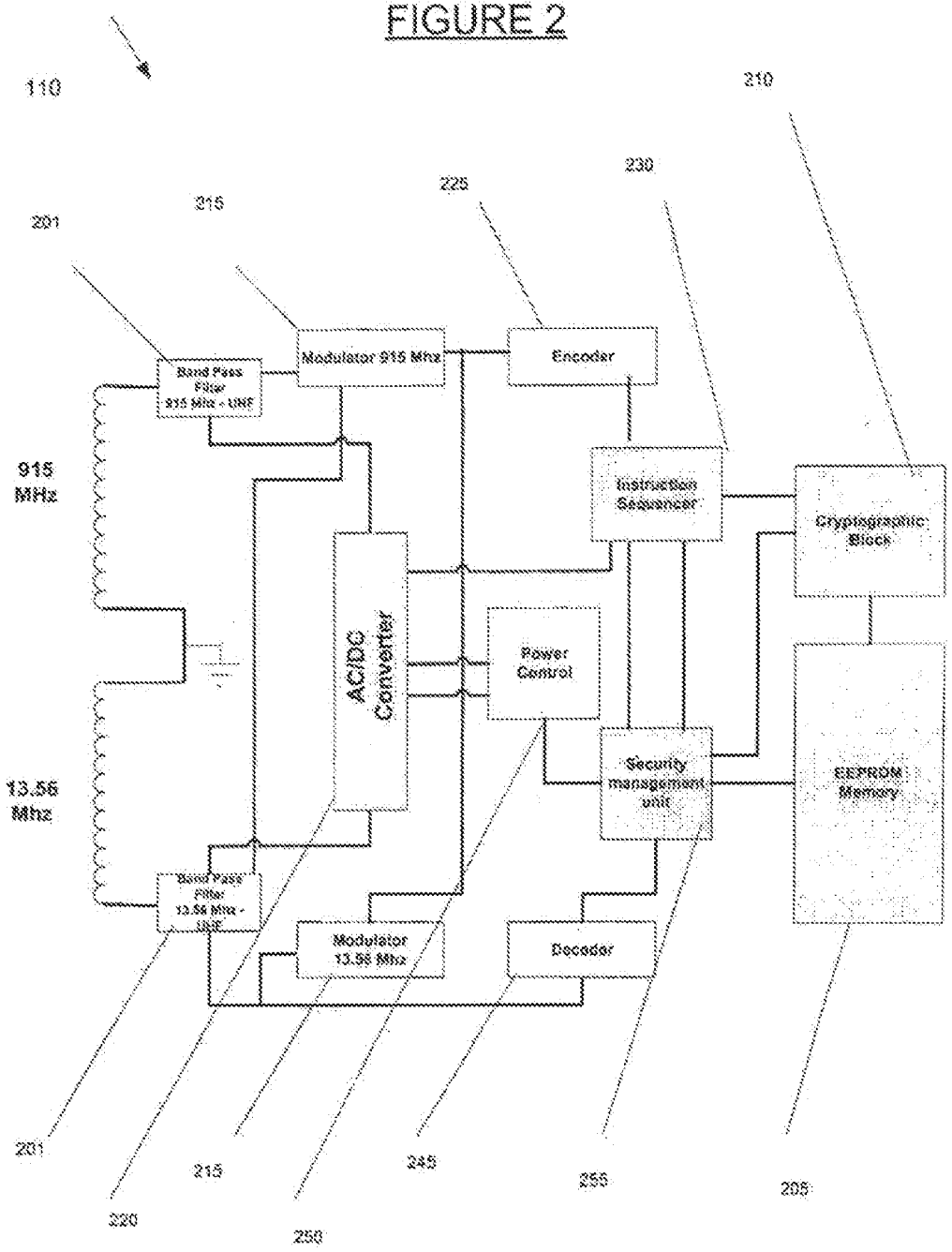

110
210
230
225
215
201
915 MHz
13.56 Mhz
Band Pass Filter 915 Mhz - UHF
Modulator 915 Mhz
Encoder
Instruction Sequencer
Cryptographic Block
AC/DC Converter
Power Control
Security management unit
EEPROM Memory
Band Pass Filter 13.56 Mhz - UHF
Modulator 13.56 Mhz
Decoder
201
215
245
255
205
220
250

FIGURE 3A

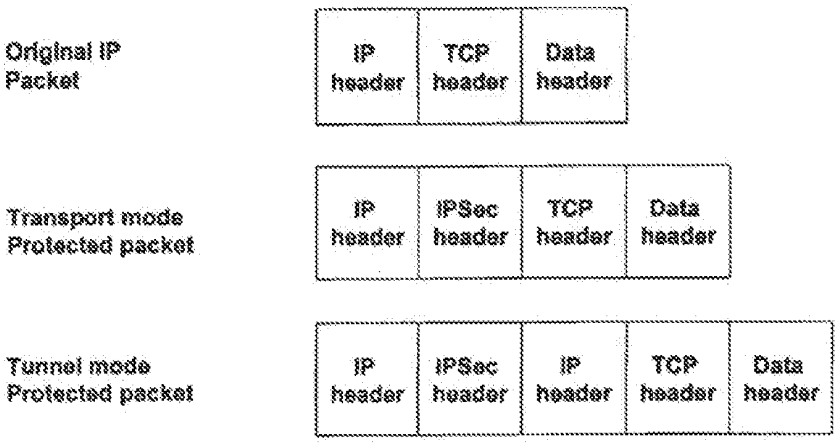
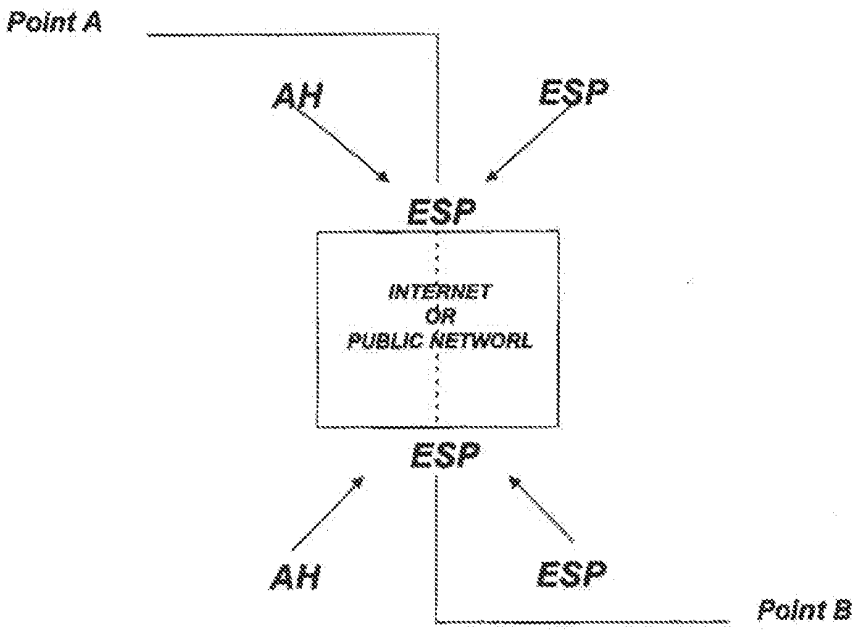

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIGURE 3B


Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORL
ESP
AH
ESP
Point B

400

FIGURE 4

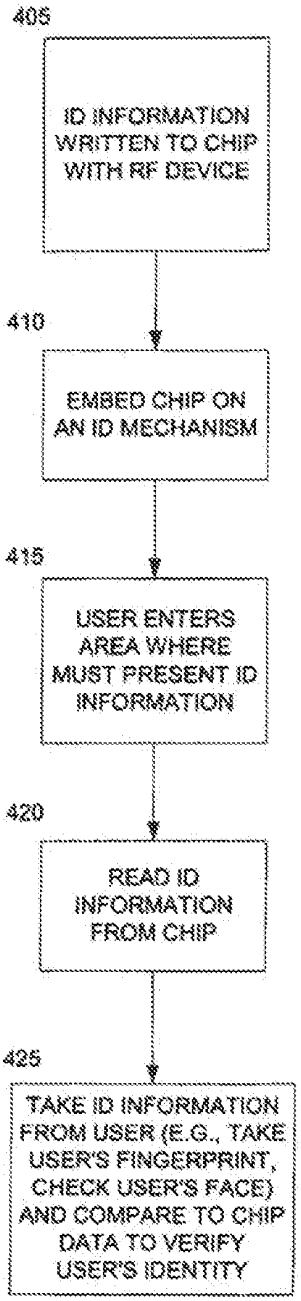

405
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
410
EMBED CHIP ON AN ID MECHANISM
415
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
420
READ ID INFORMATION FROM CHIP
425
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 5

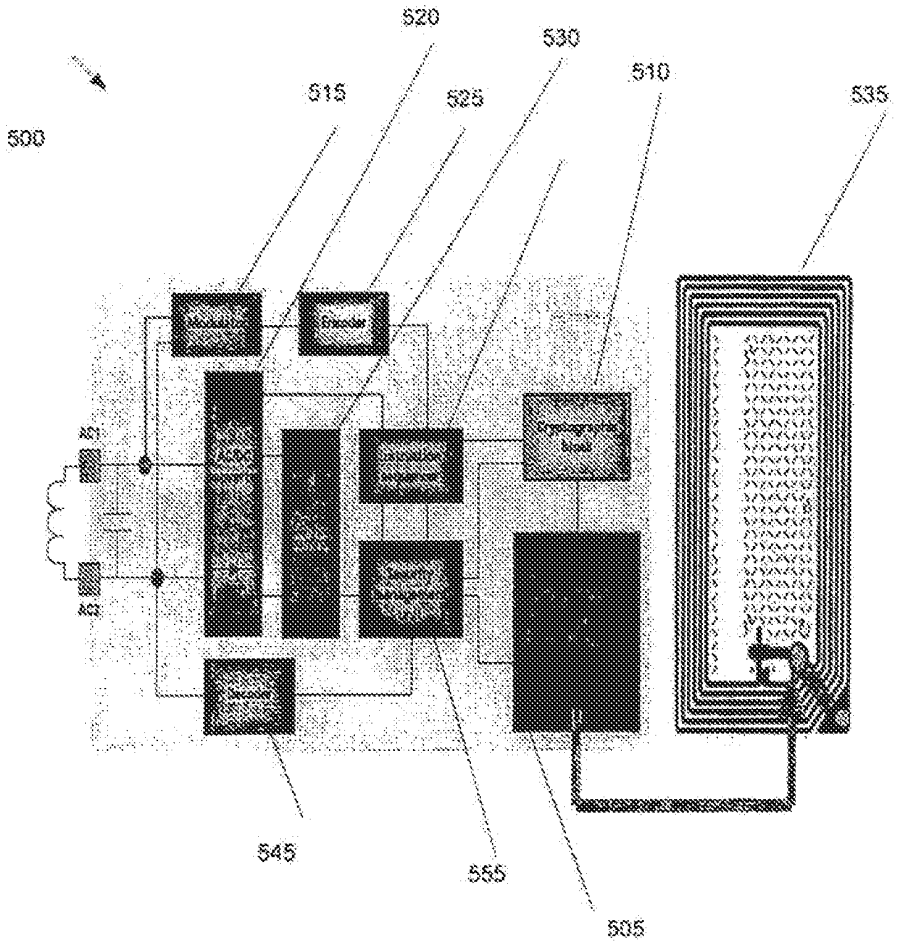


FIGURE 6

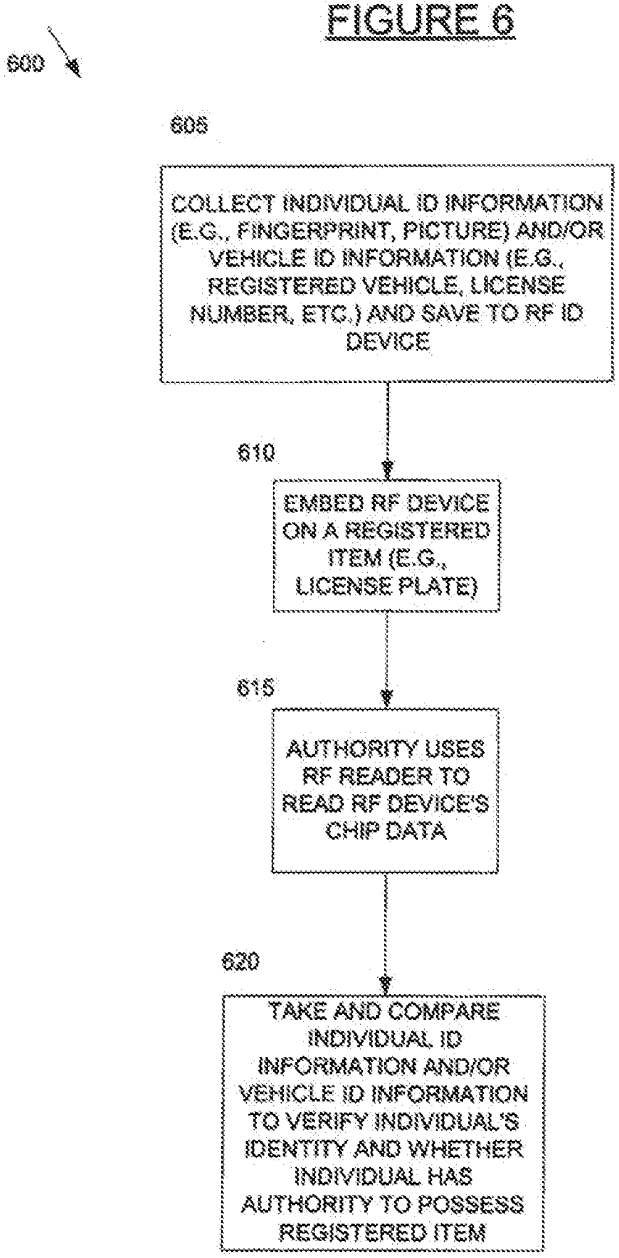

600
605
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
610
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
615
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
620
TAKE AND COMPARE INDIVIDUAL ID INFORMATION AND/OR VEHICLE ID INFORMATION TO VERIFY INDIVIDUAL'S IDENTITY AND WHETHER INDIVIDUAL HAS AUTHORITY TO POSSESS REGISTERED ITEM

FIGURE 7

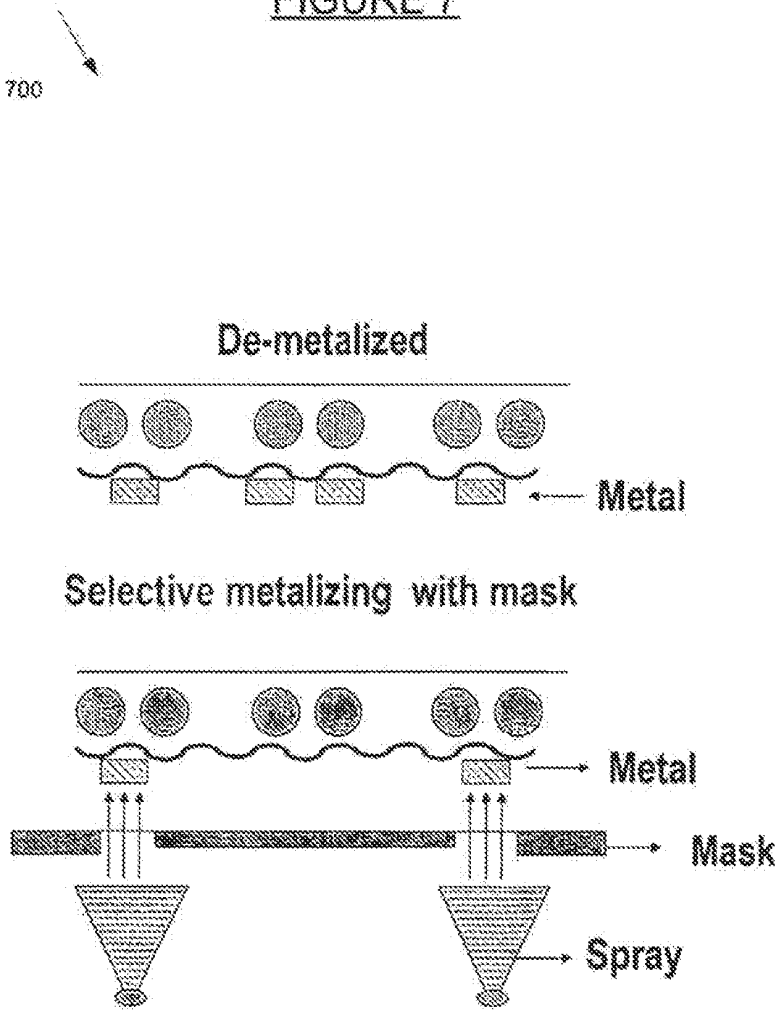

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIGURE 8

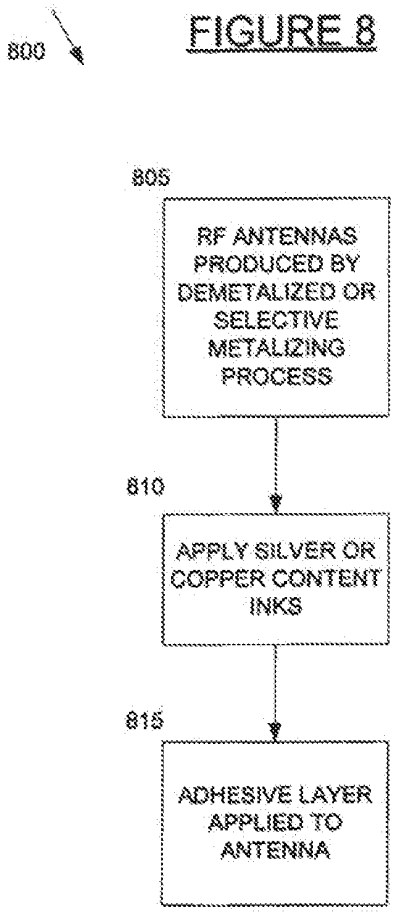

800
805
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
810
APPLY SILVER OR COPPER CONTENT INKS
815
ADHESIVE LAYER APPLIED TO ANTENNA

FIGURE 9

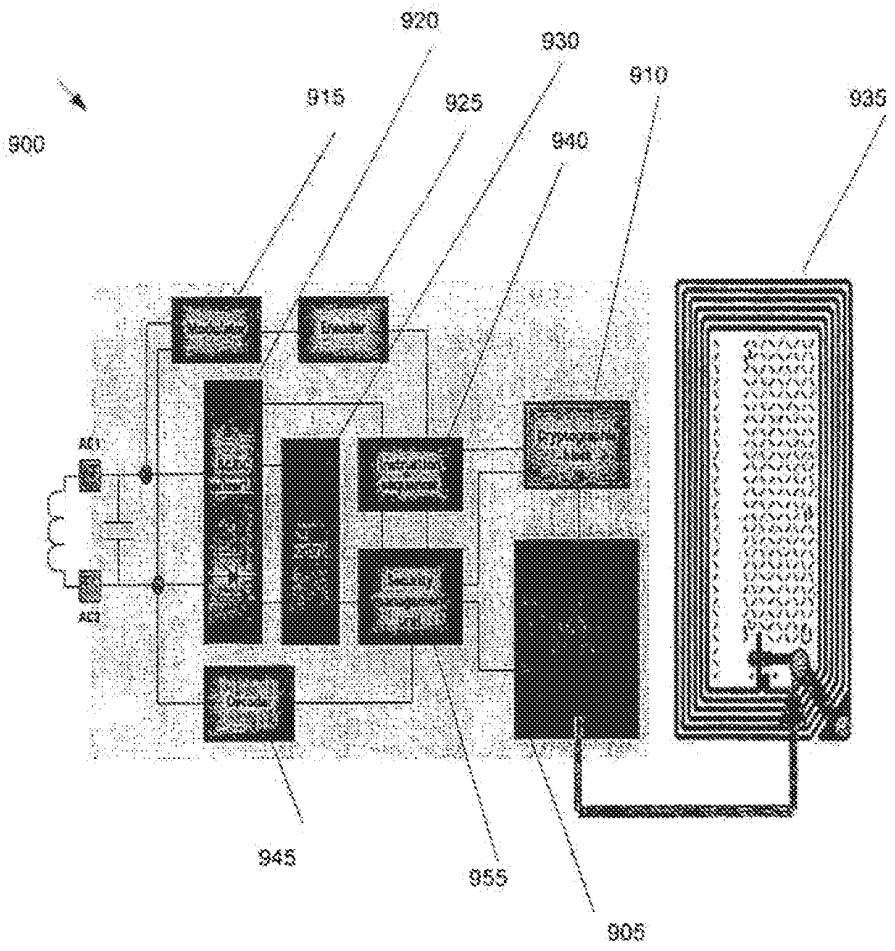


FIGURE 10

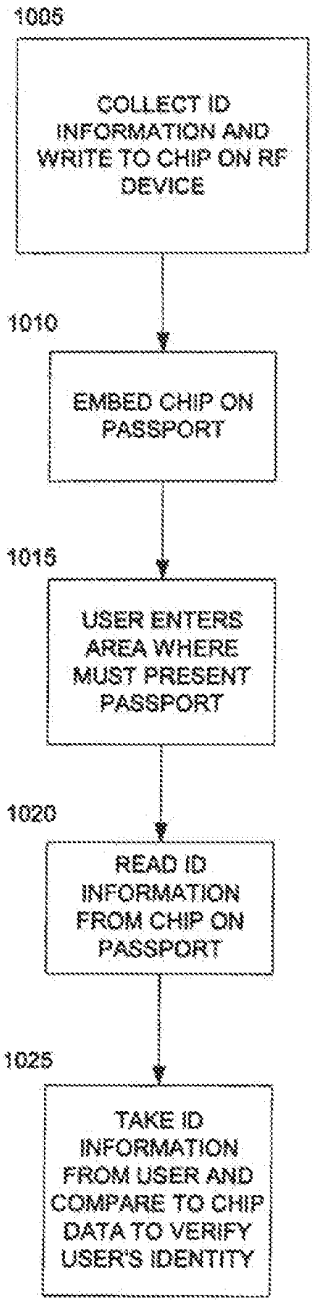

1005
COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1010
EMBED CHIP ON PASSPORT
1015
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1020
READ ID INFORMATION FROM CHIP ON PASSPORT
1025
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 11

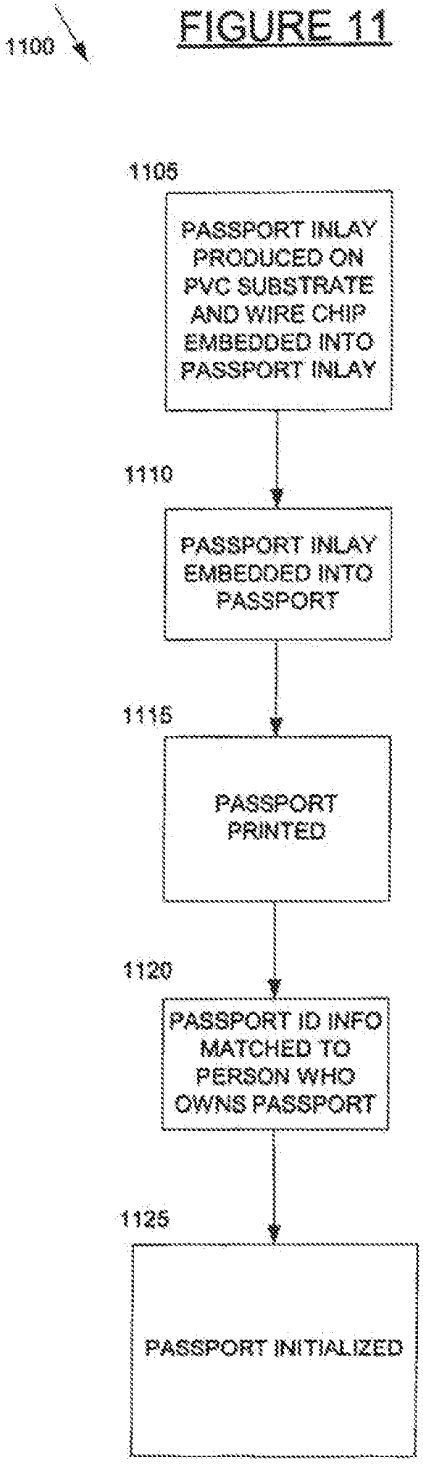

1100
1105
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1110
PASSPORT INLAY EMBEDDED INTO PASSPORT
1115
PASSPORT PRINTED
1120
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1125
PASSPORT INITIALIZED

FIGURE 12

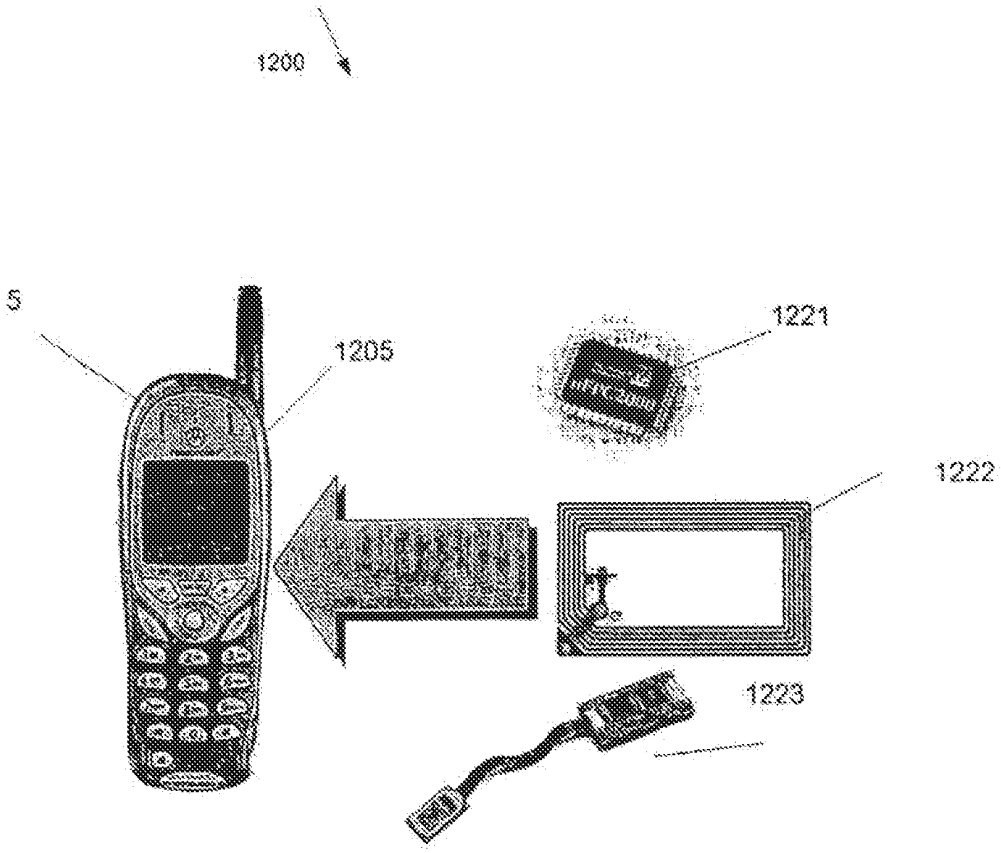


FIGURE 13

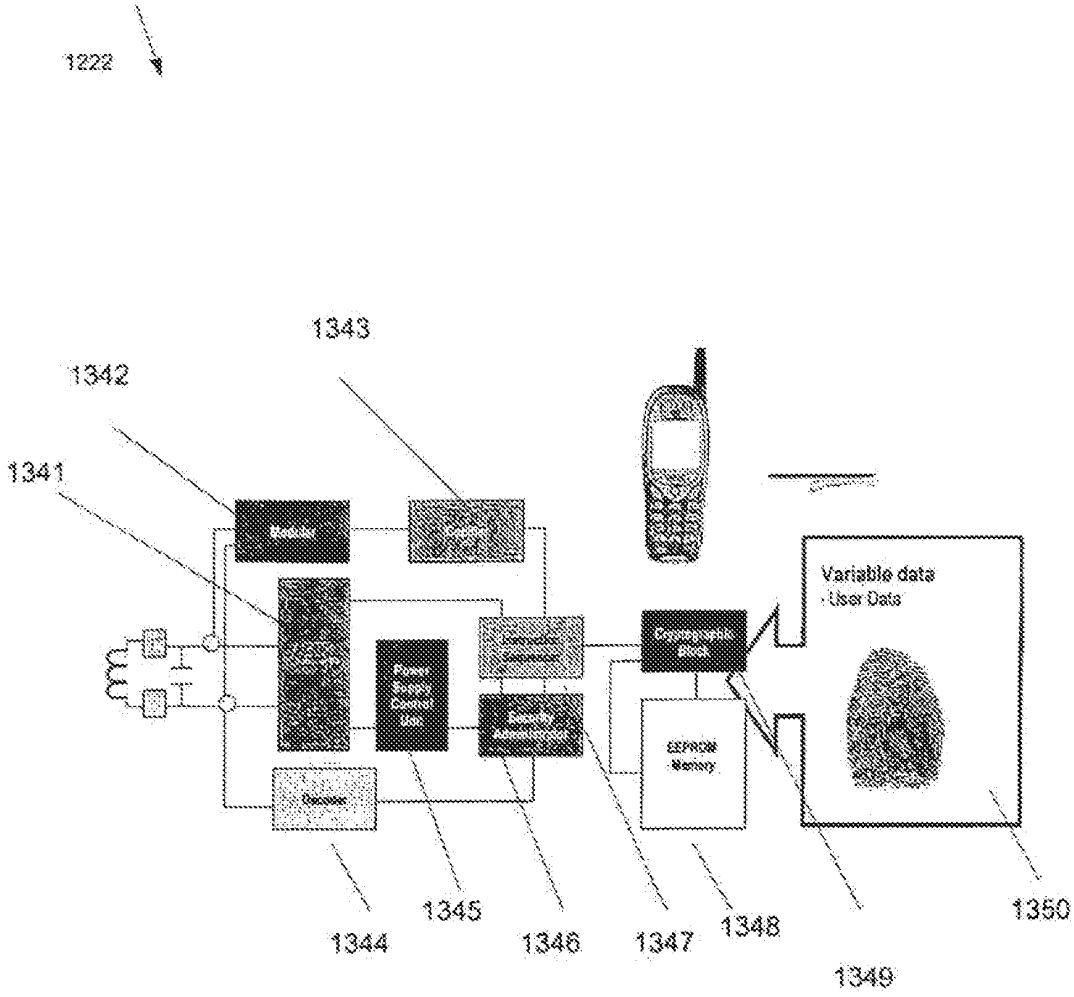

1222
1343
1342
1341
Variable data
· User Data
1344
1345
1346
1347
1348
1349
1350

FIGURE 14

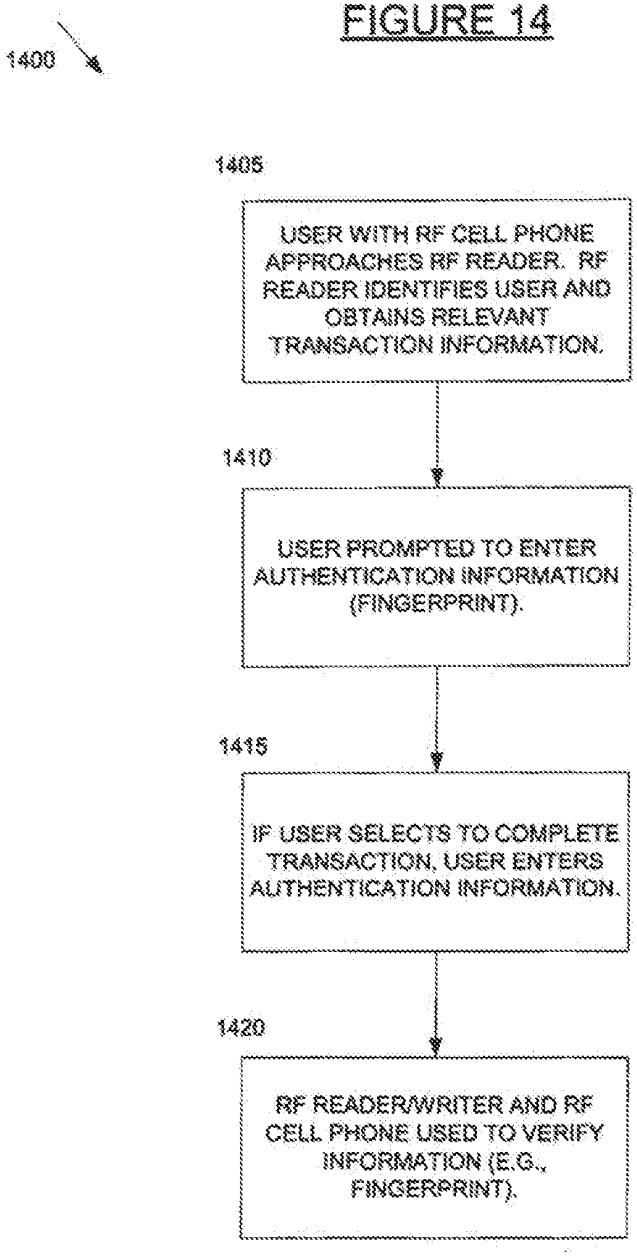

1400
1405
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION.
1410
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT).
1415
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION.
1420
RF READER/WRITER AND RF CELL PHONE USED TO VERIFY INFORMATION (E.G., FINGERPRINT).

FIGURE 15

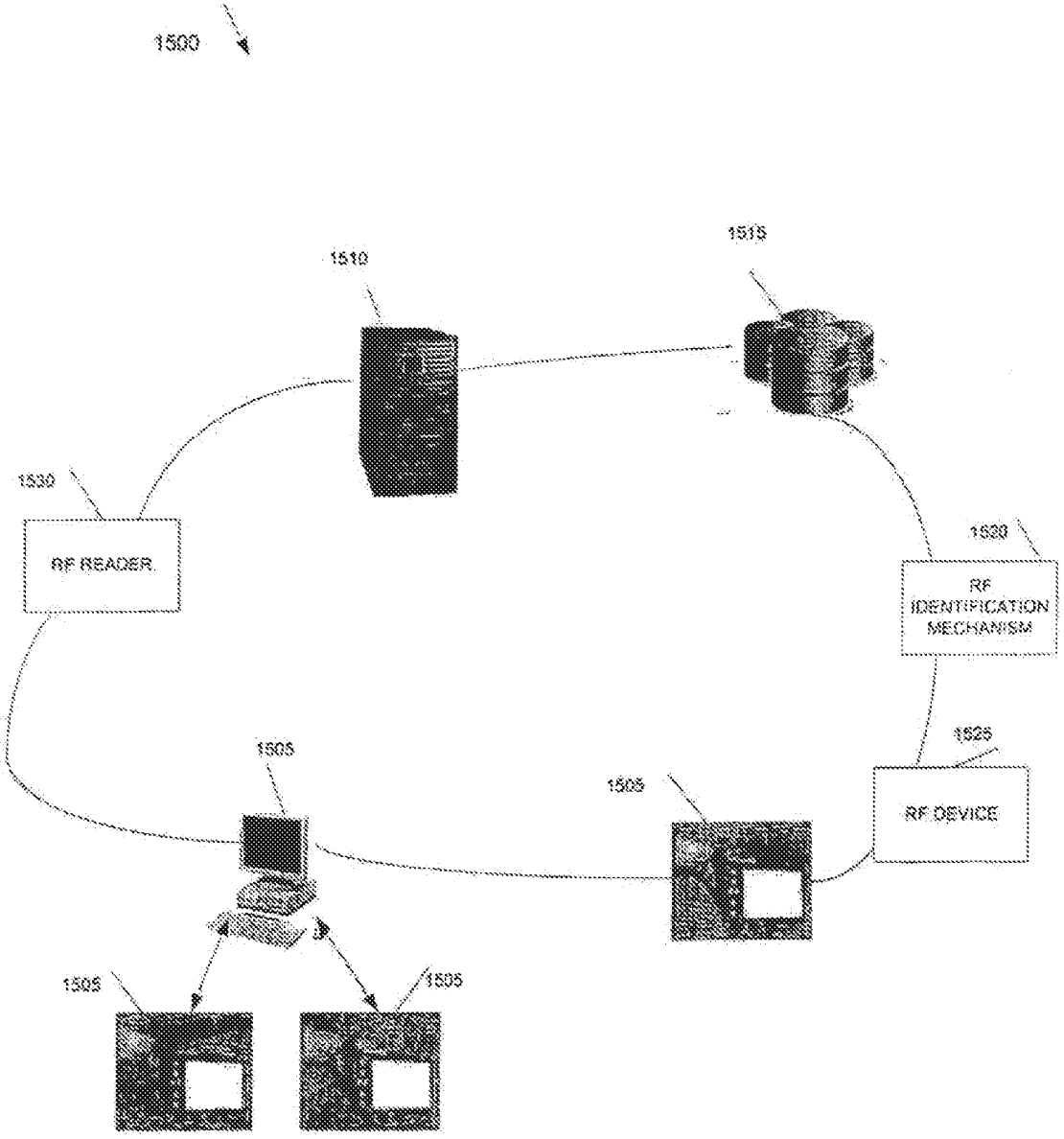

1500
1510
1515
1530
RF READER
1520
RF IDENTIFICATION MECHANISM
1525
RF DEVICE
1505
1505
1505
1505

FIGURE 16

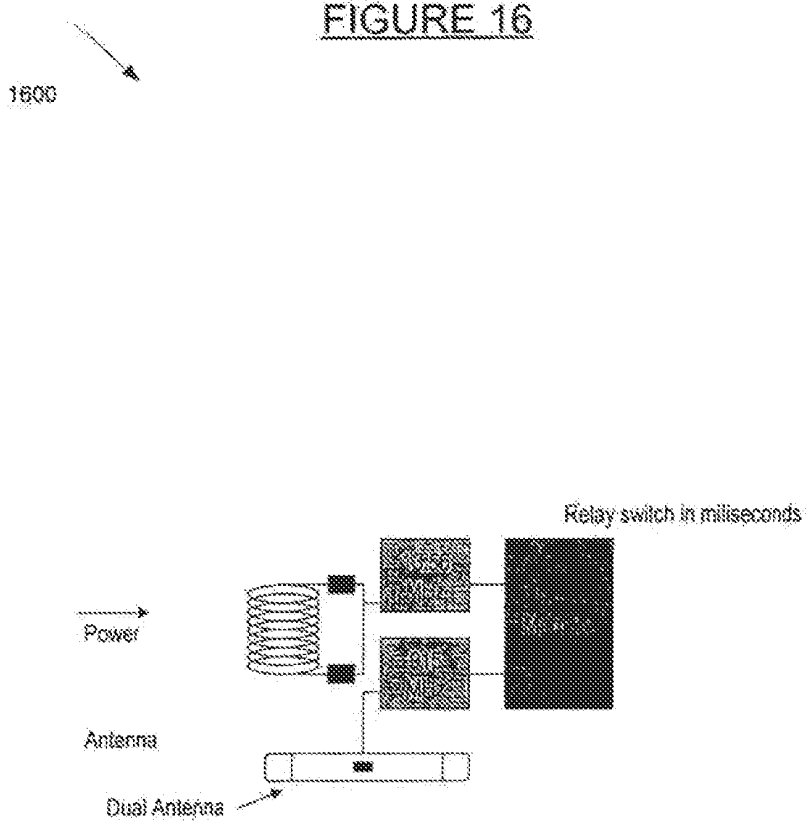

1600
Relay switch in milliseconds
Power
Antenna
Dual Antenna

FIGURE 17

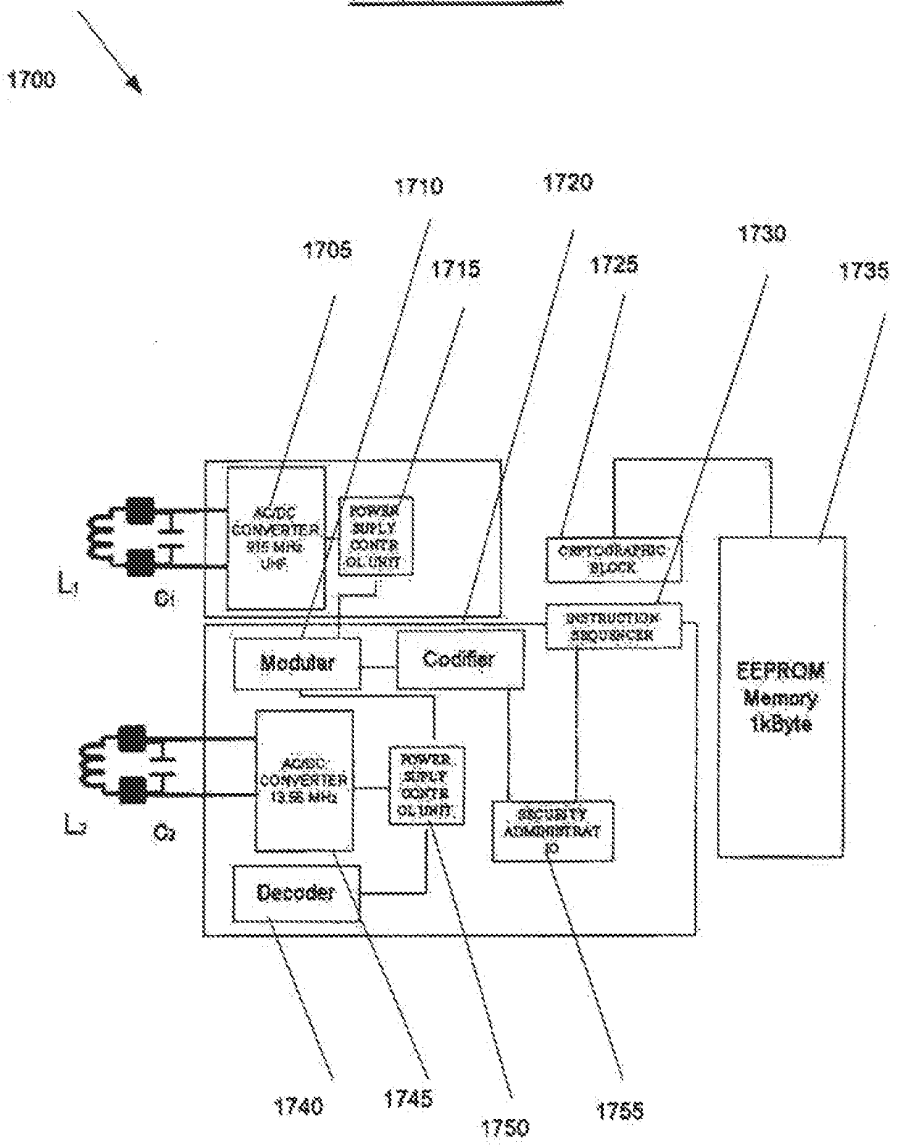

1700
1710
1720
1705
1715
1725
1730
1735
AC/DC CONVERTER 13.56 MHz UNIT
POWER SUPPLY CONTROL UNIT
CRYPTOGRAPHIC BLOCK
INSTRUCTION SEQUENCER
Modulator
Codifier
EEPROM Memory 1kByte
L1
C1
L2
C2
AC/DC CONVERTER 13.56 MHz
POWER SUPPLY CONTROL UNIT
SECURITY ADMINISTRATOR
Decoder
1740
1745
1750
1755

FIGURE 18

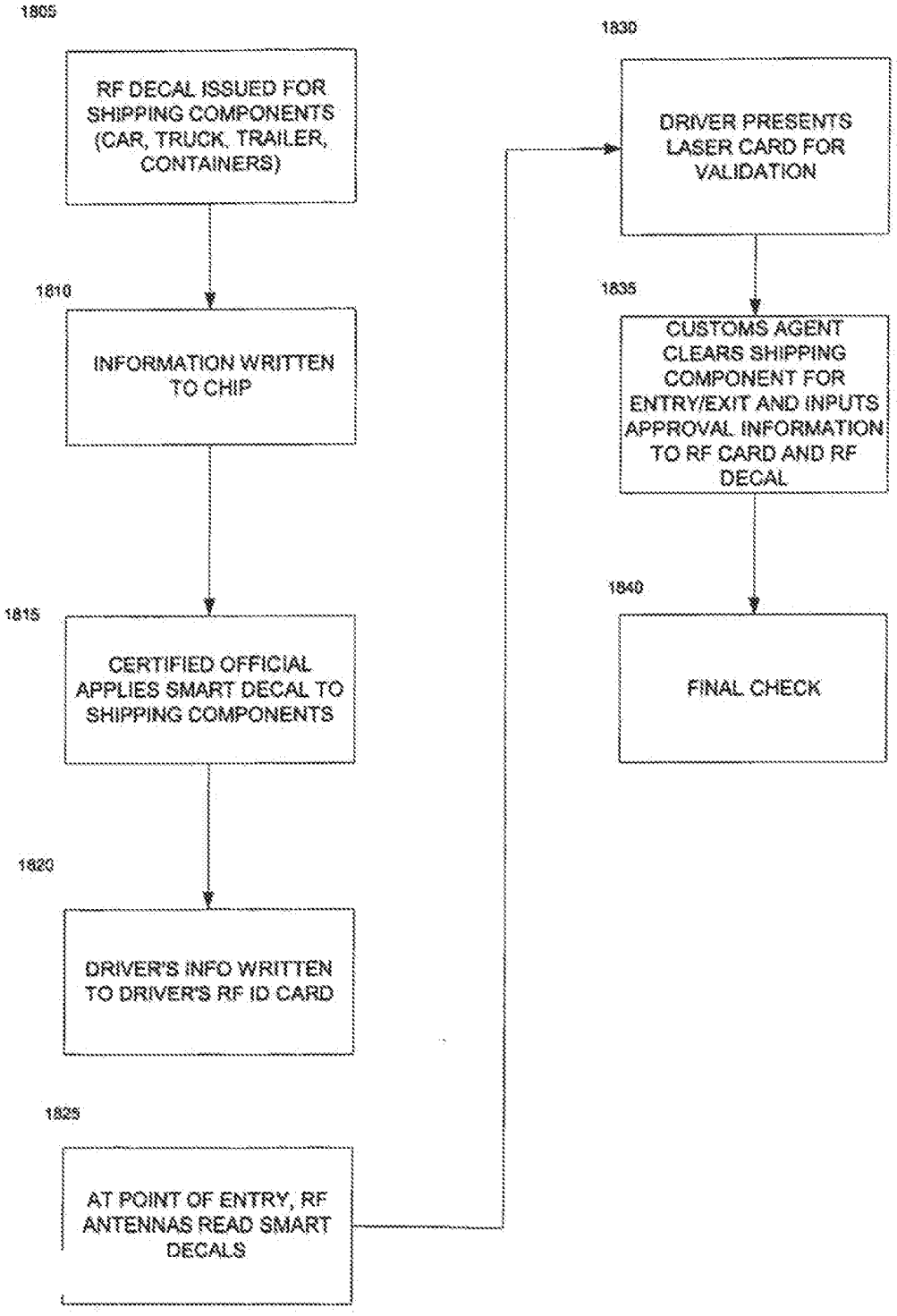

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS LASER CARD FOR VALIDATION
1835
CUSTOMS AGENT CLEARS SHIPPING COMPONENT FOR ENTRY/EXIT AND INPUTS APPROVAL INFORMATION TO RF CARD AND RF DECAL
1840
FINAL CHECK

FIGURE 19

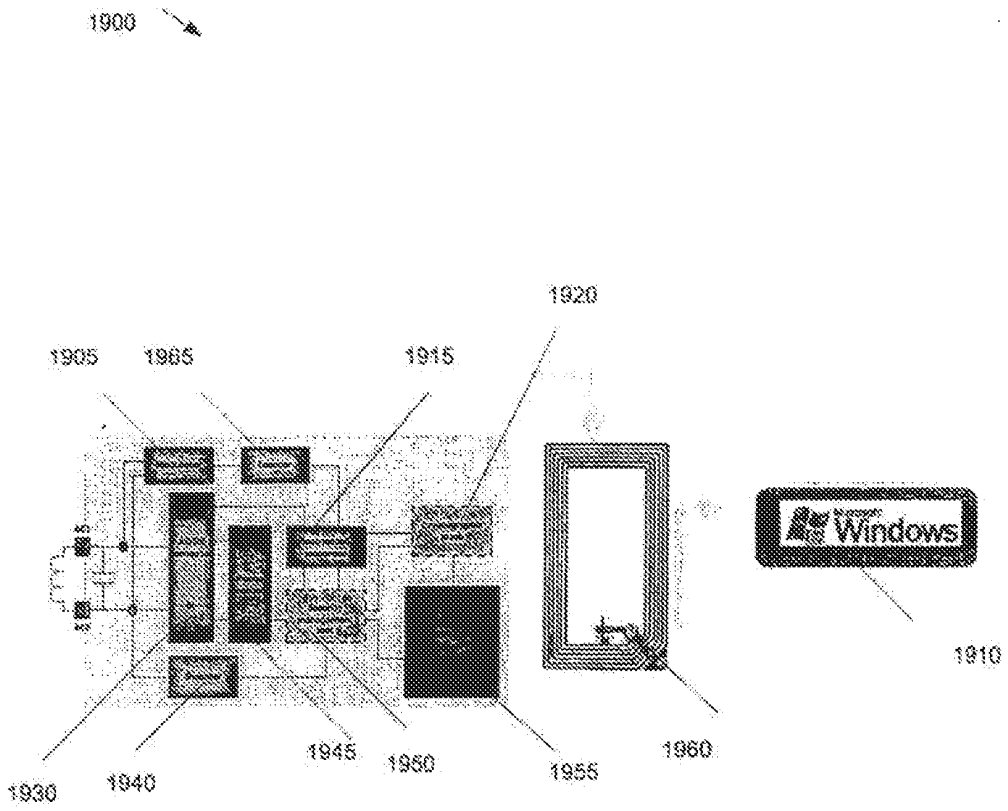
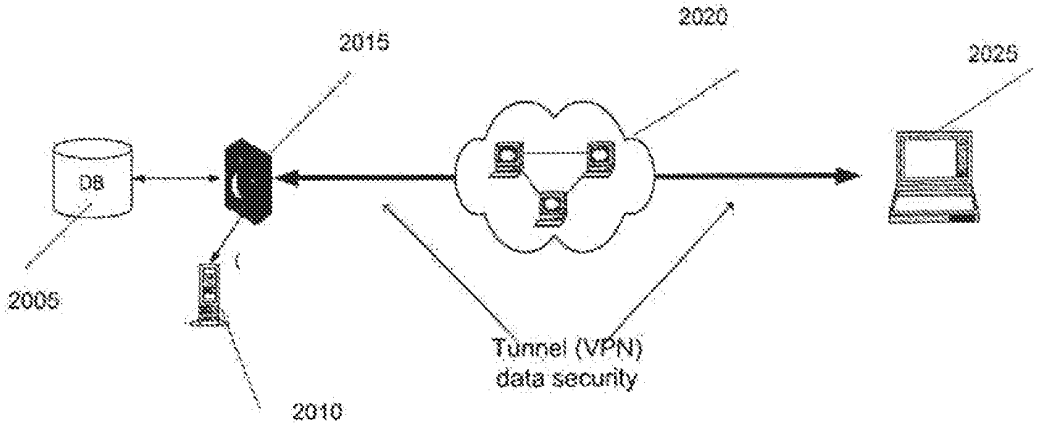

1900
1920
1905
1906
1915
Windows
1910
1930
1940
1945
1950
1955
1960

FIGURE 20



2100

FIGURE 21

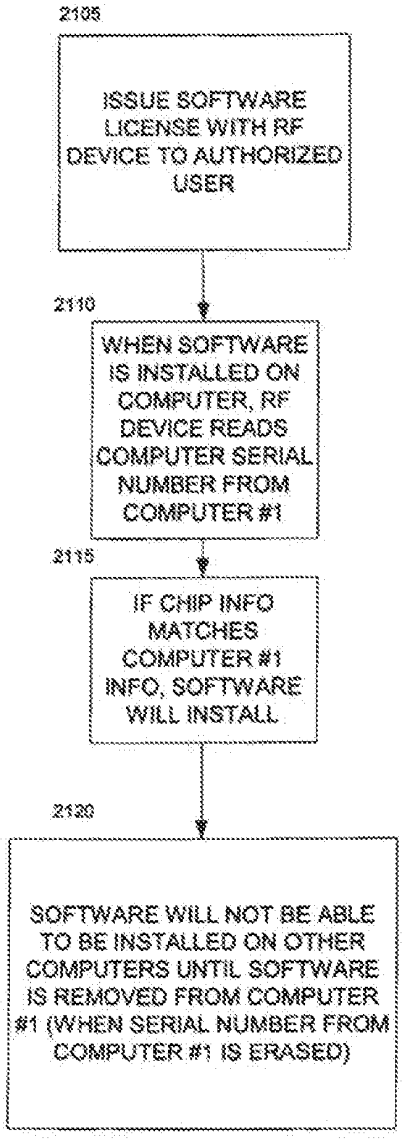


FIGURE 22

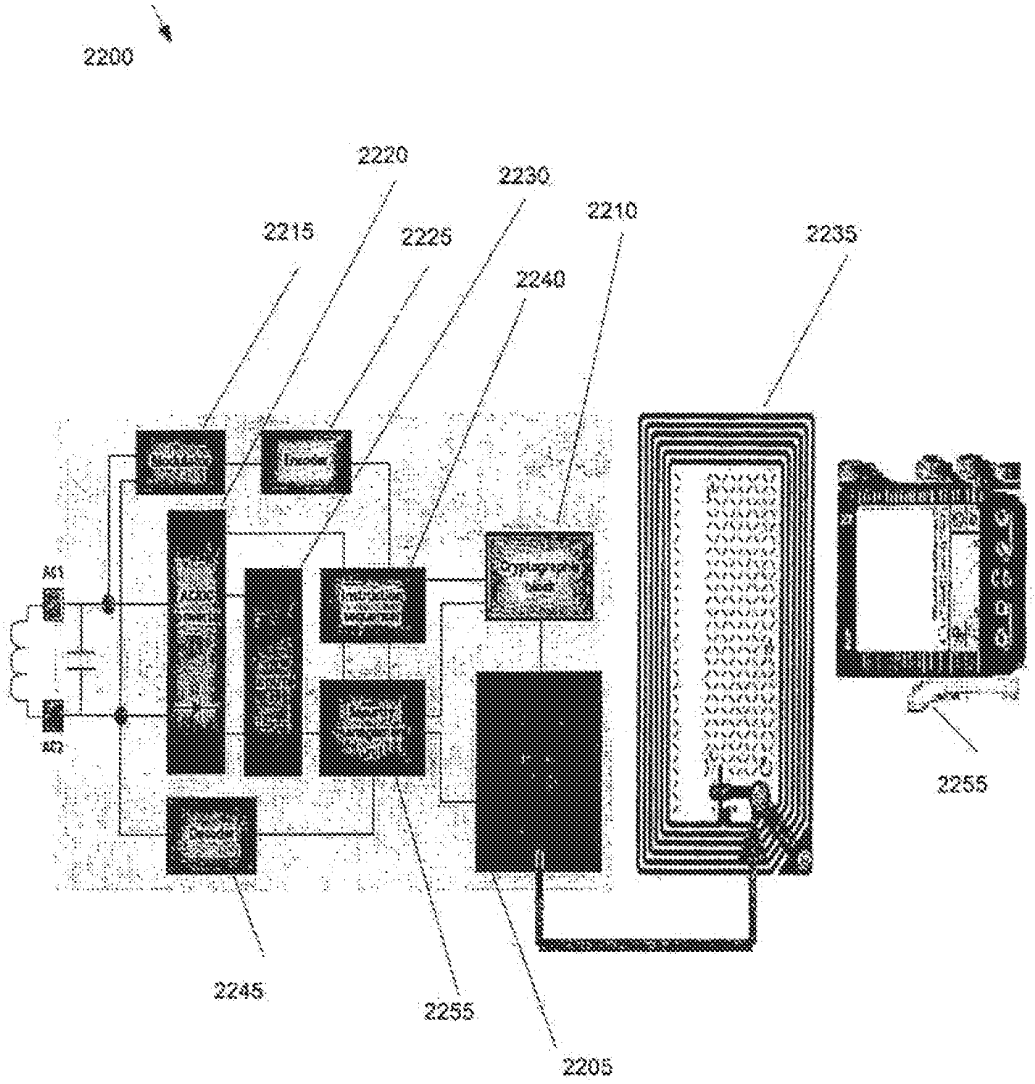
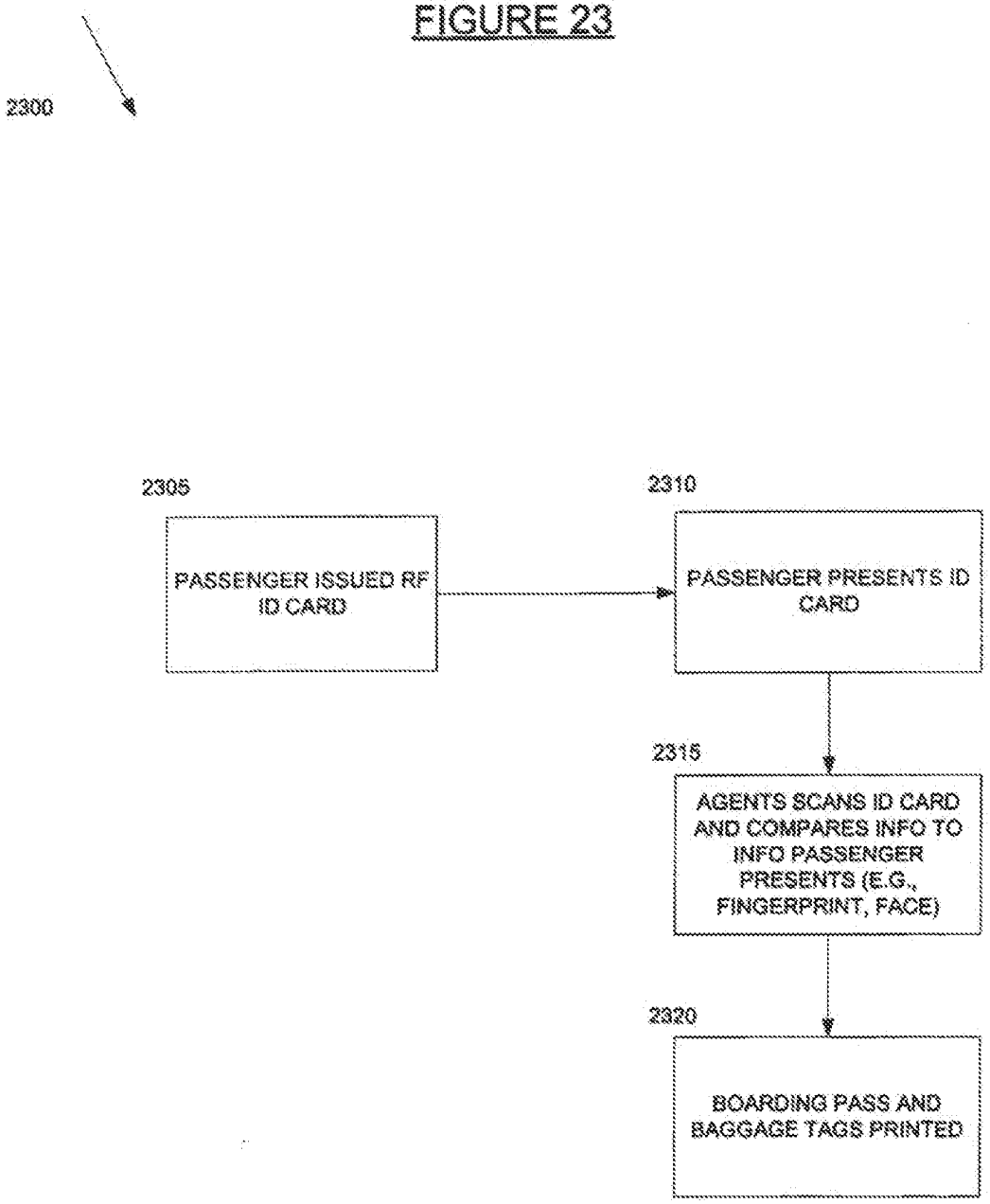


FIGURE 23


2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENTS SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

INTERNATIONAL SEARCH REPORT

Internat ... lication No
PCT/IB 03/03702

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00 G06K19/07 G06K19/10

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

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)
WPI Data, PAJ, IBM-TDB, INSPEC, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 268 796 B1 (LINDER STEFAN ET AL) 31 July 2001 (2001-07-31) claim 1	1,2,49, 51,52
X	DE 196 08 757 A (BROSOW JOERGEN) 11 September 1997 (1997-09-11) abstract; figure 1	1,2,49, 51,52
X	US 6 276 607 B1 (SATO KAZUO) 21 August 2001 (2001-08-21) abstract; figure 1	1,2,49, 51,52

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 December 2003	12/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax. (+31-70) 340-3016	Chiarizia, S

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int[illegible] Application No.
PCT/IB 03/03702

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

2. ☒ Claims Nos.: 3-48
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:
see FURTHER INFORMATION sheet PCT/ISA/210

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:

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.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 3-48

In view of the large number and also the wording of the claims presently on file, which render it difficult, if not impossible, to determine the matter for which protection is sought, the present application fails to comply with the clarity and conciseness requirements of Article 6 PCT (see also Rule 6.1(a) PCT) to such an extent that a meaningful search is impossible. Consequently, the search has been carried out for those parts of the application which do appear to be clear (and concise), namely, claims 1,2,49-52.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

Interna plication No
PCT/IB 03/03702

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6268796 B1	31-07-2001	NONE	
DE 19608757 A	11-09-1997	DE 19608757 A1	11-09-1997
		AU 1879997 A	22-09-1997
		WO 9733252 A1	12-09-1997
US 6276607 B1	21-08-2001	JP 2000122558 A	28-04-2000

Form PCT/ISA/210 (patent family annex) (July 1998)

Espacenet

Bibliographic data: JP2002042076 (A) — 2002-02-08

NON-CONTACT DATA CARRIER AND BOOKLET THEREWITH

Inventor(s): NISHIKAWA SEIICHI ± (NISHIKAWA SEIICHI)

Applicant(s): DAINIPPON PRINTING CO LTD ± (DAINIPPON PRINTING CO LTD)

Classification: **- international:** ***B42D11/00; B42D15/10; G06K19/00; G06K19/07; G06K19/077; G07D9/00;*** (IPC1-7): B42D11/00; B42D15/10; G06K19/00; G06K19/07; G06K19/077; G07D9/00

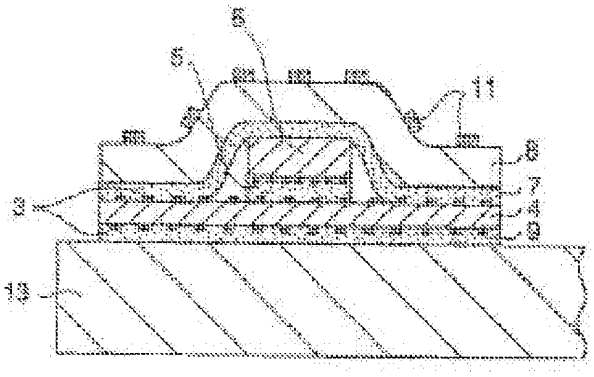
- cooperative:

Application number: JP20000220335 20000721

Priority number (s): JP20000220335 20000721

Abstract of JP2002042076 (A)

PROBLEM TO BE SOLVED: To provide a non-contact data carrier capable of communications even if a long communication distance is set between an external device and an antenna, and a booklet having such a non-contact data carrier, for reducing the causes of failure of an IC chip provided on the booklet, by preventing coil antennas provided on the booklet and the IC chip from being adversely affected by the pressure of a feed roller, and preventing the IC chip from being pressed by booklet sheets when the sheets are bound together into the booklet. SOLUTION: The non-contact data carrier has a non-contact IC chip formed with a second coil antenna and provided in an area of a first sheet of base material in which a first coil antenna is



positioned. The booklet having the non-contact data carrier is characterized in that the data carrier is affixed to the front or back cover thereof.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－42076
（P2002－42076A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/07		Ｂ４２Ｄ　11/00	Ｓ	２Ｃ００５
Ｂ４２Ｄ　11/00		15/10	５０１Ｐ	３Ｅ０４０
15/10	５０１		５０１Ｚ	５Ｂ０３５
			５２１	
	５２１	Ｃ０７Ｄ　9/00	４３６Ａ	

審査請求　未請求　請求項の数12　ＯＬ　（全　７　頁）　最終頁に続く

(21)出願番号　特願2000－220335(P2000－220335)

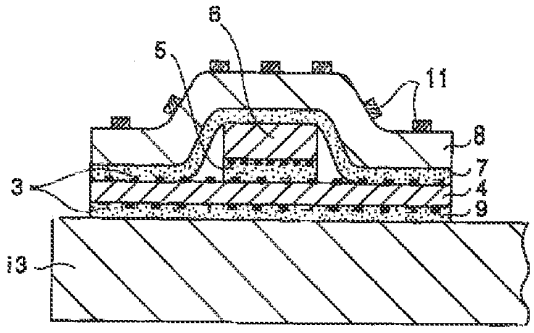
(22)出願日　平成12年７月21日(2000.7.21)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　西川　誠一
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100111659
弁理士　金山　聡

Ｆターム(参考)　2C005 HA01 HB02 HB09 JA26 KA06
KA37 KB05 LB20 MA01 MA10
MB01 MB03 NA09 PA01 PA14
PA18
3E040 AA07 BA07 BA16 CB01 FK05
5B035 BA03 BB09 CA01 CA23

(54)【発明の名称】　非接触型データキャリア及び非接触型データキャリアを有する冊子

(57)【要約】
【課題】　外部装置のアンテナとの通信距離を長く設定させても交信ができるようにした非接触型データキャリアと、更に送りローラーによる冊子に設けたコイルアンテナやＩＣチップに対する圧力による悪影響を受けず、冊子を綴じ合わせた場合に、本文用紙でＩＣチップが押されないようにし、ＩＣチップの故障の原因を少なくするようにした非接触型データキャリアを有する冊子を提供する。
【解決手段】　第１のコイルアンテナを有する第１の基材シートの前記第１のコイルアンテナが配置された領域上に、第２のコイルアンテナが形成された非接触型ＩＣチップが設けられてなる非接触型データキャリアと、前記非接触型データキャリアが、冊子の表表紙または裏表紙に貼付されてなることを特徴とする非接触型データキャリアを有する冊子。



【特許請求の範囲】
【請求項１】　第１のコイルアンテナを有する第１の基材シートの前記第１のコイルアンテナが配置された領域上に、第２のコイルアンテナが形成された非接触型ＩＣチップが設けられてなることを特徴とする非接触型データキャリア。
【請求項２】　前記第２のコイルアンテナが、前記第１の基材シート側に接着されていることを特徴とする請求項１記載の非接触型データキャリア。
【請求項３】　前記非接触型データキャリアが略三角形状で形成され、前記第１のコイルアンテナが略三角形状に配線されていることを特徴とする請求項１記載の非接触型データキャリア。
【請求項４】　前記非接触型ＩＣチップが、下面側に接着層が形成された第２の基材シートにより上方から覆われる状態で接着されていることを特徴とする請求項１記載の非接触型データキャリア。
【請求項５】　前記第１の基材シートの下面側に、接着剤層と剥離紙とが順次設けられている特徴とする請求項１記載の非接触型データキャリア。
【請求項６】　第１のコイルアンテナを有する第１の基材シートの前記第１のコイルアンテナが配置された領域上に、第２のコイルアンテナが形成された非接触型ＩＣチップが設けられてなる非接触型データキャリアが、冊子の表表紙または裏表紙に貼付されてなることを特徴とする非接触型データキャリアを有する冊子。
【請求項７】　前記非接触型データキャリアが、前記冊子の表表紙または裏表紙の内側表面の角部付近領域に貼付してなることを特徴とする請求項６記載の非接触型データキャリアを有する冊子。
【請求項８】　前記冊子を綴じ合わせた際に、前記冊子に貼付された非接触型データキャリアと、前記冊子の内側に綴じ合わされた本文用紙とが重合しないように、前記本文用紙の角部付近領域に切り欠き部を設けたことを特徴とする請求項６又は請求項７に記載の非接触型データキャリアを有する冊子。
【請求項９】　前記冊子を綴じ合わせた際に、前記冊子に貼付された非接触型データキャリアの厚さ寸法だけ、前記冊子の内側に綴じ合わされた本文用紙の角部付近領域に切り欠き部を設けたことを特徴とする請求項６～８のいずれか１項に記載の非接触型データキャリアを有する冊子。
【請求項１０】　前記冊子が、預金通帳またはパスポートであることを特徴とする請求項６～９のいずれか１項に記載の非接触型データキャリアを有する冊子。
【請求項１１】　前記非接触型データキャリアの表面と、前記冊子の前記非接触型データキャリアが貼付された側の表面とに、同一の地紋印刷が施されていることを特徴とする請求項６～１０のいずれか１項に記載の非接触型データキャリアを有する冊子。
【請求項１２】　前記冊子には、非接触型データキャリアを貼付する位置を示すマークが印刷されていることを特徴とする請求項６～１１のいずれか１項に記載の非接触型データキャリアを有する冊子。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、外部処理装置との通信を非接触で行うことができるコイルアンテナが形成されたＩＣチップが内蔵された非接触型データキャリア及び非接触型データキャリアを有する冊子に関するものである。
【０００２】
【従来の技術】従来から、外部処理装置との通信を非接触で行うことができる非接触型ＩＣ記憶媒体として、例えば非接触型ＩＣカード等が一般に知られている。これらの非接触型ＩＣカードは、通常プラスチック製であり、例えばポリ塩化ビニル基材による０．７６ｍｍの厚さのカードの内部に、信号の入出力を非接触で行うデータ通信用コイルと該データ通信用コイルに接続したＩＣチップ（半導体集積回路）からなる非接触ＩＣモジュールを内蔵させて非接触型ＩＣカードを構成するのが一般的である。
【０００３】これらの非接触型ＩＣカードは、通常プラスチック製であるため内蔵する非接触ＩＣモジュールの形状によって、カード基材の加工・成形が必要なことからカードの製品価格が比較的高く、非接触方式の顧客サービスシステムを導入してサービスの改善を図ろうとする各業界の動向を阻害する要因にもなっている。
【０００４】また、最近では非接触ＩＣモジュールの薄型化が可能となり、カード基材にポリエチレンテレフタレート基材を用いて、例えば０．２５ｍｍの厚さの非接触型ＩＣカードも開発されているが、これらの非接触ＩＣ記憶媒体としての非接触型ＩＣカードは、プラスチック製であるため各種の情報やデータを記入したり、プリンター等により印字したい場合にも、記入や印字をすることが出来ないので、データ記入や印字が必要な通帳やパスポート等の各種冊子には適さないという問題がある。
【０００５】このため、冊子に非接触ＩＣ記憶手段を設けるために、非接触ＩＣモジュールを内蔵させた樹脂製シートにより表表紙または裏表紙を形成して、この表表紙と裏表紙の間に冊子の本文用紙を綴じ合わせて、紙製の本文用紙に記入することができるようにした冊子も開発され公知となっている。しかしながら、これらの冊子は、通常非接触ＩＣモジュールを冊子の表面側に設けた樹脂製シート内の中央付近に内蔵させた構造であるため、例えばこのような構造の冊子を通帳等に用いた場合には、ＡＴＭ装置（自動入金出金装置）によるプリンター印字処理の際に、通帳の中央付近を走行する送りローラーにより、内蔵されたＩＣチップや非接触ＩＣモジュ

ールに圧力が加わり、ＩＣチップや非接触ＩＣモジュールを壊す危険性があるので好ましくない。

【０００６】また、冊子の表表紙または裏表紙に非接触ＩＣモジュールを内蔵させるには、製造コストも高くなる為に、通帳のような再利用することができない印刷物にこれを用いるには資源上も無駄が多く問題がある。また、外部装置と電磁誘導を利用して非接触で交信する場合に、外部装置のアンテナと非接触型データキャリアとの距離を数ミリの至近距離に保つ必要があり、使用に際して読取り精度に問題がある。

【０００７】

【発明が解決しようとする課題】本発明は、従来品に比べて外部装置のアンテナとの通信距離を長く設定させても交信ができるようにした非接触型データキャリアを提供する。また、従来品に比べて外部装置のアンテナとの通信距離を長く設定させても交信ができるようにし、更に、特に通帳等のようなプリンター印字装置による印字処理を行う必要がある用途の冊子に用いた場合も、プリンター印字装置内の送りローラーによる冊子に設けたコイルアンテナやＩＣチップに対する圧力による悪影響をできるだけ受けないように構成すると共に、冊子を綴じ合わせた状態にした場合でも、冊子の内部に綴り合わせた本文用紙でＩＣチップが押されないように工夫され、ＩＣチップの故障の原因を少なくするように構成された非接触型データキャリアを有する冊子を提供するものである。

【０００８】

【課題を解決するための手段】上述の目的を達成するために、本発明の非接触型データキャリアは、第１のコイルアンテナを有する第１の基材シートの前記第１のコイルアンテナが配置された領域上に、第２のコイルアンテナが形成された非接触型ＩＣチップが設けられてなることを特徴とする。

【０００９】また、前記第２のコイルアンテナが、前記第１の基材シート側に接着されていることを特徴とする。更に、前記非接触型データキャリアが略三角形状で形成され、前記第１のコイルアンテナが略三角形状に配線されていることを特徴とする。そして、前記非接触型ＩＣチップが、下面側に接着層が形成された第２の基材シートにより上方から覆われる状態で接着されていることを特徴とする。また、前記第１の基材シートの下面側に、接着剤層と剥離紙とが順次設けられている特徴とする。

【００１０】そして、本発明の非接触型データキャリアを有する冊子は、第１のコイルアンテナを有する第１の基材シートの前記第１のコイルアンテナが配置された領域上に、第２のコイルアンテナが形成された非接触型ＩＣチップが設けられてなる非接触型データキャリアが、冊子の表表紙または裏表紙に貼付されてなることを特徴とする。

【００１１】また、前記非接触型データキャリアが、前記冊子の表表紙または裏表紙の内側表面の角部付近領域に貼付してなることを特徴とする。更に、前記冊子を綴じ合わせた際に、前記冊子に貼付された非接触型データキャリアと、前記冊子の内側に綴じ合わされた本文用紙とが重合しないように、前記本文用紙の角部付近領域に切り欠き部を設けたことを特徴とする。そして、前記冊子を綴じ合わせた際に、前記冊子に貼付された非接触型データキャリアの厚さ寸法だけ、前記冊子の内側に綴じ合わされた本文用紙の角部付近領域に切り欠き部を設けたことを特徴とする。

【００１２】また、前記冊子が、預金通帳またはパスポートであることを特徴とする。更に、前記非接触型データキャリアの表面と、前記冊子の前記非接触型データキャリアが貼付された側の表面とに、同一の地紋印刷が施されていることを特徴とする。そして、前記冊子には、非接触型データキャリアを貼付する位置を示すマークが印刷されていることを特徴とする。

【００１３】

【発明の実施の形態】以下、本発明を図面を用いて詳細に説明する。図１（ａ）は、表面にコイルアンテナが形成された非接触型ＩＣチップの平面図、図１（ｂ）は、表面にコイルアンテナが形成された非接触型ＩＣチップの斜視図、図２（ａ）は、本発明の非接触型データキャリアの実施形態の平面図、図２（ｂ）は、本発明の非接触型データキャリアにおける第１の基材シート上に非接触型ＩＣチップが接着された状態を表面側から見た場合の平面図、図２（ｃ）は、本発明の非接触型データキャリアにおける第１の基材シートの裏面側から見た場合の平面図、図３は、図２（ａ）のＡ－Ａ線断面図、図４は、本発明の非接触型データキャリアを有する冊子の一部断面図、図５は、本発明の非接触型データキャリアを有する冊子の裏表紙を開いた状態を示す斜視図、図６は、本発明の非接触型データキャリアを有する冊子の裏表紙を開いた後、本文用紙の一部をめくった状態を示す斜視図、図７は、本発明の非接触型データキャリアを有する冊子を閉じた状態を示す平面図、図８（ａ），（ｂ）は、それぞれ異なる形状の非接触型データキャリアを貼付する位置を示すマークが印刷されている冊子の一部切り欠き平面図である。

【００１４】本発明の非接触型データキャリア２は、図２，図３に示すように、外部装置と電磁誘導を利用して無線通信をすることができる第１のコイルアンテナ３を有する第１の基材シート４上に、下面側に第２のコイルアンテナ５を有する非接触型ＩＣチップ６が接着され、前記非接触型ＩＣチップ６を覆う状態で前記第１の基材シート４上に、下面側に接着層７が形成された第２の基材シート８が接着されている。図２（ａ）及び図２（ｂ）に示すように、第２の基材シート８の下側に、上側に第１のコイルアンテナ３が配置された第１の基材シ

ート４及びそれらの第１のコイルアンテナ３が配置された領域の所定位置の上方に非接触型ＩＣチップ６が接着されている。また、図２（ｃ）に示すように、第２の基材シート８の裏面側にも、第１のコイルアンテナ３が配置されている。更に、この非接触型データキャリア２を種々の媒体などに簡単に貼付できるようにするために、前記第１の基材シート４の下面側に、接着剤層９と剥離紙１０とを順次設けることが好ましい。これにより、剥離紙１０を剥離するだけで接着剤層９により簡単に非接触型データキャリア２を貼付することができる。

【００１５】更に、第２の基材シート８の上面に種々の地紋印刷１１を施してもよく、この地紋印刷１１は非接触型データキャリア２を貼付する媒体に施す地紋印刷などと同一の模様にすることが不正行為の防止上も好ましい。また、前記第１のコイルアンテナ３及び前記非接触型データキャリア２は、貼付する冊子の角部付近に貼り付けることを考慮して、略三角形状に構成することが好ましい。非接触型データキャリア２を略三角形状に構成することで、第１のコイルアンテナ３の配線のできるだけたくさん配線させるため、これに合わせて略三角形状に配線させることが好ましい。これにより、外部装置のアンテナとの電磁誘導を利用した無線通信を、比較的離れた距離でも行なうことができる。

【００１６】また、非接触型ＩＣチップ６には、その表面上に図１（ａ），（ｂ）に示すように無線によりデータの交信を可能にするためにコイルアンテナ５が形成されている。この非接触型ＩＣチップ６の作製方法を説明すると、ＩＣチップの端子パッド部分をマスクし、ポリイミド等でチップ表面に厚さ１０μ程度の絶縁皮膜を電着技術で形成し、その後にマスクを剥離する。熱処理により完全絶縁体となり、その後、金属層の密着性向上のために表面を粗面化処理するのが望ましい。そして、無電解Ｎｉメッキにより給電層を形成し、次にフォトレジストでマスクを形成し、電解メッキにより微細コイル配線を行い、最後にレジストと無電解Ｎｉメッキを剥離し、チップ表面上に非接触端子パッドと接続されたアンテナが加工される。尚、Ｎｉだけでなくでも可能である。上記のようにして、例えば、縦横４ｍｍの四角形のＩＣチップ上に、幅が２０μで、線間が２０μ、金属厚が２０μ、の線で約４５ターンのアンテナが得られる。そして、ポリイミド等のオーバーコートによりこれらの微細コイル配線を保護することで、コイルオンチップの非接触型ＩＣチップ６が得られる。

【００１７】更に、第１の基材シート４の表裏面には、第１のコイルアンテナ３と好ましくはコンデンサとを有している。第１のコイルアンテナ３は、銅やアルミニウムなどを使用したエッチング、プリント配線方式による印刷、ワイヤによる形成など当業界で周知いずれの方法によっても形成することができる。第１のコイルアンテナ３が受信する電波は磁束の変化として誘導電流を生成する。かかる誘導電流は、第１のコイルアンテナ３に電磁結合されている非接触型ＩＣチップ６の第２のコイルアンテナ５に誘導電流を生成する。また、第１のコイルアンテナ３は、第２のコイルアンテナ５に流れる電流の変化により誘起された誘導電流から電波を生成して、外部装置のアンテナに送信することができる。

【００１８】このように、第１のコイルアンテナ３は、外部装置のアンテナ及び非接触型ＩＣチップ６と交信することができる通信部として機能する。第１のコイルアンテナ３は、外部装置のアンテナと交信することができる所定の通信距離を有しており、その大きさは調節可能であるため、かかる所定の通信距離も必要に応じて調節することができる。このため、本明の非接触型データキャリア２が、従来のマイクロ波を利用する非接触ＩＣカードの代替物として適用されるならば、上記所定の通信距離を従来の非接触ＩＣカードに求められる通信距離と同様の距離に設定することが可能である。例えば、通信距離を１０ｍｍ程度までにするのであれば第１のコイルアンテナ３を小型に構成し、また数ｃｍ程度であれば中型に構成し、更に１０ｃｍ以上であれば大型に構成することで通信可能な距離を変化させることができる。尚、これらの仕組みは、既に特開２０００－１７２８１２号に公知技術として開示されている。

【００１９】次に、本発明の非接触型データキャリアを有する冊子の実施形態について説明する。図４乃至図７には、非接触型データキャリアを有する冊子として、預金通帳の冊子を一例として示している。本発明の非接触型データキャリアを有する冊子１（以下、冊子１という。）は、前記非接触型データキャリア２を冊子の表表紙または裏表紙に貼付されてなるものである。そして、非接触型データキャリア２を、冊子１の表表紙１２または裏表紙１３の内側表面の角部付近領域に貼付することが好ましい。特に、冊子１が通帳等のような、ＡＴＭ装置のプリンター印字処理を行う用途に用いる媒体の場合には、通帳の中央付近を走行する送りローラーにより内蔵された非接触型データキャリア２がこの送りローラーの影響で圧力が加わり、ＩＣチップが壊れる危険性があるので、冊子１の表表紙１２または裏表紙１３の内側表面の角部付近領域に非接触型データキャリア２を貼付することで、これら送りローラーによる悪影響を回避することができ効果的である。

【００２０】しかしながら、冊子１を綴じ合わせると、内側に綴じ合わされた本文用紙１４が非接触型ＩＣチップ６を押して圧力が加わり損傷や故障の原因となる危険性があり、できるだけ非接触型ＩＣチップ６に余分な圧力を加えないようにするため、冊子１の表表紙１２または裏表紙１３の内側表面の角部付近領域に非接触型データキャリア２を貼付するとともに、図６に示すように冊子１の内側に綴じ合わされた本文用紙１４を表表紙１２または裏表紙１３に重ね綴じ合わせた際に、特に非接触

型データキャリア２に内蔵された非接触型ＩＣチップ６の部分と本文用紙１４とが重合しないように、前記本文用紙１４の角部付近領域に切り欠き部１５を設けた構成としてある。

【００２１】これにより、図６，図７に示すように、冊子１を綴じ合わせた状態にした時に、非接触型データキャリア２に内蔵された非接触型ＩＣチップ６が本文用紙１４により圧力を受けることによる故障等の悪影響を回避することができるものである。前記本文用紙の付近領域に形成する切り欠き部１５の形状は、コーナーカットや角丸等の所望の形状で形成すればよい。

【００２２】また、切り欠き部１５を設ける本文用紙１４は、少なくとも冊子に貼付された非接触型データキャリア２の厚さ寸法分だけの本文用紙１４に形成すればよい。これは、冊子の本文用紙が非接触型データキャリア２の厚さよりもかなり厚い場合には、全ての本文用紙１４に切り欠き部１５を設ける必要はなく、非接触型データキャリア２の厚さ寸法に応じた厚さ分の本文用紙１４の切り欠き部を設けることで、本文用紙１４による非接触型データキャリアへの加圧を回避できるからである。

【００２３】更に、非接触型データキャリア２の第１の基材シート３の表面と、冊子１の非接触型データキャリア２が貼付された側の表面とに、同一の地紋印刷１１を施すことが好ましい。同一の地紋印刷１１を施すことで、もしも不正を目的として非接触型データキャリア２を貼り替えたとしても、地紋印刷１１の部分に違和感ができ不正行為が行われたことをチェックすることができる。

【００２４】更に、冊子１には、非接触型データキャリア２を貼付する位置を示すマーク１６が印刷されている。例えば、図８に示すように、非接触型データキャリア２を貼付する位置を示すマーク１６あらかじめ印刷しておき、非接触型データキャリア２が正確な位置に貼り付けられるようにするようにしておくことが好ましい。図８（ａ）は、長方形状の非接触型データキャリア用のマークで、図８の（ｂ）は、三角形状の非接触型データキャリア用のマークが印刷されている冊子の一部切り欠き平面図を例に示してある。これにより、あらかじめ定めた正しい位置に非接触型データキャリア２の貼付を行なうことができるので、安定した品質の冊子を作製することができる。

【００２５】通常、通帳などの冊子には、表表紙１２と裏表紙１３、そして表表紙１２と裏表紙１３の間に挟み込まれて設けられている本文用紙１４とから構成されているが、本文用紙１４に非接触型データキャリア２を貼付した構成にすると、本文用紙１４をめくる際に非接触型データキャリア２が折れ曲がり、内蔵されている非接触型ＩＣチップ６に余計な応力が加わることで故障の原因となる危険性があり好ましくない。また、通常本文用紙１４には、薄い紙厚の用紙を使用するため、非接触型データキャリア２を貼付すると、使用の際に用紙がちぎれる等の損傷の原因となる危険性がある。

【００２６】また、その冊子１の使用用途に応じて、非接触型データキャリア２を表表紙１２または裏表紙１３の表面や裏面の所望の位置に貼付することで、形態を調整することができるものである。

【００２７】また、特に本発明の冊子は、その冊子が第三者により悪用されては困るような預金通帳やパスポート等に用いると効果的であり、この場合には、非接触型ＩＣチップ８に例えば本人の顔写真データ等の本人を証明する照合データを記憶させておき、外部装置との無線による信号の交信によって照合データの同一性を確認することで預金通帳やパスポート等の冊子の使用の際における確実性を確保できるようにすることが可能となるものである。

【００２８】

【発明の効果】以上、詳細に説明したように、本発明の非接触型データキャリアは、従来品に比べて外部装置のアンテナとの通信距離を長く設定させても交信ができるようにすることができる。また、本発明の非接触型データキャリアを有する冊子は、従来品に比べて外部装置のアンテナとの通信距離を長く設定させても交信ができるので、冊子の外部から電波による交信を行なう場合でも、冊子のアンテナと外部のアンテナとの距離を任意に設定することができ、種々の用途に適応することができる。更に、特に通帳等のようなプリンター印字装置による印字処理を行う必要がある用途の冊子に用いた場合も、プリンター印字装置内の送りローラーによる冊子に設けたコイルアンテナやＩＣチップに対する圧力による悪影響をできるだけ受けないように構成すると共に、冊子を綴じ合わせた状態にした場合でも、冊子の内部に綴り合わせた本文用紙でＩＣチップが押されないように工夫され、ＩＣチップの故障の原因を少なくすることができる。

【図面の簡単な説明】

【図１】（ａ）は、表面にコイルアンテナが形成された非接触型ＩＣチップの平面図、（ｂ）は、表面にコイルアンテナが形成された非接触型ＩＣチップの斜視図である。

【図２】（ａ）は、本発明の非接触型データキャリアの実施形態の平面図、（ｂ）は、本発明の非接触型データキャリアにおける第１の基材シート上に非接触型ＩＣチップが接着された状態を表面側から見た場合の平面図、（ｃ）は、本発明の非接触型データキャリアにおける第１の基材シートの裏面側から見た場合の平面図である。

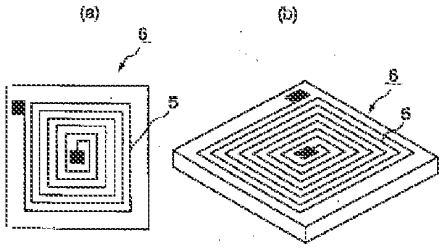
【図３】図２（ａ）のＡ－Ａ線断面図である。

【図４】本発明の非接触型データキャリアを有する冊子の一部断面図である。

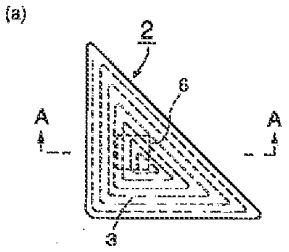
【図５】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた状態を示す斜視図である。

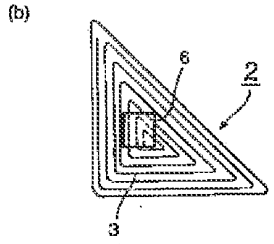
【図６】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた後、本文用紙の一部をめくった状態を示す斜視図である。
【図７】本発明の非接触型データキャリアを有する冊子を閉じた状態を示す平面図である。
【図８】（ａ），（ｂ）は、それぞれ異なる形状の非接触型データキャリアを貼付する位置を示すマークが印刷されている冊子の一部切り欠き平面図である。
【符号の説明】
１　冊子
２　非接触型データキャリア
３　第１のコイルアンテナ
４　第１の基材シート
５　第２のコイルアンテナ
６　非接触型ＩＣチップ
７　接着層
８　第２の基材シート
９　接着剤層
１０　剥離紙
１１　地紋印刷
１２　表表紙
１３　裏表紙
１４　本文用紙
１５　切り欠き部
１６　マーク

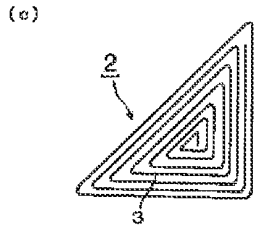
【図１】



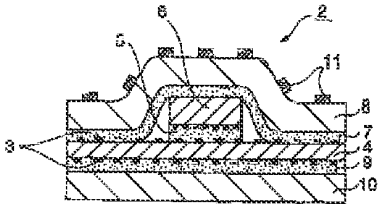
【図２】



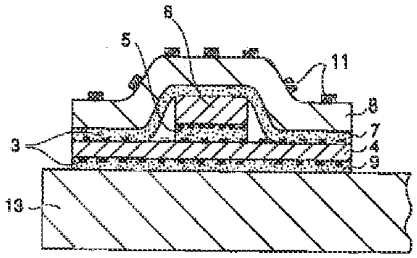




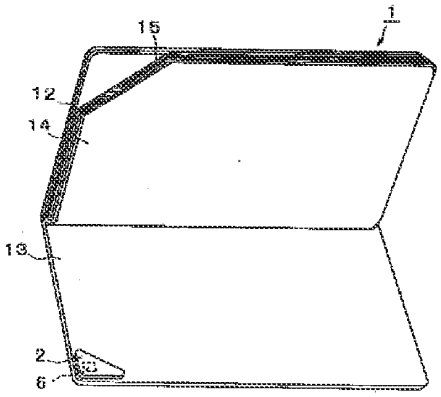
【図３】



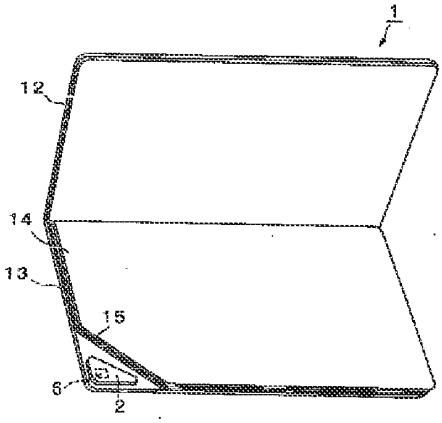
【図４】



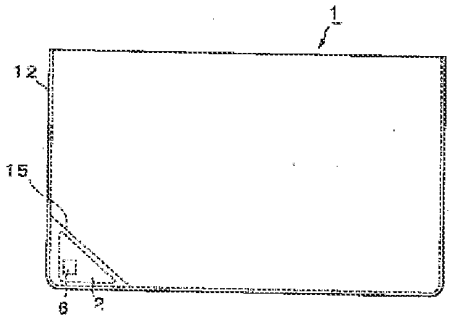
【図5】



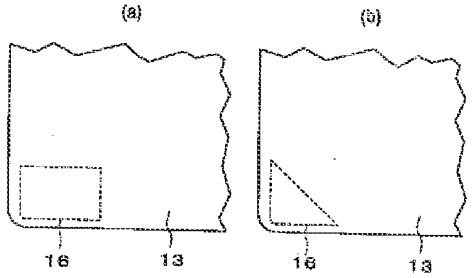
【図6】



【図7】



【図8】



フロントページの続き

(51)Int.Cl.7	識別記号	FI		(参考)
G06K 19/077		G06K 19/00	H	
19/00			K	
G07D 9/00	436		Q	

Espacenet

Bibliographic data: DE19608757 (A1) — 1997-09-11

Verfahren und Vorrichtung zur Echtheitskontrolle von Dokumenten in Form von Chipkarten

Inventor(s):

Applicant(s): BROSOW JOERGEN [AT] ± (BROSOW, JOERGEN, HOF, AT)

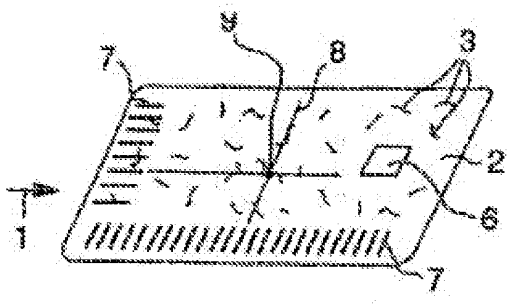
Classification: **- international:** ***G06K19/10;*** (IPC1-7): G07D7/00; G07F7/12
- cooperative: **G06K19/086**; **G06K19/10**

Application number: DE1996108757 19960306

Priority number(s): DE1996108757 19960306 ; DE1996108233 19960304

Abstract of DE19608757 (A1)

The proposed method is used for checking the authenticity of documents in the form of chip cards or smart cards fulfilling one or more functions, e.g. as bank, cash and credit cards used for withdrawing money and debiting amounts, and/or as ID documents for persons, motor vehicles (registration document, tachograph), as ke ys, etc. An inexpensive but reliable authenticity check is achieved as follows: the document comprising a base material with embedded foreign bodies whose physical properties differ from those of the base material and are distributed randomly within it is scanned for foreign bodies by a detector when first issued, in at least one scanning track selected by a random generator. The detector output values are then recorded in a first register present in the chip and locked following initialisation; the stored contents of that register cannot be read, manipulated or compared to other values from outside. When the document thus prepared is used, its foreign body data are read by at least one detector in the terminal unit which receives the document, stored in a second register in the chip which is separate from the first register, compared internally with the foreign body pattern in the first register and evaluated so as to release the document if the output values and foreign body density match.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 08 757 A 1**

(51) Int. Cl.[6]:
G 07 D 7/00
G 07 F 7/12

(21) Aktenzeichen: 196 08 757.0
(22) Anmeldetag: 6. 3. 96
(43) Offenlegungstag: 11. 9. 97

DE 196 08 757 A 1

(66) Innere Priorität:
196 08 233.1 04.03.96

(71) Anmelder:
Brosow, Jörgen, Hof, AT

(74) Vertreter:
LEINWEBER & ZIMMERMANN, 80331 München

(72) Erfinder:
Antrag auf Nichtnennung

(54) Verfahren und Vorrichtung zur Echtheitskontrolle von Dokumenten in Form von Chipkarten

(57) Das Verfahren dient der Echtheitskontrolle von Dokumenten in Form von Chipkarten oder Smartcards, die eine oder mehrere Funktionen ermöglichen, z. B. als Bank-, Cash- und Kreditkarten zur Ausgabe von Geld, zum Abbuchen von Werteinheiten dienen und/oder als ID-Dokument für Personen, Kraftfahrzeuge (Zulassungsdokument, Fahrtenschreiber), Schlüssel o. dgl. einsetzbar sind. Eine preisgünstige und dennoch sichere Echtheitsprüfung wird dadurch erreicht, daß das aus einer Grundmasse mit eingelagerten Fremdkörpern, deren physikalische Eigenschaften von denen der Grundmasse abweichen und in der Grundmasse eine Zufallsverteilung haben, bestehende Dokument zunächst bei der Erstausstellung in mindestens einer von einem Zufallsgenerator ausgewählten Abtastspur von mindestens einem Detektor auf Fremdkörper abgetastet wird. Danach werden die Ausgangswerte des Detektors in ein im Chip der Chipkarte vorgesehenes, nach Initialisierung gesperrtes erstes Register eingeschrieben, dessen gespeicherter Inhalt von außen her weder lesbar noch mit anderen Werten vergleichbar ist. Bei Anwendung des so vorbereiteten Dokuments werden schließlich dessen Fremdkörperinformationen von mindestens einem Detektor des das Dokument aufnehmenden Terminals gelesen und in einem parallel zum ersten Register im Chip vorhandenen zweiten Register gespeichert und mit dem Fremdkörpermuster im ersten Register intern verglichen und im Sinne einer Freigabe des Dokuments bei Übereinstimmung der Ausgangswerte ausgewertet.

DE 196 08 757 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 07. 97 702 037/274 5/23

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Echtheitskontrolle von Dokumenten in Form von Chipkarten oder Smartcards, die eine oder mehrere Funktionen ermöglichen, z. B. als Bank-, Cash- und Kreditkarten zur Ausgabe von Geld, zum Abbuchen von Werteinheiten dienen und/oder als ID-Dokument für Personen, Kraftfahrzeuge (Zulassungsdokument, Fahrtenschreiber), Schlüssel od. dgl. einsetzbar sind. Wertvolle Dokumente wurden bisher schon gegen Fälschung und Mißbrauch gesichert. Das geschah durch die Verwendung besonderer Papierqualitäten mit Wasserzeichen, durch Einbetten von Metallstreifen und die Verwendung eines möglichst fälschungssicheren Drucks. Die Echtheitsprüfung von Dokumenten ist unter diesen Gesichtspunkten schwierig. Sie erfordert insbesondere bei Automaten einen beträchtlichen Aufwand oder eine Verminderung der durch die Echtheitsprüfung erzielbaren Fälschungssicherheit.

Der am nächsten kommende Stand der Technik auf dem Gebiet der Sicherung von Dokumenten gegen Kopieren und Fälschung ergibt sich aus folgenden Referenzen: CH-PS 569144 "Blattförmiges Material für Dokumente", CH-PS 577722 "Gerät zur Echtheitskontrolle von Dokumenten", DE-PS 26 35 795 "Verfahren und Vorrichtung zur Echtheitskontrolle von Dokumenten", US-PS-4,218,674 "Method and System for Verifying Authenticity Safe against Forgery". Das eingangs genannte Problem der Echtheitskontrolle von Dokumenten ist auch durch diese vorbekannten Vorschläge nicht zur vollsten Zufriedenheit gelöst worden, insbesondere dann nicht, wenn es sich um den Einsatz von Smartcards, d. h. Automatenkarten, die mit einem Chip (elektronische Einheit zum Steuern, Lesen und Schreiben von Informationen) ausgerüstet sind, handelt. Für den Verkehr von Kunden mit Geldautomaten, Automaten anderer Art oder von Anwendungen in Netzwerken wie z. B. Internet wäre deshalb ein Prüfverfahren und eine dazu dienende Vorrichtung wünschenswert, das eine wirklich zuverlässige, fälschungssichere Echtheitsprüfung ermöglicht.

Das erfindungsgemäße Verfahren, nach dem eine besonders preisgünstige und dennoch sichere Echtheitsprüfung ermöglicht wird, ist im wesentlichen dadurch gekennzeichnet, daß das aus einer Grundmasse mit eingelagerten Fremdkörpern, deren physikalische Eigenschaften von denen der Grundmasse abweichen und in der Grundmasse eine Zufallsverteilung haben, bestehende Dokument bei der Erstausstellung in mindestens einer von einem Zufallsgenerator ausgewählten Abtastspur von mindestens einem Detektor auf Fremdkörper abgetastet wird, daß die Ausgangswerte des Detektors in ein im Chip der Chipkarte vorgesehenes, nach Initialisierung gesperrtes erstes Register eingeschrieben werden, dessen gespeicherter Inhalt von außen her weder lesbar noch mit anderen Werten vergleichbar ist, und daß bei Anwendung des so vorbereiteten Dokuments dessen Fremdkörperinformationen von mindestens einem Detektor des das Dokument aufnehmenden Terminals gelesen und in einem parallel zum ersten Register im Chip vorhandenen zweiten Register gespeichert und mit dem Fremdkörpermuster im ersten Register intern verglichen und im Sinne einer Freigabe des Dokuments bei Übereinstimmung der Ausgangswerte ausgewertet werden. Die Erfindung beruht somit auf der Erkenntnis, daß nunmehr eine Echtheitsprüfung mit dem Kartenleser mit einfachen Mitteln ermöglicht ist, ohne daß die

Sicherheitsinformation (d. h. die die Echtheitserkennung der Chipkarte gewährleistenden Daten) jemals den Chip der Karte verläßt.

Bei dieser Technik ist ein Trägermaterial für Chipkarten Voraussetzung, das zur Erhöhung der Fälschungs- und Kopiersicherheit mit optisch und/oder elektronisch erkennbaren Fremdkörpern zufallsmäßig versetzt ist. Durch einfache Erkennung der Position und der Eigenschaften des Fremdkörpers, sowie durch Vergleich dieser Information in einem Speicher des Chips kann die Chipkarte auf ihre Echtheit überprüft werden.

Die Koordinaten (X-Y [Position], Z [physikalische Eigenschaften]) dieser Fremdkörper werden bei der Ausstellung der Chipkarte mit Hilfe eines Zufallsgenerators erfaßt (die ganze Fläche oder ein ausgewählter Teil der Fläche X-Y) und im Kartenchip als nicht auslesbare Information gespeichert. Beim Lesen der Chipkarte in einem Chipkartenterminal werden alle Fremdkörper koordinatenmäßig gelesen und mit den im Koordinatenspeicher der Chipkarte enthaltenen Werten verglichen. Stimmen die im Kartenchip gespeicherten Daten mit den für die Koordinaten (X-Y-Z) der Fremdkörper ermittelten Daten überein, wird die Chipkarte als gültig anerkannt und der Chip für Transaktionen freigegeben. Stimmen die im Kartenchip gespeicherten Daten über die Koordinaten (X-Y-Z) der Fremdkörper nicht überein, wird die Chipkarte als ungültig erkannt und abgewiesen oder einbehalten.

Die Fremdkörper können in Abhängigkeit von ihren unterschiedlichen physikalischen Eigenschaften mit unterschiedlichen Erkennungsmethoden geortet und gelesen werden. Zu diesen Methoden zählen Laser, Infrarot-erkennung (z. B. Energieabstrahlung), magnetische Eigenschaften (hierzu wird auf die eingangs zum Stand der Technik zitierten Patentschriften verwiesen), Ultraschall (z. B. Echo-Erkennung) usw. Die verschiedenen Erkennungsmethoden können auch gleichzeitig eingesetzt werden und machen somit ein Kopieren oder Fälschen praktisch undenkbar, da jeder Fremdkörper mehrere Eigenschaften besitzt und diese Eigenschaften in der Position (Koordinate) auf der Chipkarte im Chip gespeichert sind.

Im übrigen ist es auch möglich, den Chipkartenvortrieb mit einem Schrittmotor vorzunehmen, der durch einen Taktfrequenzteiler im Chip der Chipkarte gesteuert wird, um schnell und sicher das gewünschte Koordinatenfeld (X, Y) zur erreichen.

Weitere Einzelheiten ergeben sich aus der folgenden Beschreibung anhand der beigefügten Zeichnung; es zeigen:

Fig. 1 eine sehr schematische perspektivische Ansicht einer Chipkarte mit zugeordnetem Detektor und

Fig. 2 eine analoge Ansicht der Chipkarte zur Veranschaulichung der Bedeutung der Koordinaten.

Wie ersichtlich, ist sowohl bei Ausstellung als auch beim Einsatz die in Richtung der Kartenlängsachse verlaufende Leserichtung 1 der Chipkarte 2 zu berücksichtigen. Dabei werden die Fremdkörper 3 mit Hilfe eines Fremdkörperdetektors 4 koordinatenmäßig erfaßt, und die Meßwerte werden vom Detektor 4 über ein Anschlußkabel 5 weitergeleitet. Der genaue Ort der Fremdkörper 3 wird festgestellt und im Kartenchip 6 gespeichert. In Fig. 2 ist schematisch die Taktspur 7 herausgestellt, die auf die vorstehend geschilderte Weise für die Verarbeitung der Fremdkörperinformation anhand der zur Abtastspur 8 gehörenden Koordinaten 9 eines Fremdkörpers sorgt.

Patentansprüche

1. Verfahren zur Echtheitskontrolle von Dokumenten in Form von Chipkarten oder Smartcards, die eine oder mehrere Funktionen ermöglichen, z. B. als Bank-, Cash- und Kreditkarten zur Ausgabe von Geld, zum Abbuchen von Werteinheiten dienen und/oder als ID-Dokument für Personen, Kraftfahrzeuge (Zulassungsdokument, Fahrtenschreiber), Schlüssel od. dgl. einsetzbar sind, **dadurch gekennzeichnet**, daß das aus einer Grundmasse mit eingelagerten Fremdkörpern, deren physikalische Eigenschaften von denen der Grundmasse abweichen und in der Grundmasse eine Zufallsverteilung haben, bestehende Dokument bei der Erstausstellung in mindestens einer von einem Zufallsgenerator ausgewählten Abtastspur von mindestens einem Detektor auf Fremdkörper abgetastet wird, daß die Ausgangswerte des Detektors in ein im Chip der Chipkarte vorgesehenes, nach Initialisierung gesperrtes erstes Register eingeschrieben werden, dessen gespeicherter Inhalt von außen her weder lesbar noch mit anderen Werten vergleichbar ist, und daß bei Anwendung des so vorbereiteten Dokuments dessen Fremdkörperinformationen von mindestens einem Detektor des das Dokument aufnehmenden Terminals gelesen und in einem parallel zum ersten Register im Chip vorhandenen zweiten Register gespeichert und mit dem Fremdkörpermuster im ersten Register intern verglichen und im Sinne einer Freigabe des Dokuments bei Übereinstimmung der Ausgangswerte ausgewertet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die bei der Erstausstellung längs der ausgewählten Abtastspur von dem mindestens einen Detektor festgestellten Ausgangswerte Taktimpulsen zugeordnet werden und daß das durch Zusammenfallen von Ausgangswerten des oder der Detektoren mit den Taktimpulsen erzeugte Fremdkörpermuster in das erste Register für die weitere Auswertung einschreibbar ist.

3. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Abtastspur auf dem Dokument ein Koordinatensystem zur Festlegung von Abtastpunkten längs der durch das erste Register im Chip der Chipkarte vorbestimmten Abtastspur überlagert ist.

4. Vorrichtung nach Anspruch 3, dadurch gekennzeichnet, daß die Abszisse des Koordinatensystems durch eine den Taktgeber bildende Taktspur gebildet ist.

5. Vorrichtung nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß die Taktspur aus Marken besteht, die sich in ihren physikalischen Eigenschaften von denen der Grundmasse des Dokumentes und ihrer Fremdkörper unterscheidet.

6. Vorrichtung nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, daß die horizontale Taktspur mit dem ersten Fremdkörper auf der Chipkarte beginnt.

7. Vorrichtung nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, daß der Chip auf der Chipkarte eine verschlüsselte Angabe zur Zufallsverteilung der Fremdkörper aufweist.

8. Vorrichtung nach einem der Ansprüche 3 bis 6 sowie 7, dadurch gekennzeichnet, daß für das schnelle Erreichen der gewünschten Koordinaten ein Chipkartenvortrieb für Chipkartenterminale mit einem durch einen Taktfrequenzteiler im Chip der Chipkarte gesteuerten Schrittmotor versehen ist, der durch die verschlüsselte Angabe zur Zufallsverteilung gesteuert wird.

9. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß das Terminal mit mindestens einem Fremdkörperdetektor ausgerüstet ist, durch den die Fremdkörpereigenschaften erkennbar und auswertbar sind.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 08 757 A1
Int. Cl.[6]: G 07 D 7/00
Offenlegungstag: 11. September 1997

Fig. 1

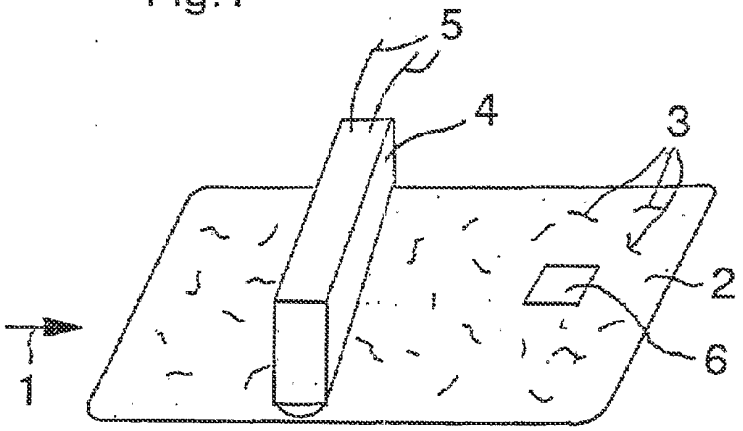
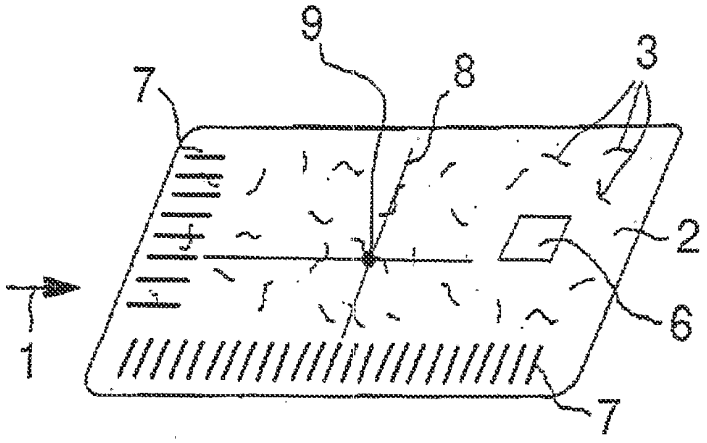


Fig. 2



702 037/274

Espacenet

Bibliographic data: DE10042805 (A1) — 2002-03-14

Electronic anti-theft protection for vehicle e.g. boat, has transponder attached to vehicle provided with identification data memory and transceiver cooperating with external data reader

Inventor(s): LANGENSTUECK HOLGER [DE] ± (LANGENSTUECK, HOLGER)

Applicant(s): BUNDESDRUCKEREI GMBH [DE] ± (BUNDESDRUCKEREI GMBH)

Classification: **- international:** ***B60R25/00; B60R25/102; B63J99/00; B64D45/00; G08B13/24;*** (IPC1-7): B60R25/00; B63B45/00; B64D45/00; G08B13/00

- cooperative: **B60R25/00**; **B60R25/102**; **B63J99/00**; **B64D45/0015**; **G06K19/0776**; **G08B13/2417**; **G08B13/2445**; **G08B13/2462**; **G08B13/2482**; **G08B13/2485**; B60R2325/105; B60R2325/304; B63B2017/0009

Application number: DE2000142805 20000830

Priority number(s): DE2000142805 20000830

Abstract of DE10042805 (A1)

The electronic anti-theft protection has a transponder (1) attached to the vehicle, provided with a data memory (2) holding identification data and a passive and/or active transceiver (3), cooperating with an external data reader, for transmission of electrical operating energy and data. The transponder is attached to the vehicle so that it is destroyed by attempted removal. An independent claim for an automatic data transmission method for vehicle electronic anti-theft protection is also included.The electronic anti-theft protection has a transponder (1) attached to the vehicle, provided with a data memory (2) holding identification data and a passive and/or active transceiver (3), cooperating with an external data reader, for transmission of electrical operating energy and data. The transponder is attached to the vehicle so that it is destroyed by attempted removal. An independent claim for an automatic data transmission method for vehicle electronic anti-theft protection is also included.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 42 805 A 1**

(51) Int. Cl.[7]:
G 08 B 13/00
B 60 R 25/00
B 63 B 45/00
B 64 D 45/00

(21) Aktenzeichen: 100 42 805.3
(22) Anmeldetag: 30. 8. 2000
(43) Offenlegungstag: 14. 3. 2002

DE 100 42 805 A 1

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(74) Vertreter:
Riebling, P., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 88131 Lindau

(72) Erfinder:
Langenstück, Holger, 61239 Ober-Mörlen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	198 09 574 A1
DE	198 09 574 A1
US	61 04 290
EP	04 26 332 A2
WO	99 65 002 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Elektronische Diebstahlsicherung für mobile Objekte, insbesondere für Wasser-,Land- und Luft-Fahrzeuge und damit verbundenes Verfahren zur Datenübermittlung

(57) Die Erfindung betrifft eine elektronische Diebstahlsicherung für mobile Objekte, insbesondere für Wasser-, Land- und Luft-Fahrzeuge, und im Speziellen für Boote für den Freizeitbereich, wobei die erfindungsgemäße elektronische Diebstahlsicherung mindestens einen mit dem Objekt verbundenen Transponder und mindestens ein externes Lesegerät beinhaltet, wobei der Transponder mindestens einen mit gespeicherten relevanten Daten versehenen Datenspeicher und mindestens eine passive und/oder aktive Sende-/Empfangseinrichtung für die drahtlose Energie- und/oder Datenübertragung mit dem mindestens einen Lesegerät beinhaltet. Es wird auch ein Verfahren zur automatischen Übertragung der relevanten Daten und GPS-Daten an Interessenten, wie z. B. die Polizei vorgeschlagen. Durch das elektronische Diebstahlsicherungs-System wird ein einfaches, sicheres und schnelles Auffinden und Identifizieren der mobilen Objekte auch aus der Entfernung wiederholt und während der gesamten Lebensdauer der Objekte ermöglicht und eine rasche Informationsübermittlung sowie Sicherung des gestohlenen Objektes ermöglicht.

DE 100 42 805 A 1

Beschreibung

[0001] Die Erfindung betrifft eine elektronische Diebstahlsicherung für mobile Objekte, insbesondere für Wasser-, Land- und Luft-Fahrzeuge, und im Speziellen für Boote für den Freizeitbereich, und damit verbundenes Verfahren zur Datenübermittlung nach dem Oberbegriff des unabhängigen Anspruches.

[0002] Im folgenden wird aus Vereinfachungsgründen anstatt allgemein auf mobile Objekte nur noch Bezug auf den bevorzugten Anwendungsfall der Erfindung bei Booten genommen. Hierbei sollen also die Boote nur stellvertretend sein für alle erdenklichen beweglichen Objekte, wie Kraftfahrzeuge, Sportflugzeuge, Fahrräder, Inline-Skates und sonstige Sportgeräte, Stückgut wie Gepäckstücke, sowie Fertigungsteile in Fertigungs- und Lagerhallen, Wert- und Sicherheitsdokumente, allgemeine Wertgegenstände und Ähnliches.

[0003] Jährlich werden eine Vielzahl von trailerbaren, d. h. einfach bewegbaren Motor- und Segelbooten, sowie Aussenborder und diverse höherwertigere Ersatzteile für diese Boote gestohlen.

[0004] Die Suche der Wasserschutzpolizei nach gestohlenen Booten gestaltet sich problematisch. Bei Routinekontrollen darf die Wasserschutzpolizei nur bei konkretem Tatverdacht ein Boot betreten. Da es sich bei den meisten Booten um Serienprodukte handelt, die keine wesentlichen Unterscheidungsmerkmale enthalten, erweist sich die Identifikation der Boote und die Zuordnung zum ursprünglichen Besitzer als extrem schwierig bzw. als nahezu unmöglich.

[0005] Individuell gestaltete Boote können relativ leicht verändert, und die herkömmlichen Bootskennungen nach dem Stand der Technik relativ leicht entfernt werden.

[0006] Die am Markt angebotenen elektrisch betriebenen Alarmanlagen für Boote sind häufig zu teuer und der Einsatz meist nur bei kostenintensiveren Booten mit Kajüte oder abschliessbaren Behältnissen sinnvoll, da ansonsten die Alarmanlagen leicht entschärft werden können und den Witterungsverhältnissen nahezu schutzlos ausgesetzt sind. Als Alternative zu den elektrischen Alarmanlagen stehen mechanische Sicherungen gegen Diebstahl zur Verfügung, die jedoch nur begrenzten Schutz ermöglichen und das Auffinden eines einmal gestohlenen Bootes nicht erleichtern.

[0007] Aufgabe der vorliegenden Erfindung ist es daher eine elektronische Diebstahlsicherung für mobile Objekte, insbesondere für Wasser-, Land- und Luft-Fahrzeuge, und im Speziellen für Boote für den Freizeitbereich bereit zu stellen, welche elektronische Diebstahlsicherung ein einfaches, sicheres und schnelles Auffinden und Identifizieren der mobilen Objekte auch aus der Entfernung wiederholt und möglichst während der gesamten Lebensdauer der Objekte ermöglicht.

[0008] Gefordert wird insbesondere eine Lösung für kleinere Bootsklassen und für Aussenborder, die präventiv Diebstahl verhindert und ex-post das Auffinden und Identifizieren von gestohlenen Booten erleichtert.

[0009] Zur Lösung der gestellten Aufgaben dient die technische Lehre des unabhängigen Anspruches.

[0010] Wesentliches Merkmal hierbei ist, dass die erfindungsgemässe elektronische Diebstahlsicherung mindestens einen mit dem Objekt verbundenen Transponder und mindestens ein externes Lesegerät beinhaltet, wobei der Transponder mindestens einen mit gespeicherten relevanten Daten versehenen Datenspeicher und mindestens eine passive und/oder aktive Sende-/Empfangseinrichtung für die drahtlose Energie- und/oder Datenübertragung mit dem mindestens einen Lesegerät beinhaltet.

1) Transponder

[0011] Jeder Transponder besteht also aus mindestens einem Datenspeicher, als flüchtiger (RAM) oder nichtflüchtiger (ROM, EPROM, EEPROM) Speicher und mindestens einer Antenne als passive und/oder aktive Sende-/Empfangseinrichtung.

[0012] Bevorzugt wird, wenn der Transponder derart am Boot befestigt ist, dass er beim Versuch des Entfernens zerstört wird. Dies wird insbesondere dadurch erreicht, dass zur eindeutigen Kennzeichnung des Bootes am Bootsrumpf der Transponder einlaminiert oder entsprechend mit einer Schutzschicht überklebt wird. Die Einlaminierung/Überklebung geschieht wiederum bevorzugt derart, dass der Transponder nicht sichtbar ist und somit eine Manipulation erschwert wird.

[0013] Folgende Hauptvorteile besitzt dieser erfindungsgemässe Transponder für eine Diebstahlsicherung für mobile Objekte, insbesondere zur Bootssicherung:

- Nahezu unsichtbare und nicht ablösbare Markierung in Form des Transponders/Datenspeichers;
- eindeutige Kennzeichnung des Bootes;
- Manipulationssicherer Datenspeicher;
- Über Entfernung drahtlos auslesbar (Sicherheit für Prüfpersonen);
- Lange Lebensdauer;
- Unempfindlich gegen Schmutz, Wasser, UV-Strahlen und Witterung;

[0014] Weitere Vorteile von Transpondern sind:

- Bequemes Handling
  Lesen und Beschreiben der Transponder über Entfernung
- Lagenunabhängige Kommunikation mit dem Transponder, d. h. der Transponder muss beim Lesen oder Schreiben nicht mehr in eine bestimmte Richtung ausgerichtet werden
- Antikollisionsschutz, d. h. es können bis zu 40 Transponder pro Sekunde parallel gelesen werden
  Flexibler und sicherer Datenspeicher
- Variabler Datenspeicher, d. h. der Transponder kann beliebig oft beschrieben und gelesen werden
- Offline Speicherung von Daten
- Manipulationssichere, eindeutige Seriennummer
- Durch die geringe Höhe und das flexible Trägermaterial kann ein Transponder ideal in Produkte integriert werden
- Unempfindlich gegenüber Schmutz, Staub, Wasser, UV-Strahlen und Witterung

[0015] Der Boots-Transponder ist also ein Mikro-Chip, auf dem beispielsweise alle wichtigen Bootsdaten wie Werft, Baujahr, Typ und Rumpfnummer plus einer Identifikationsnummer (ID-Nummer) gespeichert sind. Ein solcher Transponder kann in Minutenschnelle nachträglich am Boot, am Motor oder Zubehör montiert werden. Er benötigt als passives Element weder Batterien noch irgendeine Pflege. Wird das Boot als gestohlen gemeldet und kontrolliert, kann z. B. die Polizei diese Daten von aussen per Lesegerät abrufen und den rechtmässigen Eigner ermitteln.

[0016] Die bevorzugt zum Einsatz kommenden passiven Transponder (d. h. sie benötigen keine zusätzliche Batterie) arbeiten mit einer Übertragungsfrequenz von 13,56 MHz. Je nach Lesegerät und Grösse der Transponderantenne kann eine Schreib-/Leseentfernung von bis zu 1, 20 m erreicht werden. Der Transponder verfügt über eine nutzbare Spei-

cherkapazität von 384 Bit und einer 64 Bit langen, einmaligen und unveränderbaren Seriennummer, die direkt vom Chiphersteller vergeben wird. Es wird eine dauerhafte Temperaturfestigkeit bis 70°C und kurzfristige Temperaturfestigkeit bis 180°C gewährleistet. Transponder sind Schmutz, Wasser, Witterungs- und UV-Strahlen unempfindlich und können daher auch bei extremen Umweltbedingungen eingesetzt werden.

1a) Befestigungsort Transponder

[0017] Die Transponder werden insbesondere in einer Vielzahl von z. B. 3, 5 oder 7 Stück in einem bevorzugt definierten Bereich von ca. 30 cm Höhe oberhalb der Wasserlinie möglichst gleichmässig verteilt an den Bootsseiten, sowie am Bootsspiegel (Heck) angebracht. Die Anzahl der Transponder richtet sich nach der Bootslänge, wobei durch das Vorsehen mehrerer Transponder dann liegt ein redundantes Markierungssystem am Boot vorliegt, wodurch zum einen eine Manipulation erschwert wird und zum anderen bei der Überprüfung durch eine Prüfperson nur ein begrenzter Teil des Bootes untersucht werden muss. Dies bringt eine rasche und zuverlässige Prüfung mit sich.

Bootslänge:

- < 6 m: 3 Transponder (je einen an jeder Seite und einen am Heck)
- 6–8 m: 5 Transponder (je zwei an jeder Seite und einen am Heck)
- 8–10 m: 7 Transponder (je drei an jeder Seite und einen am Heck)
- > 10 m: 9 Transponder (je vier an jeder Seite und einen am Heck)

[0018] Aufgrund der kleinen Abmessungen und dem geringen Kosten sind derartige Transponder-Diebstahlsicherungen für alle Neu- und Gebrauchtboote insbesondere vom 3-m-Schlauchboot bis zur 15-m-Motoryacht geeignet.

1b) Datenspeicher des Transponders

[0019] Die erfindungsgemässen Transponder (auch RFID = Radio Frequency Identification genannt) beinhaltet einen elektronischen, bevorzugt wiederbeschreibbaren Datenträger – einem Computerspeicherchip zur Speicherung von Daten.

[0020] In den Datenspeichern des Transponders sind bevorzugt eine eindeutige, einzigartige Seriennummer, eine Referenznummer, sowie Identifizierungsdaten über das Boot gespeichert.

[0021] Auch Bootseigner, Bootstyp, Baujahr, Name des Bootes, Erstwasserung, Rumpfnummer, Motornummer und wenn vorhanden die Zulassungsnummer, werden unter den festen, unveränderbaren Nummern der Transponder (Seriennummer und Referenznummer) in die Datei aufgenommen und auch in einen nachfolgend beschriebenes Dokument, einen sogenannten "Transponderpass" eingetragen.

[0022] Auch können Informationen über den Eigentümer, den Hersteller, die Versicherung oder ähnliches in dem Datenspeicher gespeichert sein.

1c) Sende-/Empfangseinrichtung des Transponders

[0023] Die erfindungsgemässen Transponder (auch RFID = Radio Frequency Identification genannt) beinhaltet eine integrierte Antenne zur Daten- und/oder Energieübertragung.

[0024] Die Energieversorgung des Datenträgers, sowie der Datenaustausch erfolgen über elektromagnetische Felder, vergleichbar der Funk- und Radartechnik. Dies bedeutet, dass der Datenaustausch kontaktlos über eine bestimmte Distanz erfolgt.

2) Lesegerät

[0025] Zum Auslesen der Bootstransponder an Land oder vom Bootssteg aus werden mobile, zumeist mit Batterien/Akkus betriebene Handleseterminals eingesetzt. Das Handheld Terminal "Psion Workabout" wird hierzu um RFID Reader/Writer Module erweitert. Über die serielle Schnittstelle kann in das Handlesegerät die Black List der gestohlenen Boote geladen werden.
Grösse: 65 × 89 × 55 mm
Power Supply: 5 VDC
Frequenz: 13,56 MHz
Schnittstelle: Serielle, asynchrone 9600 Baud, TTL
Operationsentfernung: 0–ca. 10 cm

[0026] Zum Orten und Identifizieren der Transponder von einem Inspektionsboot wird auch ein stationäres Lesegerät eingesetzt. Das Lesegerät muss für diese Anwendung und deren Bedingungen speziell entwickelt werden.
Grösse: Leseantenne integriert in eine witterungsfeste Handkelle inkl. LED-Anzeige angeschlossen mit einem Spiralkabel an einen Longrange-Reader und einen PC/Notebook
Power Supply: 220 V
Frequenz: 13,56 MHz
Schnittstelle: RS **232** und RS **485**
Operationsentfernung: 0– ca. 60 cm

3) Transponderpass

[0027] Das vorgeschlagene Diebstahl-Sicherungssystem beinhaltet zusätzlich zum eigentlichen Transponder am Boot und dem zugehörigen mobilen/stationären Lesegerät unter anderem noch einen sogenannten Transponderpass als Wert- und Sicherheitsdokument.

[0028] Der Bootseigner kann einen Transponderpass beispielsweise bei seiner Bootsversicherung oder bei einer ähnlichen zentralen Stelle anfordern.

[0029] Bootseigner, Bootstyp, Baujahr, Name des Bootes, Erstwasserung, Rumpfnummer, Motornummer und wenn vorhanden die Zulassungsnummer, werden unter den festen, unveränderbaren Nummern der Transponder (Seriennummer und Referenznummer) in die Datei aufgenommen und im Transponderpass eingetragen.

[0030] Dieser Transponderpass dient wie ein Kraftfahrzeugschein als Beweis des Eigentümers und als Informationsquelle im Falle eines Diebstahls des Bootes.

4) Registrierung und Markierung von Booten

[0031] Die Registrierung und Markierung von Booten geschieht etwa folgendermassen:
Ein mit sicherheitsdrucktechnischen Verfahren erstellter Transponderpass wird von einer zentralen Sicherheitsstelle (z. B. Datenbankbetreiber und/oder Versicherungen) nummeriert und registriert. In den Transponderpass werden die personalisierten Transponder eingeklebt, sowie die relevanten Bootsdaten eingedruckt und an den Bootshersteller oder den Bootseigner versendet. Nach Erhalt werden die Transponder in den Bootsrumpf einlaminiert. Bei fabrikneuen Booten werden die Transponder direkt vom Hersteller oder vom Importeur, bei gebrauchten Booten vom Bootseigner selbst angebracht.

[0032] Im Normalfall ist jedoch der Versicherer nicht der Datenbankbetreiber und somit gibt die Versicherung also mit Zustimmung des Eigners die Daten des Eigners und des Bootes (Baujahr, Grösse, Bootstyp etc.) elektronisch an die zentrale Sicherheitsstelle weiter. Diese Sicherheitsstelle registriert die Daten in einer zentralen Datenbank, speichert die relevanten Daten in den Transpondern und erstellt den personalisierten Transponderpass. Transponder, Transponderpass und Einbauanleitung werden an den Bootseigner gesendet, der die Transponder gemäss Anleitung an seinem Boot anbringt.

[0033] Der Transponderpass soll dann nicht auf dem Boot aufbewahrt werden. Zusätzlich kann der Bootseigner an seinem Boot einen Aufkleber sichtbar anbringen, der anzeigt, dass das Boot durch Transponder gesichert ist.

[0034] Einen Transponder sollte der Eigentümer an einer nur ihm bekannten Stelle verstecken, dessen Plazierung nur er weiss und von ihm im Transponderpass beschrieben wird. Dieses ermöglicht eine letzte endgültige Feststellung des Eigentümers auch dann, wenn von den Dieben, die in der Bordwand befindlichen Transponder ausgeschnitten wurden. Dieses ist aber fast unmöglich, da hier ein komplettes Aufschneiden der Bordwand erforderlich würde.

[0035] Vergleichbar zur Entwicklung der Wegfahrsperre bei Autos soll die Transponderabsicherung zur Verringerung des Versicherungsbeitrages führen und/oder Grundvoraussetzung für eine Bootsversicherung werden. Auch Bootseigner, die keine Bootsversicherung abschliessen wollen, können den Transponderpass natürlich erwerben.

5) Diebstahlmeldung

[0036] Den Diebstahl seines Bootes meldet der Bootseigner möglichst kurzfristig bei der zentralen Stelle, welche die entsprechenden Transponderdaten aus der zentralen Datenbank selektiert und eine "Black List" erzeugt. Diese Black List wird online an die Datenbank der Wasserschutzpolizei gesendet (täglich oder mehrmals täglich). Die Daten in den mobilen Handlesegeräten werden beim Laden der Batterie up-gedatet.

[0037] Bei Routinekontrollen oder bei Kontrollen bei Verdacht überprüft die Wasserschutzpolizei die Existenz einer Transponderabsicherung, in dem sie das stationäre Lesegerät an der Bootsaussenwand vorbeifährt. Die LED zeigt die Existenz eines Transponders an. Die Daten werden automatisch ausgelesen und mit der Black List verglichen. So kann die Wasserschutzpolizei sofort feststellen, ob das Boot gestohlen wurde und den rechtmässigen Eigentümer etc. identifizieren.

[0038] Prüfpersonen beispielsweise der Wasserschutzpolizei können mit speziellen Lesegeräten die an den Booten angebrachten Transponder also orten und den Dateninhalt über eine Entfernung von z. B. ca. 60 cm auslesen. Die ausgelesenen Daten werden mit der Black List der gestohlenen Boote verglichen, so dass gestohlene Boote von der Wasserschutzpolizei sofort erkannt und identifiziert werden können.

[0039] Ohne das vermeintliche Diebesgut betreten zu müssen, kann von aussen mit einem Lesegerät durch die Bordwand der bevorzugt von innen eingeklebte Transponder gelesen werden. Die im Lesegerät erscheinende Nummer gibt sofort Aufschluss ob das Boot als gestohlen gemeldet wurde. Ausserdem ist es möglich, die Übereinstimmung der in der Zentrale gespeicherten persönlichen Daten des Eigentümers mit denen in den Bootspapieren zu überprüfen.

[0040] Bootspapiere können jederzeit gefälscht werden, die eingeklebten Transponder und deren Daten aber nur sehr schwer. Ein durch Transponder gesichertes Boot ist immer, auch nach Jahren zu identifizieren.

[0041] Im folgenden wird die Erfindung anhand von lediglich einen Ausführungsweg darstellenden Zeichnungen näher erläutert. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere erfindungswesentliche Merkmale und Vorteile der Erfindung hervor.

[0042] **Fig.** 1 zeigt einen erfindungsgemässen Transponder;

[0043] **Fig.** 2 zeigt einen schematischen Überblick über die Möglichkeiten der Übermittlung von relevanten Daten zur Diebstahlsicherung;

[0044] **Fig.** 3 zeigt einen schematischen Flussplan der Übermittlung von relevanten Daten zur Diebstahlsicherung.

[0045] In **Fig.** 1 ist ein erfindungsgemässer Transponder **1** dargestellt, welcher auf einer Trägerfolie **4** aufgebracht ist und im Wesentlichen aus einem Datenträger **2** in Form eines Mikrochips und einer Sende-, Empfangsantenne **3** besteht. Die Sende-, Empfangsantenne **3** ist spiralförmig auf dem quadratischen Träger **4** von aussen nach innen gewunden und besitzt etwa 10 volle Spiralen in Form von Leiterbahnen insbesondere aus Kupfer. Diese Sende-, Empfangsantenne **3** kann durch die üblichen Ätzmethoden der Platinenherstellung gewonnen werden.

[0046] Die Verbindung zwischen Sende-, Empfangsantenne **3** und Mikrochip **2** wird durch Kontaktierungen **5** insbesondere aus Edelmetall wie Gold bewerkstelligt, welche Kontaktierungen ebenfalls als dünne Leiterbahnen vorliegen und über einen zusätzlichen Träger stabilisiert werden.

[0047] Die Kontaktierung **5** bewirkt in den Bereichen **6**a und **7**a eine elektrisch leitende Verbindung zwischen dem einen Ende der Antenne **3** und dem einen Ende des Mikrochips **2** und bewirkt in den Bereichen **6**b und **7**b eine elektrisch leitende Verbindung zwischen dem anderen Ende der Antenne **3** und dem anderen Ende des Mikrochips **2**.

[0048] Die Trägerfolie **4** ist an ihrer Oberseite, auf welcher Mikrochip **2**, Antenne **3** und Kontaktierungen **5** angebracht sind mit einer Klebstoffschicht versehen zur leichten Anbringung an dem Bootsrumpf. Die Dicke der Trägerfolie **4** beträgt nur etwa einen Millimeter oder weniger und kann daher ohne Probleme und ohne ersichtlich zu werden auf den Bootsrumpf laminiert werden.

[0049] **Fig.** 2 zeigt einen schematischen Überblick über die Möglichkeiten der Übermittlung von relevanten Daten zur Diebstahlsicherung. Hier ist der Transponder **1** auf einem Bootsrumpf **8** auflaminiert dargestellt und tauscht mit dem Lesegerät **9** relevante Daten aus. Das hier als Handgerät dargestellte Lesegerät **9** besitzt ein Navigationssystem (GPS), mit welchem es die Ortkoordinaten via Satellit (Sat) empfangen und weiterleiten kann.

[0050] Diese Daten in Form von ID-Daten des Transponders (und des Bootes) und in Form von Ortkoordinaten können dann verschiedenartigen Interessenten in unterschiedlicher vorselektierter Form übermittelt werden.

[0051] Derartige Interessenten sind in **Fig.** 2 als zentrale Datenbank (DB), Exekutive bzw. Zentrale der Wasserschutzpolizei (Bx), Versicherung (V), Presse (P), Internet (I) und Sonstige (S) wie der Eigentümer selbst, dargestellt.

[0052] Diese Interessenten können dann die Daten entsprechend ihren Vorgaben und Aufgaben verarbeiten und insbesondere die Datenbank und die Polizei senden dann Daten zurück an das Lesegerät **9** zurück. Die Datenbank sendet dann Informationen über gestohlen gemeldete Boote und die Polizei weitere Instruktionen für den Bediener des Lesegerätes **9** und evtl. Informationen über die vermuteten Personen auf dem Boot.

[0053] **Fig.** 3 zeigt einen schematischen Flussplan der Übermittlung von relevanten Daten zur Diebstahlsicherung. Hier wird ausgehend von dem Überprüfen des Bootes nach

einem Transponder eine Abfrage gestartet, ob überhaupt ein Transponder geortet wurde. Wenn nein, kann die Überprüfung beliebig oft wiederholt werden, wenn ja, dann werden die im Speicher befindlichen Daten des Transponders in das Prüfgerät (Lesegerät) geladen. Wenn diese Daten nicht vollständig oder falsch formatiert sind, dann wird die Prüfung wiederholt, ansonsten werden die Daten einer externen Datenbank übermittelt oder Informationen aus dieser in das Prüfgerät geholt.

[0054] Diese Daten aus der externen Datenbank dienen dann zur Ermittlung, ob das Boot als gestohlen gemeldet ist. Diese Abrage kann im Prüfgerät selbst oder in der externen Datenbank erfolgen.

[0055] Falls das Boot als gestohlen gemeldet ist werden die in der Beschreibung der **Fig.** 2 erwähnten Interessenten benachrichtigt. Diese Benachrichtigung kann wiederum vom Prüfgerät oder von der externen Datenbank bzw. dessen Betreiber erfolgen.

[0056] Die Interessenten können dann ihrerseits wiederum Informationen an den Betreiber des Prüfgerätes senden, welcher dann entsprechende Schritte unternimmt.

[0057] Durch die vorliegende Erfindung ist es erstmals möglich eine elektronische Diebstahlsicherung für Boote bereit zu stellen, welche Diebstahlsicherung ein einfaches, sicheres und schnelles Auffinden und Identifizieren der Boote auch aus der Entfernung wiederholt und während der gesamten Lebensdauer Boote ermöglicht.

Zeichnungslegende

1 Transponder
2 Datenträger
3 Antenne
4 Trägerschicht
5 Kontaktierungen
6 Kontaktierungsbereich Antenne
7 Kontaktierungsbereich Datenträger
8 Objekt (Boot)
9 Lesegerät
GPS Navigationssystem (Standortbestimmung)
DB Datenbank
Ex Exekutive (Polizei)
V Versicherung
P Presse
I Internet
S Sonstige (Eigentümer)

Patentansprüche

1. Elektronische Diebstahlsicherung für mobile Objekte (**8**), insbesondere für Wasser-, Land- und Luft-Fahrzeuge, **dadurch gekennzeichnet**, dass die elektronische Diebstahlsicherung mindestens einen mit dem Objekt (**8**) verbundenen Transponder (**1**) und mindestens ein externes Lesegerät (**9**) beinhaltet, wobei der Transponder (**1**) mindestens einen mit gespeicherten Daten versehenen Datenspeicher (**2**) und mindestens eine passive und/oder aktive Sende-/Empfangseinrichtung (**3**) für die drahtlose Energie- und/oder Datenübertragung mit dem mindestens einen Lesegerät (**9**) beinhaltet.

2. Elektronische Diebstahlsicherung nach Anspruch 1, dadurch gekennzeichnet, dass der Transponder (**1**) derart am Objekt (**8**) befestigt ist, dass er beim Versuch des Entfernens zerstört wird.

3. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass der Transponder (**1**) auf einer Trägerfolie (**4**) aufgebracht ist.

4. Elektronische Diebstahlsicherung nach Anspruch 3, dadurch gekennzeichnet, dass die Trägerfolie (**4**) auf der Seite, auf welcher der Datenspeicher (**2**) und die Sende-/Empfangseinrichtung (**3**) sich befinden, mit Klebstoff beschichtet ist.

5. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Transponder (**1**) am Objekt (**8**) einlaminiert wird.

6. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Transponder (**1**) am Objekt (**8**) mit einer Schutzschicht überklebt wird.

7. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Datenspeicher (**2**), als flüchtiger (RAM) oder nichtflüchtiger (ROM, EPROM, EEPROM) Speicher ausgebildet ist.

8. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass innerhalb des Datenspeichers (**2**) mindestens Identifikationsdaten des Transponders (**1**) gespeichert sind.

9. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Identifikationsdaten des Transponders (**1**) eine Seriennummer und Referenznummer beinhaltet.

10. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass innerhalb des Datenspeichers (**2**) Identifikationsdaten des Objektes (**8**) gespeichert sind.

11. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass innerhalb des Datenspeichers (**2**) Identifikationsdaten von auf das Objekt (**8**) bezogenen Personen oder Einrichtungen gespeichert sind.

12. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Sende-/Empfangseinrichtung (**3**) passiv ohne eigene Energiequelle ausgebildet ist.

13. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Sende-/Empfangseinrichtung (**3**) aktiv mit eigener Energiequelle ausgebildet ist.

14. Elektronische Diebstahlsicherung nach Anspruch 13, dadurch gekennzeichnet, dass die aktive Energiequelle Batterien und/oder wieder aufladbare Akkumulatoren beinhaltet.

15. Elektronische Diebstahlsicherung nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass das Lesegerät (**9**) ein Navigationssystem (GPS) beinhaltet, über welches Ortkoordinaten ermittelt werden können.

16. Verfahren zur automatischen Übertragung relevanter Daten mittels der elektronischen Diebstahlsicherung gemäss einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass durch das externe Lesegerät (**9**) aus dem Datenspeicher (**2**) des am Objekt (**8**) befestigten Transponders (**1**) via Antenne (**3**) relevante Daten drahtlos ausgelesen werden und mit den Daten einer speziellen externen Datenbank (DB) verglichen werden und bei einem als gestohlen gemeldeten Objekt (**8**) Informationen an externe Interessenten automatisch weitergeleitet werden.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass das Lesegerät (**9**) über sein Navigationssystem (GPS) Ortkoordinaten via Satelit (Sat) einliest, welche den Aufenthaltsort des gestohlenen Objektes angeben.

18. Verfahren nach einem der Ansprüche 16 oder 17,

dadurch gekennzeichnet, dass der Datenvergleich mit der speziellen externen Datenbank (DB) über eine Hardware-Schnittstelle oder drahtlos geschieht.

19. Verfahren nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (**8**) die relevanten aus dem Datenspeicher (**2**) ausgelesenen Identifikationsdaten enthalten.

20. Verfahren nach einem der Ansprüche 16 bis 19, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (**8**) die über Navigationssystem (GPS) des Lesegeräts (**9**) eingelesenen Ortkoordinaten enthalten.

21. Verfahren nach einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (**8**) mindestens an eine zentrale exekutive Stelle (Ex), wie z. B. die Wasserschutzpolizei weitergeleitet werden.

22. Verfahren nach einem der Ansprüche 16 bis 21, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (**8**) an die Versicherung und/oder den Versicherten weitergeleitet werden.

23. Verfahren nach einem der Ansprüche 16 bis 22, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (**8**) an die Öffentlichkeit in Form der Presse und/oder eine Adresse im Internet weitergeleitet werden.

Hierzu 3 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 42 805 A1
Int. Cl.[7]: G 08 B 13/00
Offenlegungstag: 14. März 2002

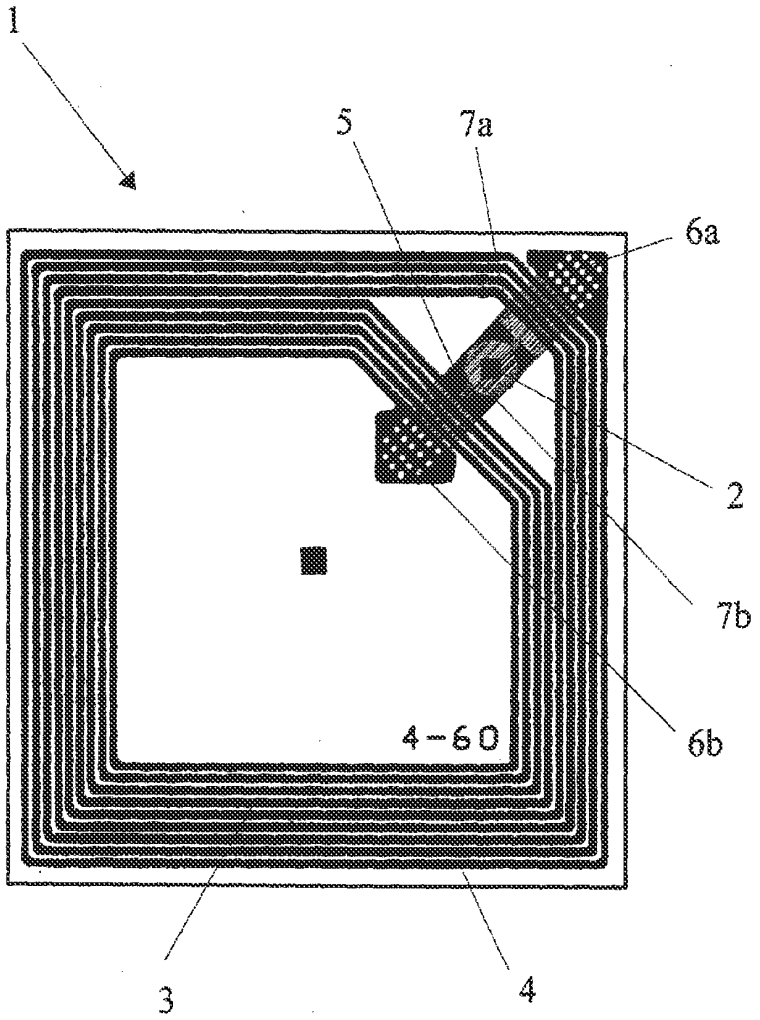


FIG. 1

Nummer: DE 100 42 805 A1
Int. Cl.[7]: G 08 B 13/00
Offenlegungstag: 14. März 2002

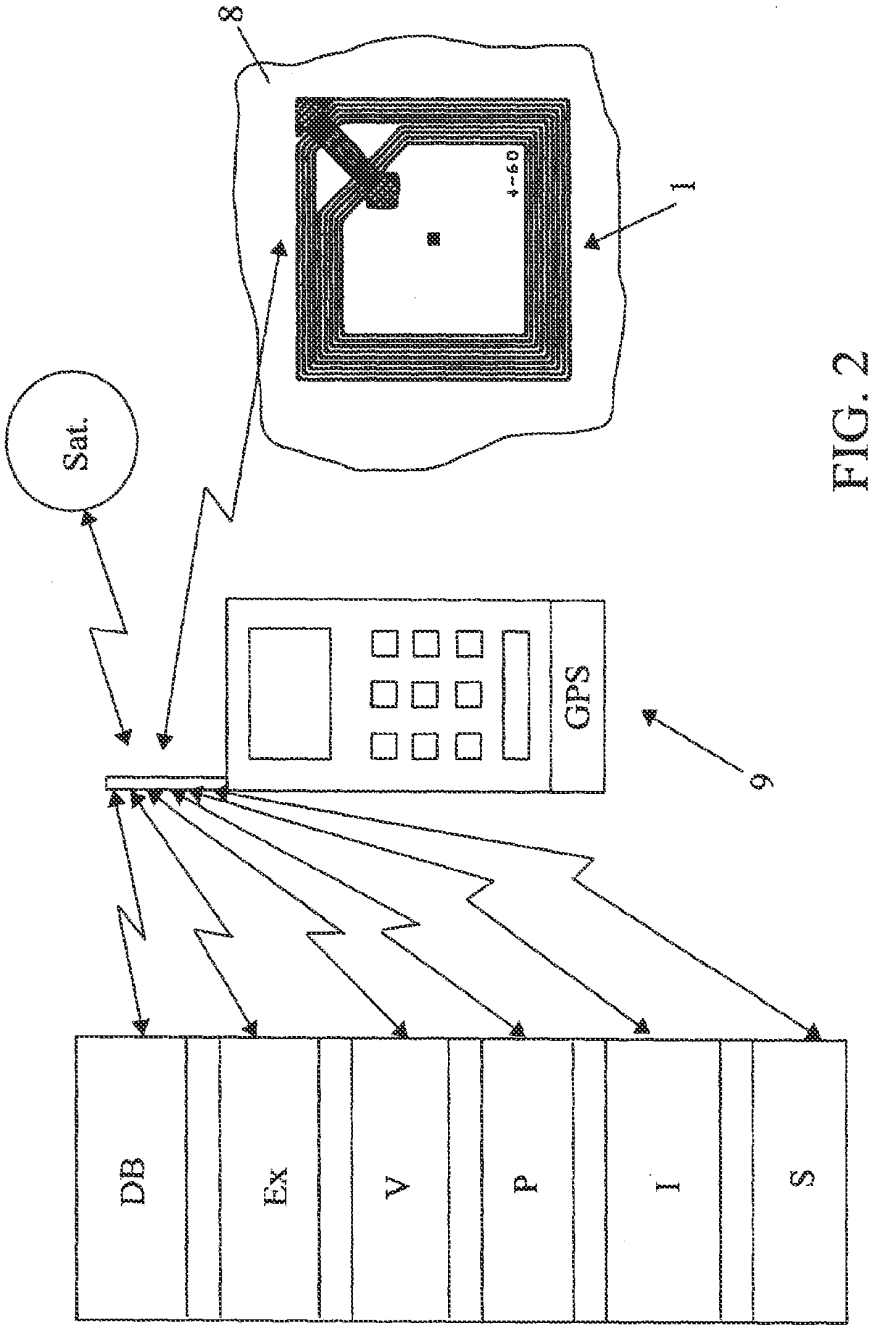


FIG. 2

Nummer: DE 100 42 805 A1
Int. Cl.[7]: G 08 B 13/00
Offenlegungstag: 14. März 2002

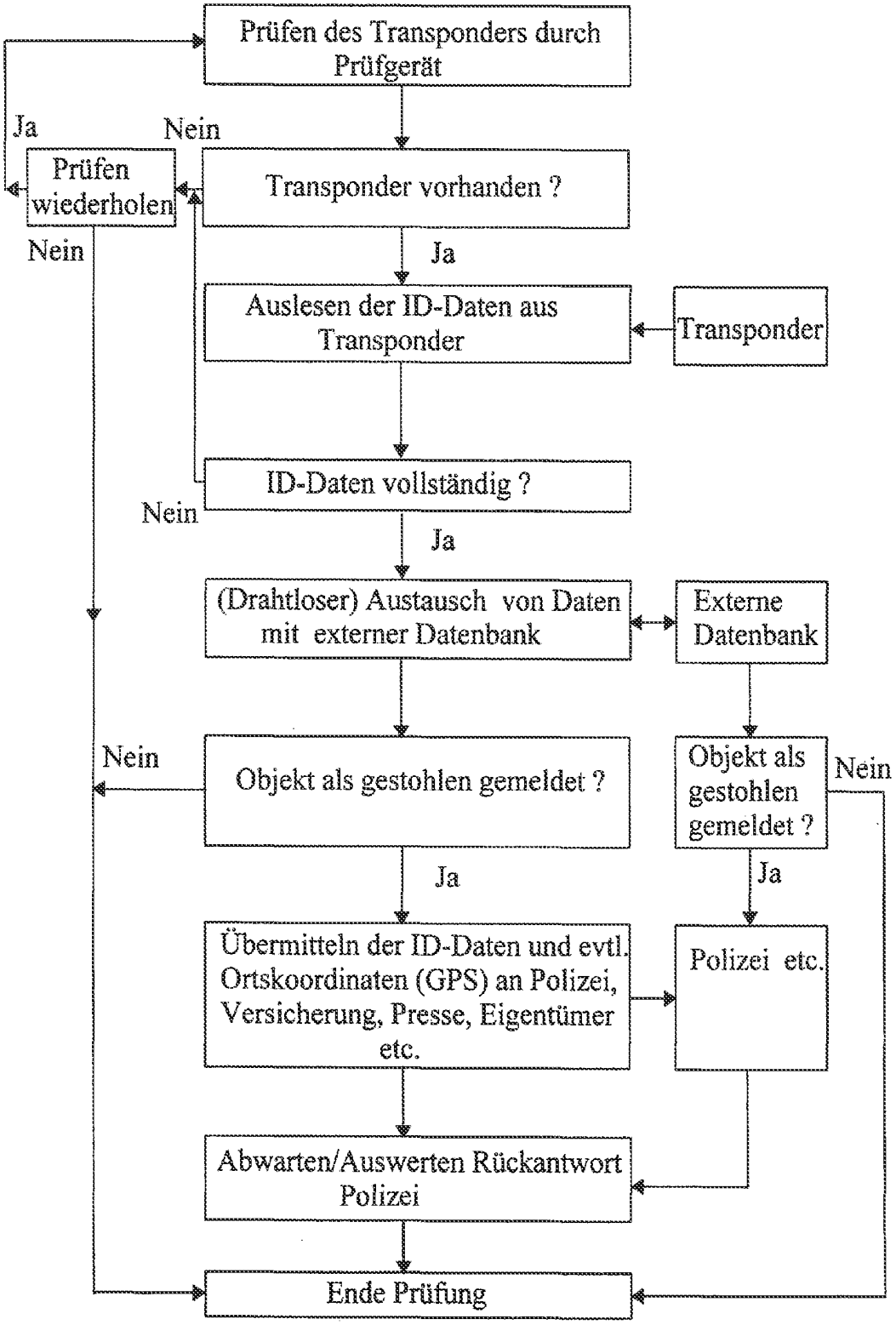


FIG. 3

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G01S | A2

(11) International Publication Number: **WO 98/43104**

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/US98/05686

(22) International Filing Date: 23 March 1998 (23.03.98)

(30) Priority Data:
08/824,242 25 March 1997 (25.03.97) US

(71)(72) Applicant and Inventor: PRICE, Frederick, J., R-W. [US/US]; 540 Buckingham #513, Richardson, TX 75081 (US).

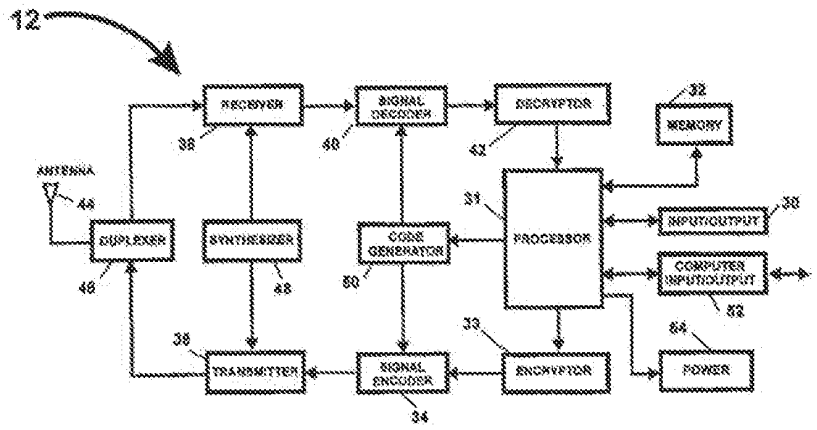
(72) Inventor: CLEVELAND, Joseph, Robert; 911 Grinnell Drive, Richardson, TX 75081 (US).

(74) Agents: CAYWOOD, Michael et al.; Locke Purnell Rain Harrell, Suite 300, 100 Congress Avenue, Austin, TX 78701 (US).

(81) Designated States: BR, CA, MX, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: VEHICLE IDENTIFICATION SYSTEM



(57) Abstract

A vehicle identification system for identifying motor vehicles in a group of vehicles at distances in excess of 200 feet is disclosed. The system includes an interrogator for directionally broadcasting an interrogation signal toward a vehicle of interest and a set of vehicle identification tags attached to the vehicles for receiving interrogation signals and sending a response signal to the interrogator. The response signal consists of information from the memory in the vehicle identification tag which allows the interrogator to identify the ownership or registration of the vehicle. Preferably, the tags have at least two memory portions with one portion being more secure than the other. Information useful to law enforcement agencies may be stored in the more secure memory portion and information for public or commercial use, such as parking access codes and toll information may be stored in the less secure memory portion. The system can link to an external database to verify and obtain more information regarding the owner of the vehicle, such as name, address, and record of traffic violations. Each tag on the vehicle also communicates with the other tags in the tag set on the vehicle, and, if the tags within a set are separated beyond a present distance or otherwise subjected to tampering, the tags will transmit an alarm to any nearby interrogator.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

VEHICLE IDENTIFICATION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an identification system for use in connection with the identification of motor vehicles. The vehicle identification system has particular utility in connection with law enforcement.

2. Description of Related Art

In the execution of their responsibilities to protect life and property, law enforcement officials must determine the registration and ownership of motor vehicles from the vehicle's license plate as quickly and safely as possible. Optical identification means historically used by these officials to determine the registration and ownership of motor vehicles adds to their burden to quickly resolve uncertain or dangerous situations. The current procedure limits the access to critical information because existing methods of determining a license plate number require visually reading the number from the plate, often from the rear of the vehicle. Optical or visual methods do not allow a rapid determination of a mismatch between the vehicle description and original registration or license information. In some circumstances, criminal intent, mud or poor lighting limits the visibility of license plate numbers.

Radio frequency identification techniques with compact, low-powered devices have long been known in the art. However, present devices and systems have deficiencies which hamper their effectiveness. Current approaches consist of a single tag and an interrogator. The current tags usually are small in size and transmit radio frequency electromagnetic signals at low power to extend the battery life. These approaches do not employ advanced signal techniques to thwart data errors caused by automotive electromagnetic interference or fading caused by multipath propagation. The small size of existing tags also results in an inefficient antenna. Tags with low power and inefficient antennae limit the transmission distance of the tag's transmissions to less than two hundred feet. Because the unaided eye can distinguish license plate numbers at similar ranges, the operation of an RF tag/interrogator system

at these ranges does not provide any significant advantage over optical or visual techniques for determination of license plate numbers. In addition, current interrogators do not have means to distinguish the signals transmitted by multiple tags that receive the interrogator transmission or to consult local or remote databases. Further, the information transmitted by current tag systems is not secure, thereby permitting unauthorized people to access the personal information of a motor vehicle owner.

The need, therefore, exists for a tag/interrogator system which can safely and reliably improve the identification of motor vehicles.

SUMMARY OF THE INVENTION

The system of the present invention overcomes the above-mentioned disadvantages and drawbacks which are characteristic of the related information. The present invention is a system for identification of a motor vehicle comprising an interrogator for sending an interrogation signal and a set of vehicle identification tags for receiving the interrogation signal and sending a response signal consisting of information in a memory of the vehicle identification tag. The memory of each vehicle identification tag comprises two portions with one portion being more secure than the other. Law enforcement information such as vehicle registration and owner identification records, may be stored in the secure memory portion of each tag. The less secure layer of memory can store information for public use, such as parking access and toll information.

Interrogators may be mobile or fixed at a location, depending on the intended use of the system. Interrogators for use by law enforcement prompt a vehicle identification tag to respond with information from the secure memory. Interrogators available to non-governmental entities prompt a vehicle identification tag to respond with information from the less secure memory. Both interrogators can cross-link the data in the vehicle identification tag to an external database, which may in a computer hardwired to the interrogator or in a remote location and using a communications link. An interrogator may also rewrite the less secure layer of memory. For example, if data in the less secure

layer comprises prepaid tolls, the interrogator can deduct toll charges from the data and rewrites the less secure layer with a new credit balance.

The system can determine a vehicle's identification even when multiple vehicles within the range of the system respond to the interrogator's signals. The interrogator receives this information, which is encrypted for security purposes, and can link to an external database to verify the information and use it to obtain other records, such as identification, address, and vehicle owner traffic violation and criminal record information. Each tag on a vehicle also communicates with the other tag(s) in the set, and, if the tags within a set are separated beyond a preset distance or otherwise subjected to tampering, the tags will transmit an alarm to any nearby interrogator. Each separated tag will also produce a visible alarm signal.

Numerous objects, features and advantages of the present invention will be readily apparent to those of ordinary skill in the art upon a reading of the following detailed description of the presently preferred, but nonetheless illustrative, embodiments of the present invention when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a basic vehicle identification system that uses RF signals as a medium to obtain vehicle registration data.

FIG. 2 is a representation of a vehicle identification system in use.

FIG. 3 is a block diagram of the functional components of the vehicle identification tag interrogator of the present system.

FIG. 4 is a block diagram of the functional components of a vehicle identification tag.

FIG. 5 is a flowchart of a software procedure to initialize and control the operation of the interrogator.

FIG. 6 is a flowchart of a software procedure used by an interrogator to create, encode and transmit a message.

FIG. 7 is a flowchart of a software procedure used by an interrogator to receive, decode and process a message.

FIG. 8 is a flowchart of a software procedure for the interrogator to search computer databases to link information in the database with information obtained from the vehicle identification tag.

FIG. 9 is a flowchart of a software procedure to initialize and control the operation of a vehicle identification tag.

FIG. 10 is a flowchart of a software procedure used by an identification tag to receive, decode and process a message.

FIG. 11 is a flowchart of a software procedure used by an identification tag to create, encode and transmit an message.

FIG. 12 is a flowchart of a software procedure for the identification tag to enter, change or add data to the identification tag memory.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to the drawings, and particularly to FIGS. 1 – 3, a preferred embodiment of a vehicle identification system of the present invention is shown and generally designated by the reference numeral 10.

FIG. 1 is a block diagram of a preferred mode of the automatic vehicle identification system. The system comprises an interrogator 12 for sending a radio frequency (RF) interrogation signal to a set of vehicle identification tags (VITs) 16.

In operation, an interrogator 12 transmits an interrogation signal 14 consisting of an encoded signal modulated onto a RF carrier signal to two or more vehicle identification tags (VITs) 16 mounted on respective vehicles 18 in its vicinity as shown in the figure. The signal from the interrogator 12 is directional, enabling the interrogator 12 to identify vehicles within a limited area. The interrogator signal 14 is an encoded, encrypted signal in order to protect against jamming, assure the integrity of transmitted and received data, provide reliable data exchange in noisy electrical conditions and prevent unauthorized access to internal processes and data. The interrogator 12 may be located in a police car on patrol or it may be at a fixed location, such as in a high crime area. Each VIT 16 that receives RF signals 14 first processes the signal to validate the authenticity of the received message. When the VIT 16 receives a properly encoded RF signal 14 from an interrogator 12, it performs a

decoding decryption process to extract the encoded message from the signal 14. After receipt of a validated message, the VITs 16 within a set on a vehicle communicate with each other to determine which VIT 16 received the strongest signal from the interrogator 12. The VIT 16 receiving the strongest signal then emits a response signal 20, which is an encoded RF signal, in response to the interrogator signal 14. By having the VIT 16 which receives the strongest signal respond to the interrogator, the reception distance is optimized. As a further advantage of having only a single VIT 16 emit a signal, less power is expended. In the alternative, all VITs 16 could transmit a response signal 20 and the interrogator 12 could filter weak or duplicate responses, processing only the strongest of the signals received from the same vehicle.

The memory of each VIT 16 has a secure portion and a less secure portion. Law enforcement information, such as vehicle registration and owner identification records, are stored in the secure layer of memory of each tag. Interrogators 12 for use by law enforcement prompt a VIT 16 to respond with information from the secure memory portion. A less secure layer of memory can store information for public use, such as parking access and toll information. Interrogators 12 available to non-governmental entities may prompt a VIT 16 to respond with information from the less secure memory portion. An interrogator 12 may also modify or rewrite the less secure portion of memory. For example, if data in the less secure portion comprises prepaid tolls, the interrogator can deduct toll charges from the data and rewrites the less secure layer with a new credit balance. At the end of its transmission, the VIT 16 turns off its transmission circuitry and turns on its receiver circuitry.

Upon receipt of a response signal 20 from a VIT 16, the interrogator 12 processes the signal to recover the data contained in the signals. Preferably, the RF signal generated by each VIT 16 is modulated and has unique identification codes embedded therein to allow the interrogator to distinguish response signals 20 transmitted by one VIT 16 from other VIT response signals 20, when, for example, multiple VITs 16 respond to a signal 14 transmitted from an interrogator 12. When the interrogator 12 receives a valid response message from a VIT 16, it stores the vehicle identification information contained in the message in memory and displays the data to the operator. When connected to a remote or local computer database server 22 by a

communications link 24 for access to databases such as motor vehicle records, criminal files, or warrant files to analyze vehicle identification records and owner information, the interrogator 12 allows authorized law enforcement officers to compare the stored registration information in the interrogator 12 with computer databases to determine if grounds exist to investigate the vehicle or its occupants. The computer database server 22 can also contain information, such as parking authorization or entrance authority, for commercial use. The interrogator 12 may also use a communications protocol such as the Point-To-Point Protocol (PPP), X.25 or Transport Control Protocol/Internet Protocol (TCP/IP), or any other protocol that will be obvious to those skilled in the art, to establish the communications link 24 with the remote computer database server 22. The interrogator 12 has the capability to communicate with remote computer database servers 22 over communications paths that include, but are not limited to: wire telephony circuits, cellular telephony circuits, and satellite circuits. During communications with a remote computer database server, the interrogator 12 can display the status of the computer network query to the interrogator operator. The interrogator 12 and VIT 16 take no action on received transmissions with messages that cannot be authenticated.

FIG. 2 depicts the preferred embodiment of the system in more detail. The interrogator 14 may be located in a moving vehicle, such as a police car 25, or at a fixed location, such as a limited access gate 26. Fixed interrogators may also be used for vehicle polling. For example, the interrogator can be used to poll vehicles in a high crime location, monitor traffic speeds, or monitor access to a car park or toll road.

A plurality of VITs 16 are attached to vehicles 18. In the embodiment shown, a set of two VITs 16 is used. The first VIT 16 is affixed to a license plate 28 of a vehicle. The second tag is placed in a secure location, such as the inside of the windshield 29. A position underneath the hood of the vehicle, however, could also be a suitable secure location for a tag.

State vehicle registration agencies, department of motor vehicle (DMV) agencies or other authorized government agencies could issue a set of VITs 16 in conjunction with a license plate at the time of vehicle registration. VITs 16 may be programmed with data selected and entered by the issuing governmental agency,

including a permanent registration number and expiration date. The information entered by the agency cannot be altered without a password; however, a secondary memory layer or portion may be programmed by a user interface, allowing VITs 16 also to function as parking cards, toll tags and other types of access or charge cards. The VIT 16 set remains in an inactive state until it is mounted to the vehicle. The purpose for this inactive setting is to prevent unintentional activation of a VIT 16 by interrogators in its radio reception range prior to its being attached to registered vehicles 18. The VITs 16 are mounted to the vehicles 18 at a place designated by the state. The expiration date of the VIT is printed on the VIT 16 and visible on the exterior of the vehicle. The VIT 16 uses secure techniques to prevent unauthorized entry of an activation pass key or access to internal processes and data. Once activated, the VIT 16 processor turns on power to the receiver circuitry for reception of the RF signals and turns off power to the transmission circuitry to conserve internal power. The VIT operates from an internal power source that can be externally recharged.

Different types of interrogators 12 may be used in conjunction with VITs 16. The primary type of interrogator would only be made available to governmental agencies, and receives information programmed by the issuing agency from the VITs. A secondary interrogator may be acquired by non-governmental establishments and used to receive information programmed by the establishment into the VIT's second memory portion, such as car park access, entry authority and toll road charges.

FIG. 3 is a block diagram of the interrogator 12 presented in FIGs. 1 & 2. The interrogator 12 comprises an operator input/output 30, a processor 31 for message data generation and detection, digital memory 32 for storage of program software and data, encryptor circuit 33 for data protection of transmitted messages, signal encoding circuit 34 for generating an encoded signal by transmitter 36 which up-converts and amplifies the signal, receiver 38 which amplifies and down-converts the received signal from a transmitting VIT, one or more signal decoding circuits 40 for demodulating the received signals, decryptor 42 for received messages, an antenna 44 to transmit and receive encoded RF signals, duplexer 46 for switching transmitted electromagnetic signals from the transmitter 36 to the antenna 44 and for switching

signals received by the antenna 44 to the receiver 38, a synthesizer 48 for generating high frequency carrier to the transmitter 36 for up-conversion of the RF signal to the transmission frequency and to the receiver 38 for down-conversion of the received RF signal from the transmission frequency, a code generator 50 for generating one of a plurality of codes for spread spectrum coding of the RF signal, a computer input/output circuit 52 for connecting the interrogator 12 to a remote computer database server over external circuits and a suitable power supply 54. In a preferred embodiment, the interrogator power supply 54 uses either standard 110-volt ac power, 12-volt dc power from a vehicle electrical system or from internal rechargeable battery power, although other types of power supplies known to those in the art could be used.

To initiate interrogation of a VIT 16 on a vehicle 18, the operator uses the input/output 30 to command the processor 31 in the interrogator 12 to generate a query message for transmission. The processor 31 is a commercially available digital signal processor. The processor 31 performs encoding and interleaving of the message data prior to passing the message data to the encryptor circuit 33. Preferably, the encryptor 33 employs the Digital Encryption Standard (DES) algorithm, however, other types of encryption, preferably other algorithms approved by the National Institute of Science and Technology (NIST), may be used. Preferably, the encryptor 33 employs a separate encryption circuit, however, a software-based encryption algorithm could be used by the processor 31.

The signal encoding circuit 34 receives the encrypted digital data from the encryptor 33 and modulates the code provided by the code generator 50. Preferably, high frequency, spread-spectrum modulation is used; however, other forms of signal propagation may be used. High-frequency, spread-spectrum modulation improves signal detection under multipath propagation conditions and lowers the peak power of the transmitted RF electromagnetic waveform. The signal encoder circuit 34 uses conventional spread-spectrum modulation.

The transmitter 36 mixes the high frequency carrier signal with the spread-spectrum modulated signal to up-convert the spread-spectrum modulated signal to the transmission frequency band and provides any needed amplification and filtering of the spread-spectrum modulated signal prior to transmission by the antenna 44 through

the duplexer 46. The antenna 44 converts the spread-spectrum modulated signal into a RF spread-spectrum signal. Upon initiation of the interrogator 12 by the operator via the input/output 30, the processor 31 switches the duplexer 46 to the transmitter 36 to protect the receiver 38 from damage by the RF signal sent from the transmitter 36 to the antenna 44 during transmission of the encoded RF signals. Upon completion of the transmission of the RF signals, the processor 31 switches the duplexer 46 from the transmitter 36 to the receiver 38 in order for the interrogator 12 to receive RF signals transmitted by one or more VITs.

During reception, the antenna 44 receives RF signals and converts the RF encoded signals into RF spread-spectrum modulated signals which pass through the duplexer 46 to the receiver 38. The receiver 38 provides any needed amplification of the received RF spread-spectrum signal from the antenna 44 and mixes the high frequency carrier signal from the synthesizer 48 with the received spread-spectrum signal to down-convert the spread-spectrum RF signal. Spread-spectrum modulation provides improved signal detection of signals received from the VIT under multipath propagation and high electromagnetic noise conditions.

One or more signal decoders 40 receive the down-converted spread-spectrum modulated RF signal from the receiver 38. The decoder 40 performs spread-spectrum demodulation with the code provided by the code generator 50 to produce one or more digital data streams that contains one or more encrypted message data transmitted by one or more VITs. Each signal decoder includes a digital data buffer to store the digital data for encryption. The signal decoder 40 uses conventional spread-spectrum demodulation circuitry. The signal decoder 40 passes the demodulated digital data stream to the de-encryptor 42, which uses the same algorithm and encryption key as used by the encryptor 33. The processor 31 performs decoding and de-interleaving of the data message received from the de-encryptor 42 then displays the received vehicle registration data on the input/output 30 to the authorized operator. The operator may elect to establish a connection to a remote computer database server through a computer input/output 52.

Modulation encoding used by the interrogator 12 and VITs 16 mitigates two basic causes of performance degradation of signal quality, namely (1) multipath fading

of the radio link and (2) interference caused either by other radio transmitters in the vicinity and by electromagnetic interference from automotive devices. The system 10 uses wideband spread spectrum modulation encoding with a pseudorandom binary sequence for both the interrogator and VIT signals to enhance performance in the presence of these degradations. The pseudorandom number (PN) sequence, or code, gives the transmitted signal an individual signature code. Each receiving VIT uses the same code to demodulate the received signals. To respond to an interrogator, each VIT randomly selects a unique binary sequence, or code, from a list stored in its memory. The number of available codes is large enough so that the probability that two or more VITs in the same vicinity will select the same code is small. The interrogator uses a directive antenna which limits the width of radiation pattern so that only a few vehicle VITs will receive an interrogator transmission that is powerful enough to be recognized.

The receiver of the modulation encoded signals has a synchronized signal decoder which despreads the spectrum with the same PN sequence as that of the corresponding transmitter. Each signal decoder uses a correlator that accepts only signal energy from the binary sequence defined by the assigned code and despreads the spectrum. Signals with codes that do not match the correlator code are not despread. All other waveforms not correlated with the selected binary sequence or code, such as automotive electromagnetic interference, are effectively spread over a wider bandwidth than that of the final demodulator bandwidth. The interrogator has a signal decoder for each possible binary sequence selectable by the VIT. The VIT has a single decoder which uses a code matched to the pseudorandom sequence used by the interrogator to modulation encode the signal for transmission. The wideband character of the modulation by the pseudorandom binary sequence introduces frequency diversity which mitigates against multipath propagation. The waveform also rejects multipath returns that fall outside the correlation interval of the pseudorandom modulation encoding.

The capability of an interrogator to query and receive responses from one or more VITs separated by a distance d up to or greater than 200 feet (~61 meters) is limited by the link loss budget and by the noise or interference at the receiver. Those

familiar with the art will recognize the expression for the link loss budget L(d) given by:

$$L(d) = P_R(dBm) - P_T(dBm) = 20\log\left[\frac{c}{4\pi f}\right] + g_T + g_R - 10n\log(d) + X_\sigma$$

where P_T is the power into the transmitter antenna in dBm, P_R is the power from the receive antenna in dBm, c is the speed of light, f is the frequency, n is the power law relationship between distance and received power, g_T is the transmit antenna gain in dB, g_R is the receive antenna gain in dB, and X_σ is a zero mean random variable in units of dB that reflects the variation of received power due to the effects of reflection, diffraction and scattering on the propagation of the signal. In an urban setting for distances up to 200 feet (~61 meters), the power law factor n has a spread of 2~3.5, with a mean value of ~2.7. If the ratio of the received power to the noise (N) plus interference (I), expressed as C/(N+I), exceeds a minimum value, reliable communications exists. In the preferred embodiment, the threshold level corresponds to a bit error rate of 10^{-6} or better. In the typical urban environment, automobile ignition noise is a major contributor to interference, which may be greater than 40 dB above the thermal noise level. With spread spectrum modulation, combined with channel encoding of the present embodiment, a C/(N+I) value of typically -15 dB will provide reliable reception. As a result, the required transmitter power P_T is approximately 6 milliwatts or greater with g_T=3 dB, g_R=0 dB and n=2.7 at a carrier frequency of 800 MHz.

The term X_σ describes the statistical variation of the received power. The system 10 allows remote interrogation of a VIT by an interrogator 12 under stationary conditions or when either or both are in motion. As the interrogator 12 and VIT 16 move over distances relative to each other, the instantaneous received signal strength will fluctuate rapidly to give rise to fading. The result is that the many contributions have random phases so the sum behaves as a noisy signal manifested as Rayleigh fading. The received signal power may vary by as much as 20-30 dB when the transmitter-to-receiver separation changes by only a fraction of a wavelength. During periods of fading, the received signal may fall below that needed for reliable reception. It is commonly know that at a frequency of 850 MHz and a relative speed of 15 miles

per hour, the rate of fluctuation of the signal reception at a 10-dB level below the average power of a fading signal is 15 nulls per second. The average duration of a fade is approximately 6.6 milliseconds, which exceeds the time period of a digital word. The preferred embodiment of the system 10 uses channel encoding and interleaving to improve reliable transmission of data these circumstances.

FIG. 4 is a block diagram of a VIT 16. The VIT is programmed via a registration input 56 by a computer that communicates with the processor 64 through the decryption circuit 62 to read or store data in memory 66. The registration computer encrypts the data exchanged with the processor 64 with the same encryption key used by the decryption circuit 62 in the VIT 16. For authorized government purposes, registration software executes in the processor 64 to store data in or retrieve data from the first layer or primary partition of memory 66 for the registration computer. For non-government establishments, registration software executes in the processor 64 to store data in or retrieve data from the secondary layer of memory 66 for the registration computer.

During reception, the antenna 74 receives RF encoded signals and converts the signals into RF spread-spectrum modulated signals which pass through the duplexer 76 to the receiver 58. The receiver 58 amplifies the received RF spread-spectrum signal from the antenna 74 and mixes the high frequency carrier signal from the synthesizer 78 with the received spread-spectrum signal to down-convert the spread-spectrum RF signal. The receiver 58 uses a phase-locked-loop to synchronize the synthesizer 78 to the carrier frequency of the received RF signal. The signal decoder 60 receives the down-converted spread-spectrum modulated RF signal from the receiver 58 and performs spread-spectrum demodulation with the binary sequence provided by the code generator 80 based on the code provided by the processor 64 to produce a digital data stream that contains the encrypted message data. To demodulate the received modulation encoded signal, the code used by the VIT 16 matches that used by the transmitting interrogator 12. The signal decoder 60 uses conventional spread-spectrum demodulation circuitry. The signal decoder 60 passes the demodulated digital data stream to the decryptor 62, which uses the same algorithm and encryption key as used by the encryptor 33. The processor 64 performs decoding,

de-interleaving and validation of the message data received from the de-encryptor 62. Upon completion of the message reception, the processor 64 switches the duplexer 76 to the transmitter 72 to protect the receiver 58 from damage by the RF signal sent from the transmitter 72 to the antenna 74 during transmission of the encoded RF signals.

For responding to the interrogator 12 after validation of the received message data, the processor 64 of the VIT 16 retrieves the requested data from memory 66 and performs encoding and interleaving of the response message data prior to passing the response message data to encryptor 68. For a message from a primary interrogator 12 used by an authorized government operator, the processor retrieves the requested data from the primary or first layer memory. For a message from a secondary interrogator used by a non-government establishment, the processor retrieves the requested data from the secondary less secure memory layer. The processor 64 is a conventional digital signal processor. Preferably, encryptor 68 employs the Digital Encryption Standard (DES) algorithm, however, other types of encryption, preferably other algorithms approved by the National Institute of Science and Technology (NIST), may be used.

The signal encoding circuit 70 receives the encrypted digital data from the encryption circuit 68 and uses the code provided by the code generator 80 to modulate the encoded message data with the pseudorandom binary sequence. The processor 64 randomly selects one of several codes for use by the code generator. In the preferred embodiment, high frequency, spread-spectrum modulation is used; however other forms of signal propagation may be used. High-frequency, spread-spectrum modulation improves signal detection under multipath propagation conditions and lowers the peak power of the transmitted RF signal. The signal encoder circuit 70 uses conventional spread-spectrum modulation circuitry.

The transmitter 72 mixes the high frequency carrier signal with the spread-spectrum modulated signal to up-convert the spread-spectrum modulated signal to the transmission carrier frequency and provides any needed amplification and filtering of the spread-spectrum modulated signal prior to transmission by the antenna 74 through the duplexer 76. The antenna 74 converts the spread-spectrum modulated signal into a RF spread-spectrum signal. Upon completion of the transmission of the RF signals,

the processor 31 switches the duplexer 46 from the transmitter 36 to the receiver 38 in order for the interrogator 12 to receive RF signals transmitted by an interrogator. The processor 64 also commands the power supply 82 to turn off power to the transmitter 72, signal encoder 70 and encryptor 68 to conserve the VIT battery power. Preferably, the VIT power supply 82 uses internal rechargeable battery power, although other types of power supplies may be used. Integrated into the power supply 82 is a digitally controlled switch for controlling the application of power to selected portions of the VIT 16 in order to conserve battery power.

FIG. 5 is a flowchart of a software procedure executed by interrogator processor 28 to initialize and control the operation of the interrogator 12 shown in FIG. 2. The interrogator processes commence when power is applied to the interrogator 12. Initialization circuit 92 performs tasks such as running self-tests on interrogator components. Initialization circuit 92 passes its results to the select query mode 94, which displays the results on the interrogator input/output 26 for operator viewing. If there is an initialization failure, the interrogator 12 branches to power-down 96 upon operator acknowledgment. If initialization 101 is successful, the interrogator input/output 26 displays a message for the operator to enter a password for authorized use of the interrogator. Failure to enter a correct password within a prescribed amount of time or a prescribed number of attempts causes the procedure to branch to power-down 96, which turns off the power to the interrogator hardware. Upon correct entry of the password, the procedure in block 94 displays options for operator input. In the present embodiment, selection of an interrogation mode by the operator causes the procedure to branch to interrogator message creation in FIG. 6. Selection of a database mode by the operator via the input/output, causes the procedure to query the operator on the input/output for a database selection. The database mode allows the operator to read stored data received from a VIT or to establish connection with a local or remote computer or database server. After a database is selected, the procedure jumps to database search mode, described in FIG. 8, to access the database. If the operator selects the receive-only mode via input/output causes the procedure to branch to block 131 in FIG. 7. Selection by the

operator via the input/output to discontinue use of the interrogator causes the circuit to branch to power down 96, which resets the procedure and turns off the interrogator.

FIG. 6 is the flowchart setting forth a software procedure for the interrogator hardware described in FIG. 3 to create, encode and transmit a message. In the present embodiment, data from the interrogator memory is used to create a message 100. The message is encoded 102. Message encoding 102 comprises channel encoding the message data for error detection, error correction and validation. Next, the encoded digital data is interleaved 104. Interleaving is used to mitigate the effects of multipath fading. After interleaving, the digital data is transmitted 106. To transmit data in the present embodiment, the interrogator duplexer is switched to the transmit path. Then the modulation code is retrieved from memory and sent to the code generator. The modulation code is appended to a digital data synchronization block. A synchronization pulse is initiated by the transmitter, which sends the interleaved and encoded digital data to the encryption block. After the digital data is transferred to the encryption block, transmit data 104 switches the duplexer to receive mode to receive any VIT responses.

FIG. 7 is the flowchart setting forth a software procedure for the interrogator hardware in FIG. 3 to receive, decode and process a message upon activation by the operator in block 94. When the interrogator is in receive data mode 110, the output of the decryption block is monitored for receipt of a digital data stream. If no digital data is received within a prescribed time period, the operator is informed via the interrogator input/output that no VIT data was received. If digital data is received, the procedure passes the digital data stream to the de-interleave message data block 112. The de-interleave block 112 removes the appended synchronization block and de-interleaves the received digital data stream to produce an encoded message data. Next, the de-interleaved data is decoded 114. Decode message data 114 performs error checking and correction. The decoded data is then validated 116 to confirm the message data was originated by an authorized interrogator operator. If the message data is not valid, the procedure branches to query mode 94 and informs the operator via input/output that an invalid message was received. If a valid message was received, the message is stored 118 in memory and displayed 120 on the input/output

for operator viewing. The operator is queried 122 via the input/output for action regarding the received message data. If the operator elects to query a computer data base for matches of vehicle registration data, the query operator procedure asks the operator to select a database operator on the input/output and then proceeds to establish connection with the desired computer database as detailed in Fig. 8. If the operator elects not to query a computer database, the procedure branches to query mode 94 for operator input regarding a new interrogator selection.

FIG. 8 is the flowchart setting forth a software procedure for the interrogator hardware in FIG. 3 to search computer databases for matches with vehicle registration data. If an operator selects to initiate a database query, the operator enters vehicle data and selects a database 124 from choices programmed into memory. A communications link to the designated computer database is established 126. Once the communications link is established 126, the operator is prompted via the input/output to log into the computer database 128. If the operator does not or is not able to log into the computer database within a specified time limit or within a specified number of attempts, the communications link to the computer is disconnected and a message that the selected computer database login failed is displayed on the input/output. If the computer database is successfully accessed, the database is searched 130 for matches to the vehicle registration data received from the VIT. Any matches found in the search of the computer database are retrieved 132 and displayed on the input/output.

FIG. 9 is a flowchart of a software procedure that executes in the VIT processor shown in FIG. 3. Upon the application of power to the VIT, program control begins at block 140. The procedure passes control to initialization 142 to perform self-tests on VIT components. Upon completion of self-tests, initialization 142 determines the test results and passes the results to query mode 144, which transfers the test results to the registration input for operator viewing by an external computer. If self-test detects a fault, the procedure notifies the operator through the registration input and returns to start 140. If the self-test procedure is successful, the procedure informs the operator via the registration input and displays a message for the operator to enter a password for authorized access to the VIT. Failure to enter a

correct password within a prescribed amount of time or a prescribed number of attempts causes the procedure to return to start 140. Upon correct entry of the password through the registration input, the procedure in block 144 displays options for operator input, for example, message creation.

FIG. 10 is the flowchart of a software procedure for a VIT to receive, decode and process a message upon receipt of a message from an interrogator. To receive data 146, the output of the decryption block is monitored for receipt of a digital data stream. When digital data is received, the digital data stream is de-interleaved 148. De-interleaving message data 148 also removes the appended synchronization block to produce encoded message data. Next, the de-interleaved data is decoded 150 and error checking and correction is also performed. The message data is validated to confirm it was originated by an authorized interrogator. If the message data is not valid, the procedure returns to receive mode 146 and awaits the next interrogation message. If the message is valid, a response to the transmitting interrogator is generated according to FIG. 10.

FIG. 11 is the flowchart setting forth a software procedure for the VIT hardware in FIG. 3 to create, encode and transmit a message upon receiving an interrogation signal. A VIT response message is created using data stored in VIT memory. The message data and format are encoded 156 for security purposes and interleaved 158 to mitigate the effects of multipath fading. Next the message is transmitted 160. To transmit a message 160, the duplexer is switched to the transmit path, a modulation code is retrieved from memory and sent to the code generator, a synchronization block is appended to the digital data, and the transmitter initiates a synchronization pulse and sends the interleaved and encoded digital data to the encryption block. Then a modulation code is randomly selected from a list of authorized codes stored in memory and the data is modulated and transmitted. After data is transmitted 160, the duplexer is returned to receive mode 146 to receive any interrogation transmissions.

The present invention allows determination of vehicle registration data from advantageously greater distances with multiple vehicles in the range of the system. It uses a radio frequency electro-magnetic wave (RF) technology to obtain encoded

vehicle identification and registration data. The invention allows authorized public safety officials to read vehicle identification and vehicle registration data in harsh or dirty conditions from any direction. It provides such officials with the capability to identify each vehicle uniquely from a remote location even when the license plate is not clearly visible. It provides capability for computer communications to compare vehicle identification with either local or remote databases such as Department of Motor Vehicles (DMV) files, criminal Files, Warrant Files, etc. The invention can replace passive visual techniques for determining the registration identification and ownership of vehicles used in public and private transportation, and overcomes the limitations imposed by passive optical reading methods. With rapid access to information about the vehicle, authorized officers have the capability to make optical or visual mismatch recognition quickly.

While preferred embodiments of the invention have been shown and described, it will be understood by persons skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the invention which is defined by the following claims

CLAIMS:

1. A system for identification of a mobile vehicle, comprising:

an interrogator for sending an interrogation signal;

a plurality of tags located on a vehicle comprising a memory and a transceiver for receiving said interrogation signal and sending a response signal comprised of vehicle identification information stored in said memory.

2. The system of claim 2 wherein said memory of said vehicle identification tags includes a first portion and a second portion wherein said first portion is used to store information requiring a higher level of security than the information stored in the second portion.

3. The system of claim 2 wherein data in said first portion of said memory is used to store information suitable for use in law enforcement.

4. The system of claim 3 wherein said interrogator sends an interrogation signal to prompt said vehicle identification tags to send a response signal which comprises data from said first portion of said memory.

5. The system of claim 4 further comprising a database having additional law-enforcement-related information wherein said interrogator can associate data from said first portion of said memory with information from said law enforcement database.

6. The system of claim 5 wherein said law enforcement database comprises information associated with the registered owner of the vehicle, such as owner identification, owner address, traffic violations and criminal record information.

7. The system of claim 2 wherein data in the second portion of said memory comprises information for public use.

8. The system of claim 7 wherein said interrogator sends an interrogation signal to prompt said vehicle identification tags to send a response signal comprising data in said second portion of said memory.

9. The system of claim 8 further comprising a database wherein said interrogator can associate data from said second portion of said memory with information in said database.

10. The system of claim 9 wherein said database comprises vehicle access privileges to a secure area.

11. The system of claim 9 wherein said interrogator can modify data in said second portion of said memory.

12. The system of claim 11 wherein said data in said second portion of said memory comprises prepaid tolls and said interrogator deducts toll charges from said data and rewrites said second portion of said memory with a credit balance.

13. The system of claim 1 wherein in response to an interrogation signal from the interrogator, said identification tags communicate with one other to determine which of said vehicle identification tags received a more powerful interrogation signal, and wherein said response signal from the vehicle is emitted by the tag receiving the most powerful signal.

14. The system of claim 1 wherein said plurality of tags on a vehicle constitute a set, and wherein the tag transceivers of the set periodically communicate with one another using a signal which can only be detected within a predetermined distance, and wherein a tag emits an alarm signal detectable by an interrogator if one vehicle identification tag is separated more than the predetermined distance from the other vehicle identification tags of the set.

15. The system of claim 14 wherein said tags include means for emitting a visible signal if a vehicle identification tag is separated more than a predetermined distance from the other vehicle identification tags of the set.

16. The system of claim 1 wherein said tag transceivers on the vehicle periodically communicate with one another, wherein a tag sends an alarm signal detectable by an interrogator if a tag is subjected to tampering.

17. The system of claim 13, 14 or 16 wherein a first tag is mounted on a license plate of said vehicle.

18. The system of claim 17 wherein a second tag is mounted in a secure location on the vehicle.

19. The system of claim 1 comprising at least one other vehicle having a plurality of tags, wherein the memory of the identification tags mounted to each vehicle contains information unique to that vehicle.

20. The system of claim 19 wherein the interrogator includes a directional antenna for limiting the direction of the interrogation signal to permit vehicle differentiation.

21. The system of claim 19 wherein said interrogator and tags include encryption means for encrypting the interrogation and response signals for security and vehicle differentiation purposes.

22. The system of claim 19 wherein said interrogator and tags include means for spread spectrum modulation of the interrogation and response signals for improved reception of the transmitted signals.

23. The system of claim 19 wherein said interrogator and tags include means for interleaving the transmission of the interrogation and response signals for increased reception.

24. The system of claim 19 wherein said vehicle identification tags further comprise antenna optimized for transmission ranges of greater than 200 feet.

25. A set of vehicle identification tags comprising a memory and a transceiver for receiving a predetermined interrogation signal and sending a response signal comprising information in said memory, wherein each vehicle identification tag in said set is able to communicate with the other vehicle identification tags in said set.

26. The set of claim 26 wherein in response to an predetermined interrogation signal, said vehicle identification tags communicate with one other to determine which of said vehicle identification tags received a more powerful signal, and said response signal is emitted by the vehicle identification tag receiving the most powerful predetermined signal.

27. The set of claim 26 wherein said vehicle identification tags transmits an alarm signal if one vehicle identification tag is separated more than a predetermined distance from the other vehicle identification tags.

28. The set of claim 26 wherein said vehicle identification tags transmit an alarm signal if a vehicle identification tag is subjected to tampering.

29. The set of claim 26 wherein said vehicle identification tags will produce a visible signal if a vehicle identification tag is separated more than a predetermined distance from the set.

30. The set of claim 26 wherein a vehicle identification tag is mounted on a license plate of said vehicle.

31. The set of claim 26 wherein a vehicle identification tag is mounted in a secure location on the vehicle.

32. A vehicle identification tag comprising:

a memory for storing information;

a transceiver for receiving a predetermined interrogation signal and sending a response signal comprising information in said memory; and

a power supply for providing power to said transceiver.

33. The vehicle identification tag of claim 33 wherein said power supply has a power conservation mode and a burst mode.

34. The vehicle identification tag of claim 34 wherein said power supply switches from said power conservation mode to said burst mode when an interrogation

signal is received, thereby enabling said vehicle identification tags to emit a signal in response to said interrogator.

35. The vehicle identification tag of claim 35 wherein said power supply switches from said power conservation mode to said burst mode according to a predetermined cycle, enabling said first identification tag to communicate with said second identification tag.

36. The vehicle identification tag of claim 33, further comprising visible vehicle identification information.

37. A method for identifying mobile vehicles, comprising:

directing an interrogation signal to an area containing vehicles with tags capable of identifying the interrogation signal and sending a response signal, said response signal consisting of information identifying the tagged vehicle;

receiving said responses from said vehicles in said area at an interrogator;

distinguishing between response signals sent by tags from more than one vehicle and processing the response from a single vehicle.

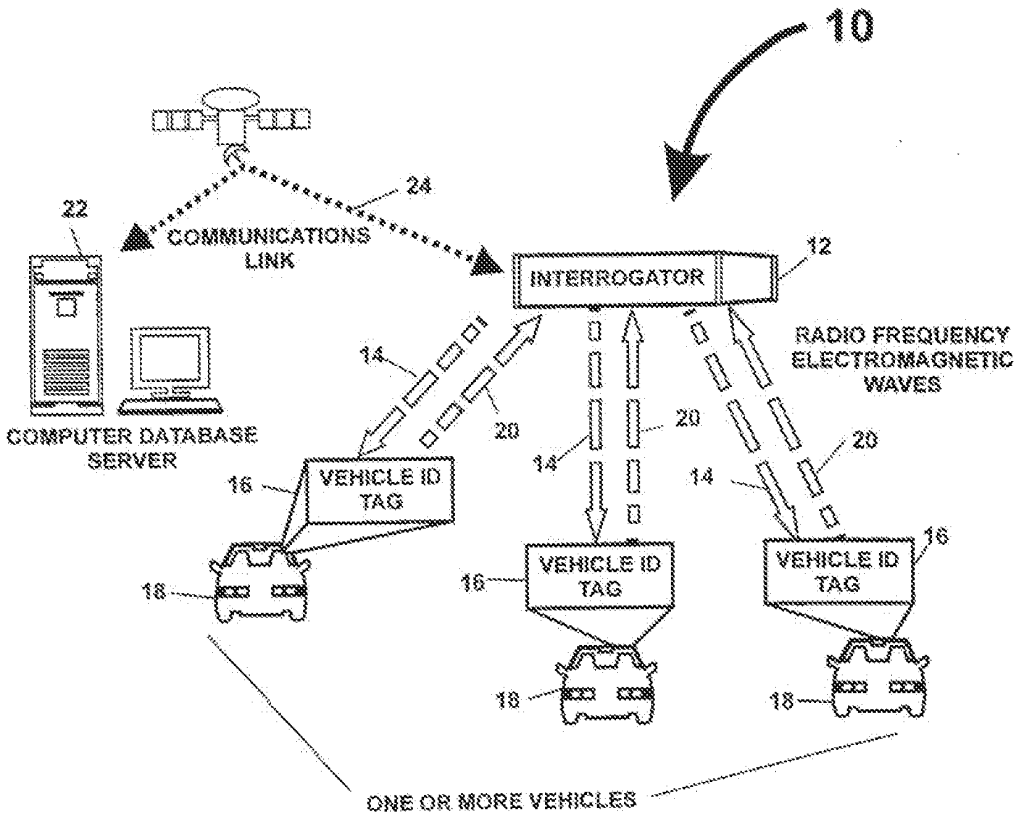

10
22
24
COMMUNICATIONS LINK
INTERROGATOR
12
RADIO FREQUENCY ELECTROMAGNETIC WAVES
COMPUTER DATABASE SERVER
14
20
16
VEHICLE ID TAG
18
ONE OR MORE VEHICLES

Figure 1

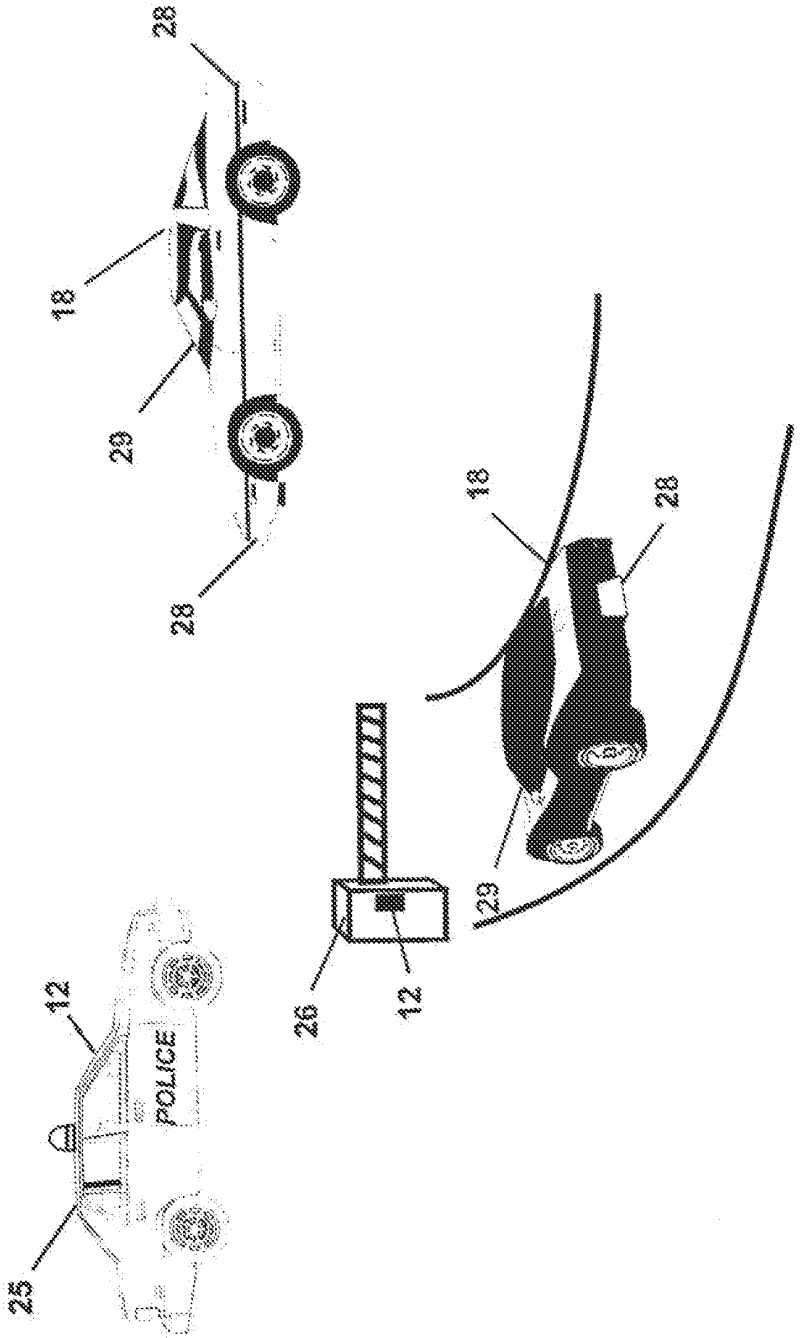


Figure 2

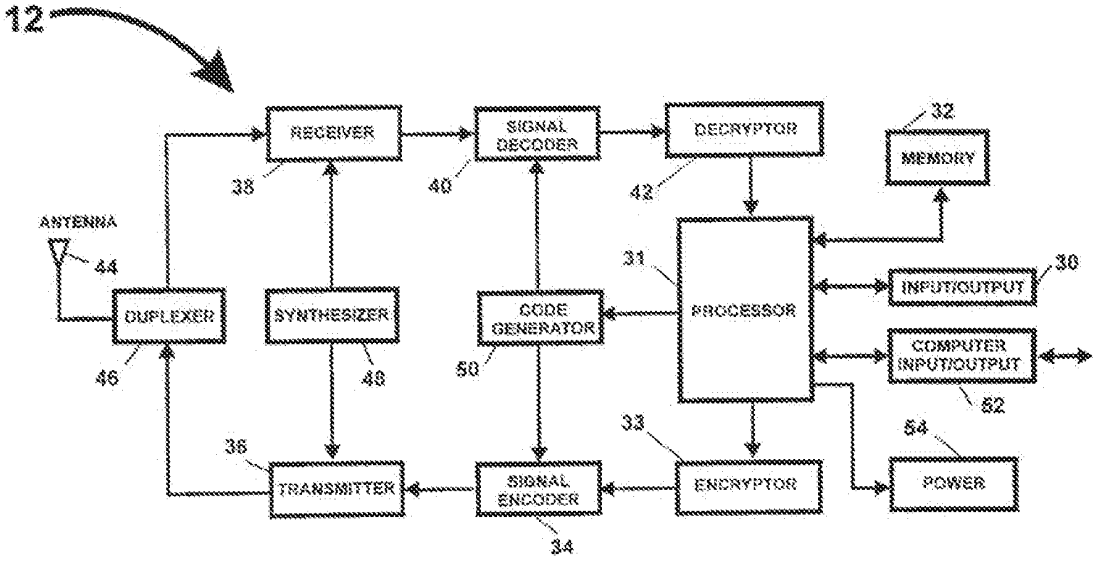

12
RECEIVER
SIGNAL DECODER
DECRYPTOR
MEMORY
32
38
40
42
ANTENNA
44
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
INPUT/OUTPUT
30
31
46
48
50
COMPUTER INPUT/OUTPUT
52
33
54
36
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR
POWER
34

Figure 3

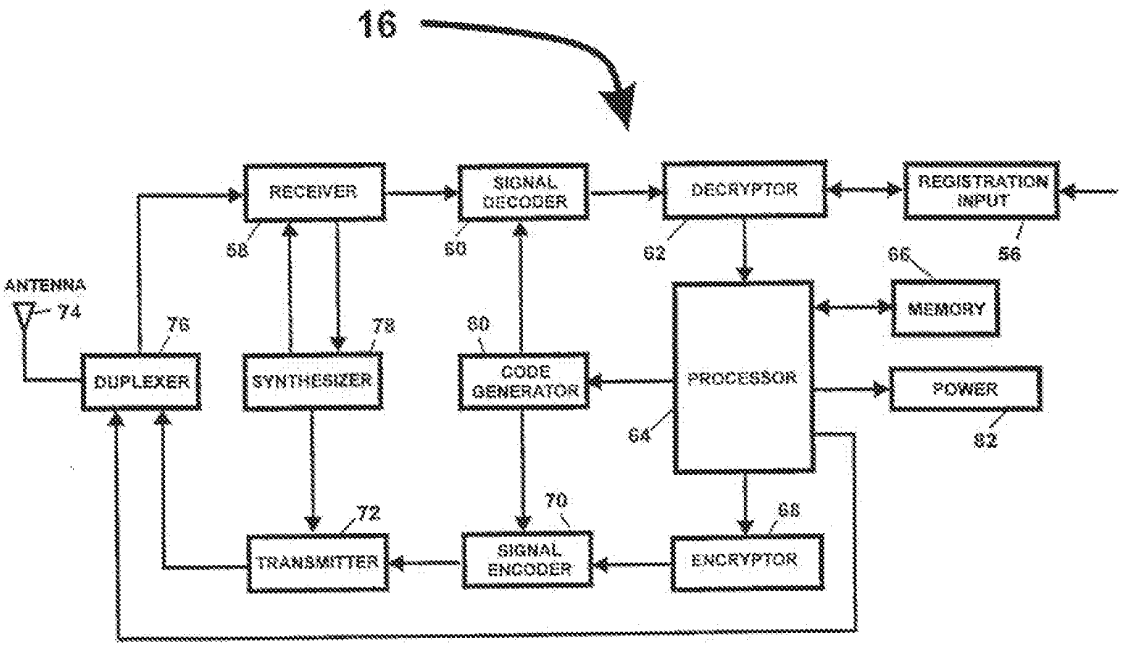

16
RECEIVER
SIGNAL DECODER
DECRYPTOR
REGISTRATION INPUT
58
60
62
56
66
ANTENNA
74
MEMORY
76
78
80
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
POWER
64
82
72
70
68
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR

Figure 4

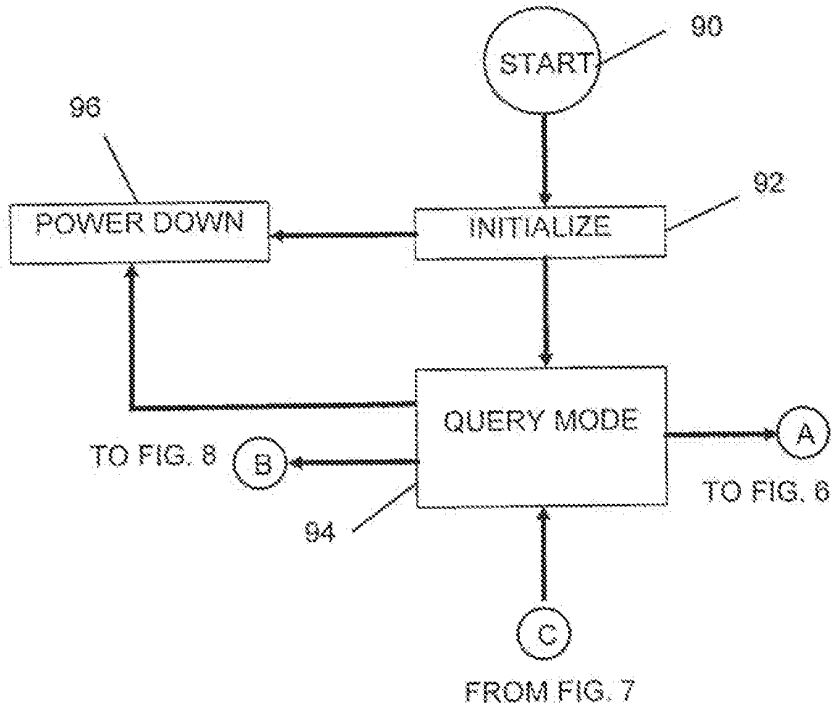

START
90
96
POWER DOWN
INITIALIZE
92
QUERY MODE
TO FIG. 8
B
A
TO FIG. 6
94
C
FROM FIG. 7

Figure 5

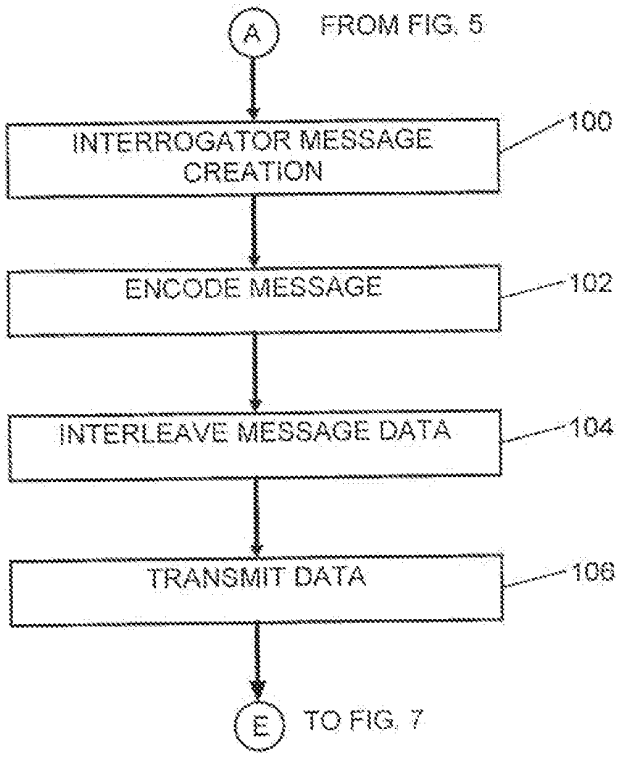

A
FROM FIG. 5
INTERROGATOR MESSAGE CREATION
100
ENCODE MESSAGE
102
INTERLEAVE MESSAGE DATA
104
TRANSMIT DATA
106
E
TO FIG. 7

Figure 6

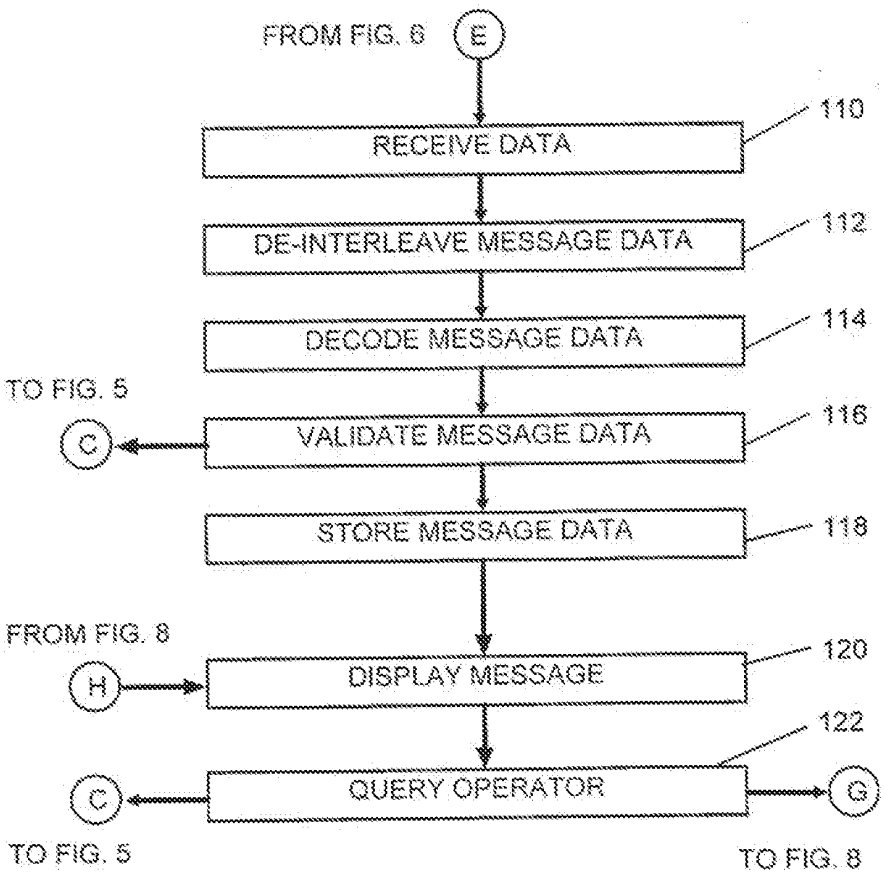

FROM FIG. 6
E
RECEIVE DATA
110
DE-INTERLEAVE MESSAGE DATA
112
DECODE MESSAGE DATA
114
TO FIG. 5
C
VALIDATE MESSAGE DATA
116
STORE MESSAGE DATA
118
FROM FIG. 8
H
DISPLAY MESSAGE
120
122
C
QUERY OPERATOR
G
TO FIG. 5
TO FIG. 8

Figure 7

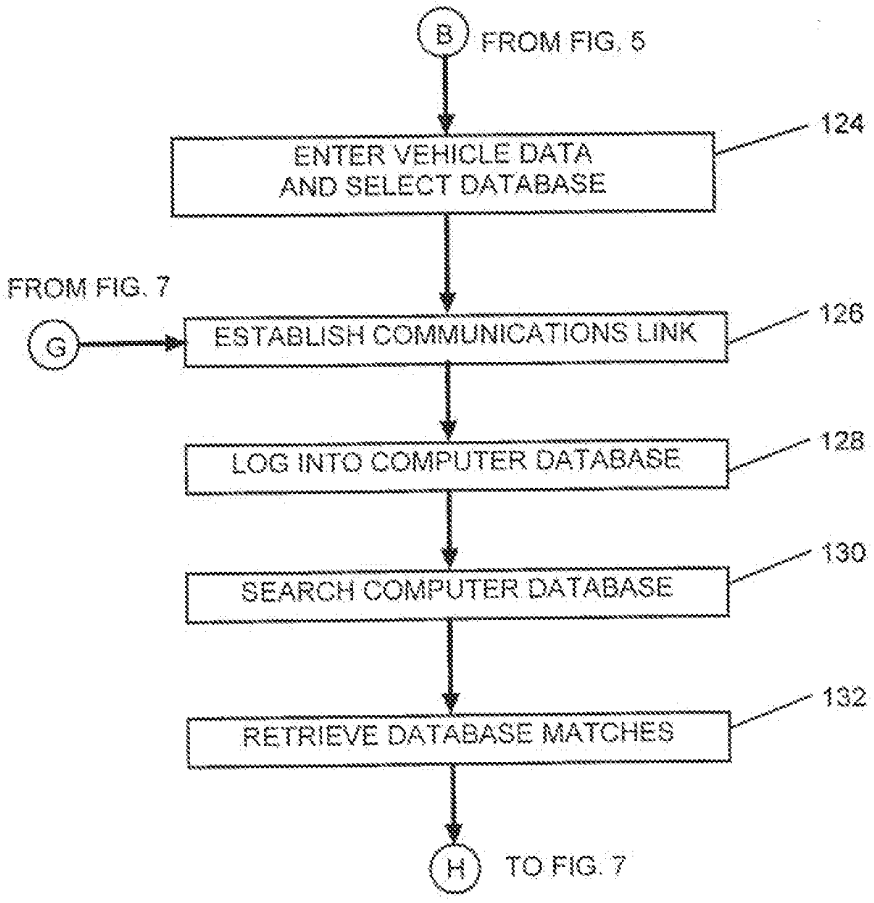

B
FROM FIG. 5
ENTER VEHICLE DATA AND SELECT DATABASE
124
FROM FIG. 7
G
ESTABLISH COMMUNICATIONS LINK
126
LOG INTO COMPUTER DATABASE
128
SEARCH COMPUTER DATABASE
130
RETRIEVE DATABASE MATCHES
132
H
TO FIG. 7

Figure 8

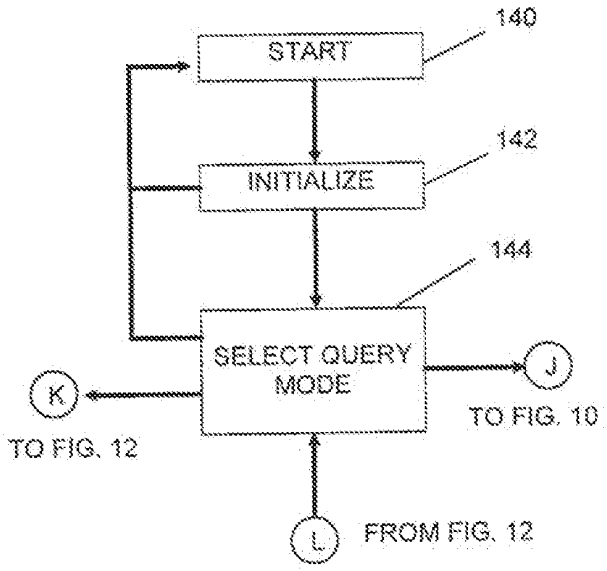

140
START
142
INITIALIZE
144
SELECT QUERY MODE
J
TO FIG. 10
K
TO FIG. 12
L
FROM FIG. 12

Figure 9

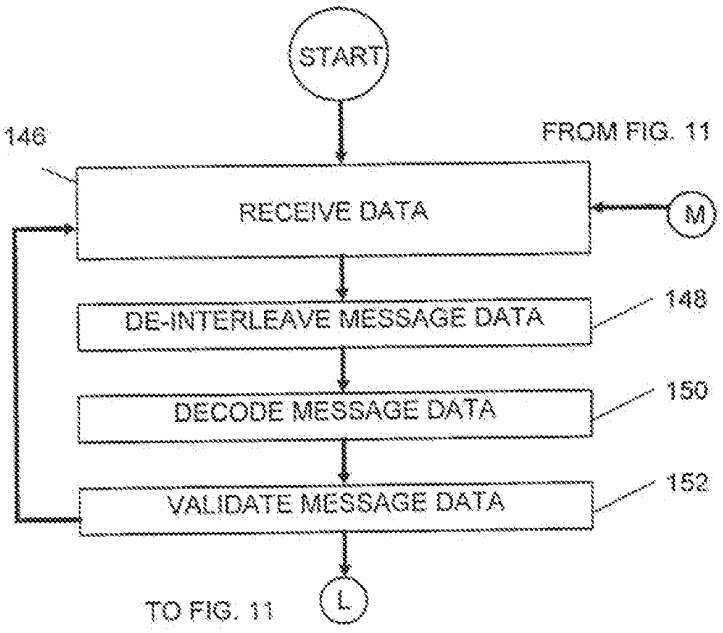

START
146
FROM FIG. 11
RECEIVE DATA
M
DE-INTERLEAVE MESSAGE DATA
148
DECODE MESSAGE DATA
150
VALIDATE MESSAGE DATA
152
TO FIG. 11
L

Figure 10

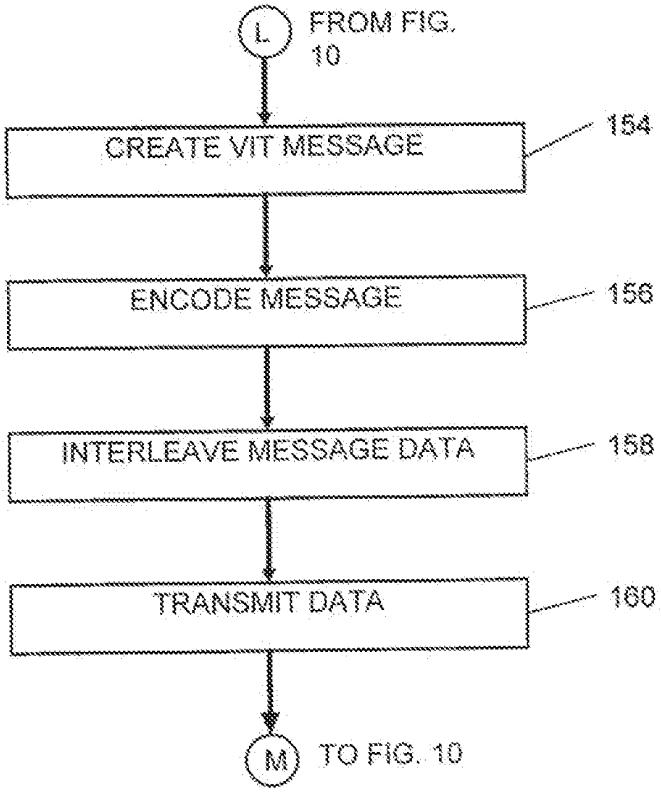

L
FROM FIG. 10
CREATE VIT MESSAGE
154
ENCODE MESSAGE
156
INTERLEAVE MESSAGE DATA
158
TRANSMIT DATA
160
M
TO FIG. 10

Figure 11

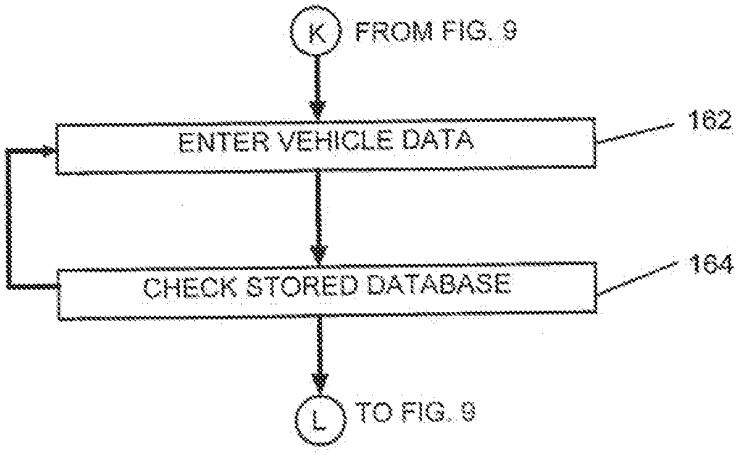

K
FROM FIG. 9
ENTER VEHICLE DATA
162
CHECK STORED DATABASE
164
L
TO FIG. 9

Figure 12

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 993 999 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.04.2000 Bulletin 2000/16

(51) Int Cl.⁷: **B60R 25/04**

(21) Application number: **99305339.6**

(22) Date of filing: **06.07.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **15.10.1998 GB 9822394**

(71) Applicant: **FORD MOTOR COMPANY LIMITED**
Brentwood, Essex CM13 3BW (GB)

(72) Inventor: **Gilmore, Paul Robert**
Billericay, Essex CM11 2LU (GB)

(74) Representative: **Messulam, Alec Moses et al**
A. Messulam & Co.
24 Broadway
Leigh-on-Sea Essex SS9 1BN (GB)

(54) Fuel pump immobilization

(57) The present invention relates to an apparatus and a method for a motor vehicle security system (1) relating to immobilizing and enabling of a fuel pump (18) for a motor vehicle engine. The system (1) comprises data input means (4,6) for receiving driver verification data, an engine control unit (ECU) (2,10) including an ECU processor (12,26) for controlling engine operation, a pump control unit (PCU) (16) including a PCU processor (44) for controlling the fuel pump (18), the PCU (16) being separate from the ECU (2,10) and integrally housed with the fuel pump (18). Communication links (24,40) permit communication between the data input means (4,6) and ECU (2,10), and between the ECU (2,10) and PCU (16). The ECU processor (12,26) is activated to control the PCU (16) when valid driver verification data is received. The PCU processor 49 is then activated to communicate a challenge code to the ECU. The ECU and PCU processors then compute respectively a first and a second response code associated with said challenge code. Finally, the PCU (16) immobilizes the fuel pump (18) until such time as the PCU (16) receives from the ECU (2,10) a first response code which matches the second response code computed by the PCU (16), whereupon the PCU is activated to control the fuel pump (18) in response to the control of the ECU (2,10).

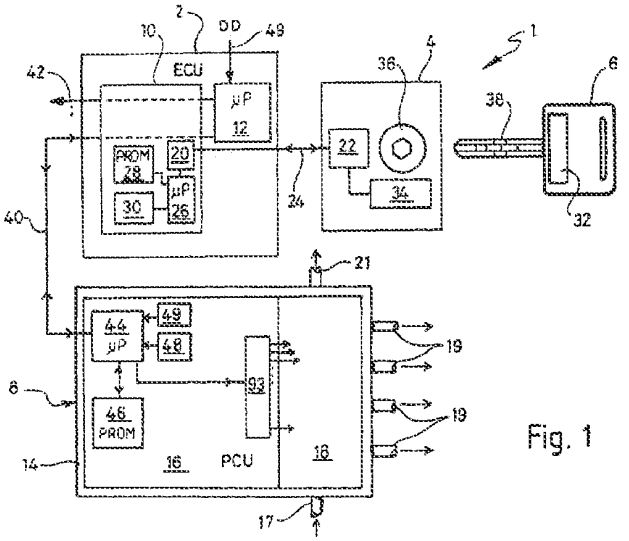


Fig. 1

EP 0 993 999 A2

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to an apparatus and a method for a motor vehicle security system, and in particular a system and method relating to immobilizing and enabling of a fuel pump for a motor vehicle.

[0002] Motor vehicles such as motor cars are prone to theft. Many different systems have therefore been proposed to make motor vehicles more secure from theft. One popular approach is to use an engine immobilizer, which is a discrete device which cuts electrical power to essential components, such as a fuel pump, an engine control unit (ECU), or spark plugs, if a security device is not deactivated when a person enters the car. Many immobilizers, however, can be bypassed to restore power.

[0003] Another approach is to incorporate the functions of the immobilizer in the ECU, and to incorporate associated electronic circuitry in a fuel pump. The fuel pump circuitry has to receive a data signal from the ECU in order to activate the fuel pump to respond to control signals from the ECU. In this way, even if the ECU is bypassed to provide power to the fuel pump, the fuel pump will not work unless it has already received a valid activation code from the engine control unit. This improves security against vehicle theft, but unfortunately, if a thief knows the correct activation code for the fuel pump, the data line from the ECU to the pump can be bypassed, and a valid activation code supplied directly to the fuel pump. It is therefore possible for a thief to defeat such a vehicle security system.

[0004] It is an object of the present invention to provide a more secure motor vehicle security system.

[0005] Accordingly, the invention provides a motor vehicle engine immobilization system comprising data input means for receiving driver verification data, an engine control unit including a first processor means for controlling engine operation, a fuel pump for delivering fuel to the engine, a pump control unit including a second processor means for controlling the fuel pump, the pump control unit being separate from the engine control unit and integrally housed with the fuel pump, means by which the data input means may communicate with the engine control unit, and means by which the engine control unit may communicate with the pump control unit, characterised in that:

a) the first processor means is activated to control the engine including the pump control unit when valid driver verification data is communicated from the data input means to the engine control unit;

b) the second processor means is activated to communicate a challenge code to the engine control unit when the engine control unit has received valid driver verification data;

c) the first and second processor means are adapted to compute respectively a first and a second response code associated with said challenge code; and

d) the pump control unit immobilizes the fuel pump until such time as the pump control unit receives from the engine control unit a first response code which matches the second response code computed by the pump control unit, whereupon the pump control unit is activated to control the fuel pump in response to the control of the engine control unit.

[0006] Also according to the invention, there is provided a method of enabling a fuel pump for delivering fuel to an engine in a motor vehicle, the vehicle comprising data input means for receiving driver verification data, an engine control unit including a first processor means for controlling engine operation, a pump control unit including a second processor means for controlling the fuel pump, the pump control unit being separate from the engine control unit and integrally housed with the fuel pump, means by which the data input means may communicate with the engine control unit, and means by which the engine control unit may communicate with the pump control unit, characterised in that the method comprises the steps of:

a) entering driver verification data into the data input means;

b) communicating said data from the data input means to the engine control unit;

c) activating the first processor means to control the engine including the pump control unit when the driver verification data is valid;

d) activating the second processor means to communicate a challenge code to the engine control unit when the engine control unit has received valid driver verification data;

e) using the first processor means to compute a first response code associated with said challenge code;

f) using the second processor means to compute a second response code associated with said challenge code;

g) using the pump control unit to activate the fuel pump following receipt by the pump control unit from the engine control unit of the first response code if this matches the second response code computed by the pump control unit; or otherwise

h) using the pump control unit to immobilize the fuel pump.

[0007] The engine management unit has vehicle security functions and is in this sense also a vehicle security controller.

[0008] The engine control unit therefore performs the initial authorization that permits a valid user of the motor vehicle to start the vehicle. In this initial stage, the engine control unit is in the position of a "master", and the pump control unit is in the position of a " slave". If the communication link between the engine control unit and pump control unit were completely secure, then this level of security authorisation would be adequate and quite secure. However, it is possible for a thief to gain access to such communication link, in order to bypass the data input means and the engine control unit. With appropriate electronic devices and knowledge of the communication protocol, it is then possible for a thief to send the right activation signal to the pump control unit in order to start the fuel pump and therefore start the engine and drive the vehicle.

[0009] The invention therefore provides a second stage of security authorization, in which the pump control unit becomes the "master", and the engine control unit becomes the "slave". Unless the pump control unit receives the correct response from the engine control unit, it cannot be activated to run the fuel pump. Because the pump control unit is housed with the fuel pump, it is much more difficult and time consuming for a thief to break into any communication link or control lines between the pump control unit and the fuel pump. For example, in a fuel injection engine the fuel pump (including solenoid valves) and pump control unit may be integrated in a metal housing bolted to a side of the engine block. In other systems, the pump control unit may be inside a fuel tank with a fuel pump.

[0010] It would therefore be necessary for a thief either to disassemble or to replace the pump control unit and fuel pump, and in practice this could take a skilled person at least fifteen minutes to accomplish. However, even this would not in general be sufficient to start the motor vehicle unless the engine control unit were similarly bypassed.

[0011] Optionally, power supply means are provided by which electrical power may be switched on or off to the pump control unit. The first processor means can then control the power supply means to switch on said power when valid driver verification data is communicated from the data input means to the engine control unit. The act of switching on the power to the pump control unit may then automatically cause the second processor means to be activated to communicate the challenge code.

[0012] Alternatively, the engine control unit may communicate an activation code to the pump control unit when valid driver verification data is communicated from the data input means to the engine control unit. The second processor means is then activated upon receipt of this activation code to communicate the challenge code when said activation code is received by the pump control unit.

[0013] Preferably, the engine control unit has first non-volatile memory, and the pump control unit has a second non-volatile memory. The non-volatile memories may, for example, be programmable read-only-memories (PROMs), or flash memories. The challenge code can then contain encrypted data computed by the second processor means according to a challenge code algorithm using a variable random (which term includes psuedo-random) number, and a constant random number stored in the second non-volatile memory. The variable random number may be generated by the pump control unit upon activation of the pump control unit by the engine control unit. The same constant random number is stored in the first non-volatile memory allowing both the first and second processor means to compute respective first and second response codes according to the same response code algorithm, using the challenge code and said stored constant random number. Such algorithms may be effectively hidden in firmware from any thief attempting to reverse engineer the security system.

[0014] In a preferred embodiment of the invention, the constant random number is generated randomly by the second processor means the first time the second processor means is activated to communicate said challenge code to the engine management unit, said challenge code not being communicated until the constant random number is generated and communicated to the first processor means. Normally, this first time will be when the engine is first started after assembly of the vehicle on a production line.

[0015] The invention will now be described in further detail, and by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic drawing of a motor vehicle engine immobilization system according to the invention; and

Figures 2A and 2B are flow charts explaining further the system and the method according to the invention of enabling or immobilizing a fuel pump.

[0016] Referring first to Figure 1, the main components of an engine immobilization system 1 according to the invention are an engine control unit (ECU) 2, a key transceiver module 4, a security ignition key 6 and a fuel pump module 8. The engine control unit 2 includes a vehicle security controller 10, and a microprocessor (μP) 12 that controls overall engine operation. The vehicle security controller 10 is preferably integrally housed with the engine control unit 2, however it would be possible for the two to be physically separate and connected by a suitable communication bus.

[0017] The fuel pump module includes a casing 14 which houses a pump control unit (PCU) 16 and a radial-piston distribution fuel injection pump 18. Fuel is sup-

plied to the fuel pump 18 from a fuel tank (not shown) via a fuel inlet line 17, and has a number of outlet lines 19 by which fuel injectors (not shown) are supplied. Excess fuel is returned to the fuel tank by a fuel return line 21.

[0018] The fuel pump 18, and the hardware of the pump control unit 16 are known and available from Bosch GmbH as respectively part numbers PG05 and VP30.

[0019] Together, the engine control unit 2, transceiver module 4, key 6 and fuel pump module 8 comprise the engine immobilization system 1. Similarly, the key transceiver module 4 and security key 6 comprise a data input means for receiving driver verification data.

[0020] The operation of the engine immobilization system 1 in the absence of the fuel pump module 8 will be described first. The vehicle security controller 10 and the transceiver module 4 each have a communications interface 20,22 between which runs a security system bus 24, for example a two wire bus conforming to the ISO 9141 standard.

[0021] The vehicle security controller interface 20 is connected to a microprocessor (μP) 26 which is itself connected to at least one non-volatile memory 28 such as a PROM, and a data verification unit 30. The data verification unit 30 may consist of discrete chips, or alternatively may be built into or programmed into the functioning of the engine control unit microprocessor 12.

[0022] The ignition key 6 also has a transceiver, referred to herein as a transponder 32. The internal components of the transponder 32 are not illustrated, but comprise a radio-frequency receiving-transmitting antenna, power storage capacitor, and a CMOS ASIC programmed with a security algorithm, all encapsulated within a glass cylinder.

[0023] The transceiver module 4 has a radio-frequency (rf) transmitter-receiver 34 in proximity with a lock mechanism 36. A shaft 38 of the key 6 is inserted into the lock 36 and turned to one of the three standard positions: accessory, run or start. The key 6 may or may not be cut to operate a tumbler mechanism within the lock, but in either case, as soon as the key is turned to or past the run position, the vehicle security controller 10 activates the key transceiver module 4 through the security bus 24.

[0024] The transceiver module's rf transmitter-receiver 34 generates an rf field of 134.2 kHz for about 50 ms, which is received by the transponder 32 to charge the storage capacitor. The energy so received is used to generate a 64 bit security code plus bits containing a cyclic redundancy check (CRC) which is transmitted serially back to the transceiver 34 using frequency modulation at 134.2 kHz and 123.2 kHz.

[0025] The transceiver module 4 transmits the security code serially down the bus to the vehicle security controller 10. The vehicle security microprocessor 26 verifies first that the data is valid using the cyclic redundancy check, and then verifies that the data corresponds with data stored in the controller's non-volatile memory 16. If the data is verified, then the security controller 10 sends a key status signal along a serial communication bus 40 to the pump control module 16 in order to activate or enable the pump control unit. Other essential motor vehicle components, such as an electronic ignition system, may be enabled on other lines 42. The key status signal is just a prompt signal, not a security signal. It is therefore possible for a thief to bypass communication between the engine control unit and send a false key status signal to the pump control unit.

[0026] Each key 6 may produce a unique security code, although in one implementation of the vehicle security system, a master key may be used to program new keys which may have a common or a different security code.

[0027] A vehicle security system as described above is known and has been implemented by the Ford Motor Company as the "passive anti-theft system" (PATS) for vehicle immobilisation. In this known system, the fuel pump becomes enabled once the key status information is communicated. In the system according to the invention, however, the pump control unit 16 continues to immobilize the fuel pump 18.

[0028] Reference is now made also to Figures 2A and 2B in considering in detail the interaction between the pump control unit 16 and the engine control unit 2. As described above, when the ignition key 6 is turned to start the engine, power is automatically supplied 50 to the pump control unit 16. This starts software running in a microprocessor (μP) 44 in the pump control unit 16, which then waits 52 for up to 0.5 seconds for the engine control unit 2 to send the key status signal. If no key status signal is received 54, then the pump control unit checks 56 first to see if the total wait time is 5 seconds or more. On the first pass, the wait time will be less than five seconds 58, in which case the pump control unit requests 60 key status information from the engine control unit 2 and then waits 52 for up to 0.5 seconds longer. If the software running in the pump control unit microprocessor 44 repeats this ten times, then the time elapsed will reach five seconds 59, in which case the pump control unit shuts itself down 61 until the next ignition power up 50.

[0029] When a key status signal is received 62 from the vehicle security controller 10 of the engine control unit 2, the pump control unit 16 checks 64 with a flag in a PROM memory 46 if this is the first time the pump control unit 16 has been powered up. If this is the first time 66, then the pump control unit microprocessor 44 generates 68 a pseudo-random number, referred to herein as a pump control unit identification number (PCU ID) using a well-known computer algorithm. An additional pseudo-random element may be introduced by using signals from an on-board fuel temperature sensor 48 and clock 49 as a random variables in the generation of the random number. Once generated, the microprocessor 44 stores the PCU ID in the pump control unit PROM

46.

[0030] The pump control unit then encrypts the PCU ID number according to an encryption protocol and communicates 70 this to the engine control unit 2. The vehicle security controller 10 then decrypts the PCU ID number according to the same protocol, and then stores 72 this number in the vehicle security controller PROM 28. Then, the vehicle security controller 10 of the engine control unit communicates 74 to the pump control unit 16 that the PCU ID has been validly received. The pump control unit 16 then proceeds to generate a challenge code 78.

[0031] In the case that this is not the first time the pump control unit has been powered up 76, the pump control unit microprocessor 44 skips steps 68, 70, 72 and 74, and proceeds directly to generate the challenge code 78, by computing a psuedo-random number, in a similar manner to that described above.

[0032] The pump control unit microprocessor 44 then encrypts the random number using the PCU ID and a first algorithm to generate a challenge code and then communicates 80 this challenge code to the vehicle security controller 10 of the engine control unit 2. The vehicle security controller 10 recalls from the PROM 28 the same PCU ID and then decrypts the challenge code 82 according to the same first algorithm to regenerate the original random number. This same random number is then encrypted using a second algorithm to generate a first response code 83.

[0033] The vehicle security controller 10 then encrypts the first response code using the PCU ID and communicates 84 this to the pump control unit. The pump control unit microprocessor 44 then decrypts using the PCU ID the first response code, and also uses the same second algorithm to generate 86 a second response code corresponding to the challenge code. The pump control unit microprocessor 44 compares 88 the first and second response codes, and if these agree 90, the pump control unit 16 communicates to the vehicle security controller 10 of the engine control unit 2 a code saying that the pump control unit 16 is now enabled 92. The pump control unit 16 is then activated 94 to control the fuel pump 18 via a pump driver interface 93 in response to commands received from the engine control unit 2, for example, in response to a driver demand signal 49.

[0034] If the first and second response codes do not agree 96, then the pump control unit 16 communicates to the vehicle security controller 10 of the engine control unit 2 a code saying that the pump control unit 16 is now disabled 98. The pump control unit 16 is then disables fuelling 100 in order to immobilize the vehicle.

[0035] Because both the engine control unit 2 and pump control unit 16 store the PCU ID, if it ever becomes necessary to replace the pump control unit or engine control unit, it is also necessary to reprogram a new PCU ID. Although not illustrated, this can be done by a motor vehicle service centre or dealer using appropriate diagnostic equipment according to a procedure that includes an access time delay sufficiently long that the delay would be a deterrent to any thief attempting unauthorised reprogramming. One example of a suitable procedure is as follows.

[0036] First the dealer would install a new pump control unit (or engine control unit) and plug the diagnostic equipment into a diagnostics port in the engine control unit. A diagnostic transmission would then be sent to the engine control unit to start a security access timer, which would then run for at least 10 minutes. After the time has elapsed, the diagnostic equipment would verify that security access has been granted by the engine control unit, which would then put the pump control unit in an "as new" state, for example, by setting a flag in an alterable non-volatile memory, such as an E^2PROM. The next time the engine was powered up, software running in the pump control unit would perform the initialization sequence for the PCU ID as set out in steps 68, 70, 72 and 74 of Figure 2A.

[0037] A particular advantage of the above-described invention is that it allows the designer of a motor vehicle security system to build upon existing motor vehicle security access systems having data input means for receiving driver verification data, such as the above-mentioned PATS system. The invention also makes it possible to use existing hardware, such as known pump control units, that can then be modified with appropriate software and/or firmware.

[0038] Those skilled in the art will recognise that there are other ways to implement the communications between the data input means, the engine management system, vehicle security controller and pump control unit. In particular, the term "engine control unit" as used herein includes the case where the vehicle security controller is physically separate from other engine management hardware.

Claims

1. A motor vehicle engine immobilization system (1) comprising data input means (4,6) for receiving driver verification data, an engine control unit (2,10) including a first processor means (12,26) for controlling engine operation, a fuel pump (18) for delivering fuel to the engine, a pump control unit (16) including a second processor means (44) for controlling the fuel pump (18), the pump control unit (16) being separate from the engine control unit (2,10) and integrally housed with the fuel pump (18), means (24,32,34) by which the data input means (4,6) may communicate with the engine control unit (2,10), and means (40) by which the engine control unit (2,10) may communicate with the pump control unit (16), characterised in that

a) the first processor means (12,26) is activated

(50) to control the engine including the pump control unit (16) when valid driver verification data is communicated from the data input means (4,6) to the engine control unit (2,10);

b) the second processor means (44) is activated (80) to communicate a challenge code to the engine control unit (2,10) when the engine control unit (2,10) has received valid driver verification data;

c) the first and second processor means (12,26,44) are adapted to compute respectively a first and a second response code (83,86) associated with said challenge code; and

d) the pump control unit (16) immobilizes (100) the fuel pump (18) until such time as the pump control unit (16) receives from the engine control unit (2,10) a first response code which matches (90) the second response code computed by the pump control unit (16), whereupon the pump control unit (16) is activated (94) to control the fuel pump (18) in response to the control of the engine control unit (2,10).

2. A motor vehicle engine immobilization system (1) as claimed in Claim 1, including power supply means by which electrical power may be switched on or off to the pump control unit (16), in which the first processor means (12,26) controls the power supply means to switch on said power when valid driver verification data is communicated (24) from the data input means (4,6) to the engine control unit (2,10), the second processor means (44) being activated (80) to communicate the challenge code when said electrical power to the pump control unit (16) is switched on.

3. A motor vehicle engine immobilization system (1) as claimed in Claim 1, in which the engine control unit (2,10) communicates (74) an activation code to the pump control unit (16) when valid driver verification data is communicated from the data input means to the engine control unit (2,10), the second processor means (44) then being activated (80) to communicate the challenge code when said activation code is received by the pump control unit (16).

4. A motor vehicle engine immobilization system (1) as claimed in any preceding claim, including in the engine control unit (2,10) a first non-volatile memory (28), and in the pump control unit (16) a second non-volatile memory (46), in which the challenge code contains encrypted data computed (80) by the second processor means (44) according to a challenge code algorithm using a variable random number generated by the pump control unit (16) upon activation of the pump control unit (16) by the engine control unit (2,10) and a constant random number stored in the second non-volatile memory (46), the same constant random number being stored in the first non-volatile memory (28).

5. A motor vehicle engine immobilization system (1) as claimed in Claim 4, in which the first and second processor means (2,10,44) each compute the respective response codes according to a response code algorithm using the challenge code and said constant random number.

6. A motor vehicle engine immobilization system (1) as claimed in Claim 4 or Claim 5, in which the constant random number is generated (68) randomly by the second processor means (44) the first time the second processor means (44) is activated to communicate said challenge code to the engine control unit (4,6), said challenge code not being communicated (80) until the constant random number is generated and communicated (70) to the first processor means (12,26).

7. A method of enabling a fuel pump (18) for delivering fuel to an engine in a motor vehicle, the vehicle comprising data input means (4,6) for receiving driver verification data, an engine control unit (2,10) including a first processor means (12,26) for controlling engine operation, a pump control unit (16) including a second processor means (44) for controlling the fuel pump (18), the pump control unit (16) being separate from the engine control unit (2,10) and integrally housed with the fuel pump (18), means (24,32,34) by which the data input means (4,6) may communicate with the engine control unit (2,10), and means (40) by which the engine control unit (2,10) may communicate with the pump control unit (16), characterised in that the method comprises the steps of:

a) entering (32,34) driver verification data into the data input means (4,6);

b) communicating (24) said data from the data input means (4,6) to the engine control unit (2,10);

c) activating (50) the first processor means (12,26) to control the engine including the pump control unit (16) when the driver verification data is valid;

d) activating (80) the second processor means (44) to communicate a challenge code to the engine control unit (2,10) when the engine control unit (2,10) has received valid driver verification data;

e) using (83) the first processor means (12,26) to compute a first response code associated with said challenge code;

f) using (86) the second processor means (44) to compute a second response code associated with said challenge code;

g) using (94) the pump control unit (16) to activate the fuel pump (18) following receipt by the pump control unit (16) from the engine control unit (2,10) of the first response code if this matches (90) the second response code computed by the pump control unit (16); or otherwise

h) using (100) the pump control unit (16) to immobilize the fuel pump (18).

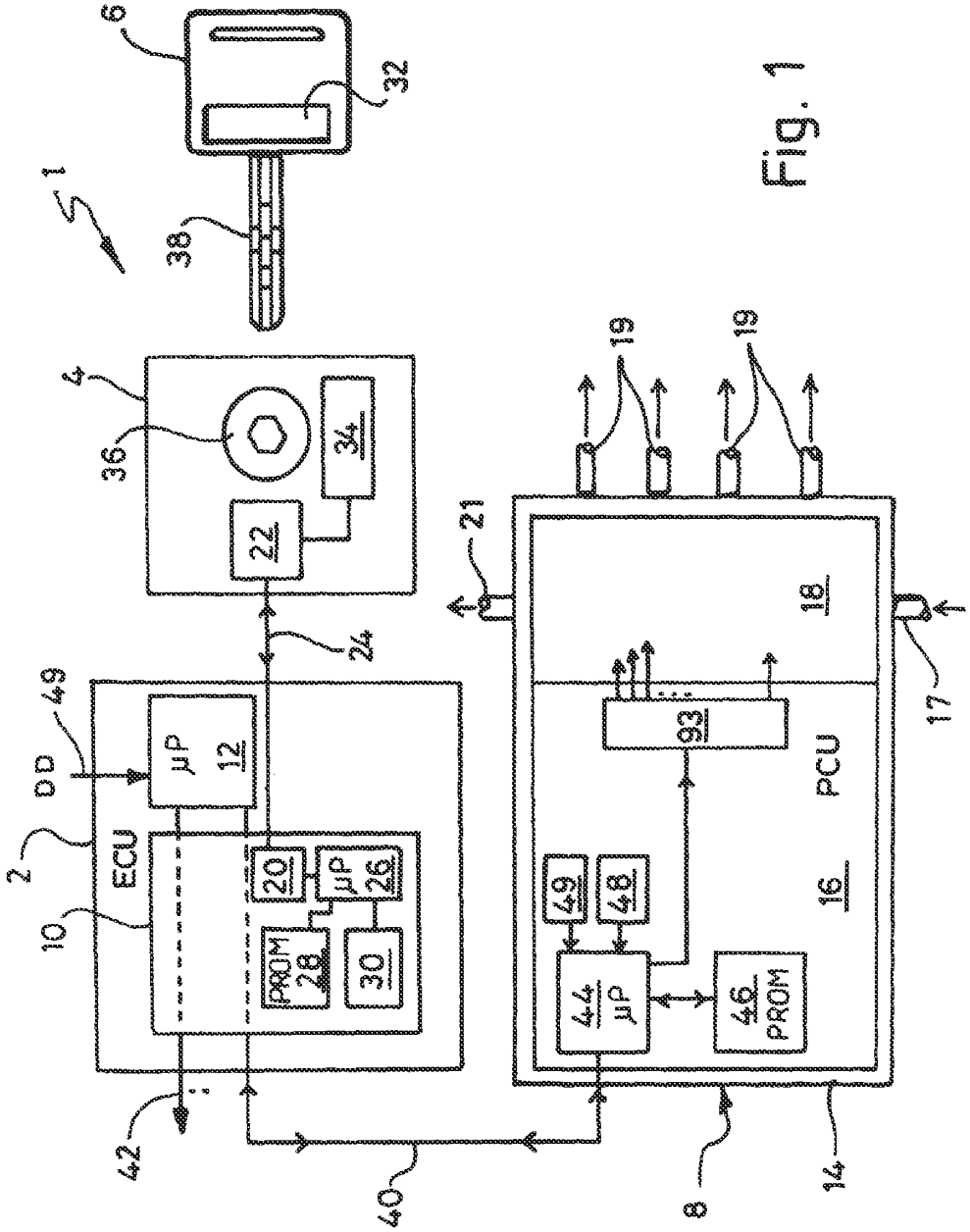

6
32
1
38
4
36
34
22
24
19
19
21
18
17
49
DD
µP
12
2
ECU
10
20
µP
26
PROM
28
30
93
PCU
16
49
48
44
µP
46
PROM
42
40
8
14

Fig. 1

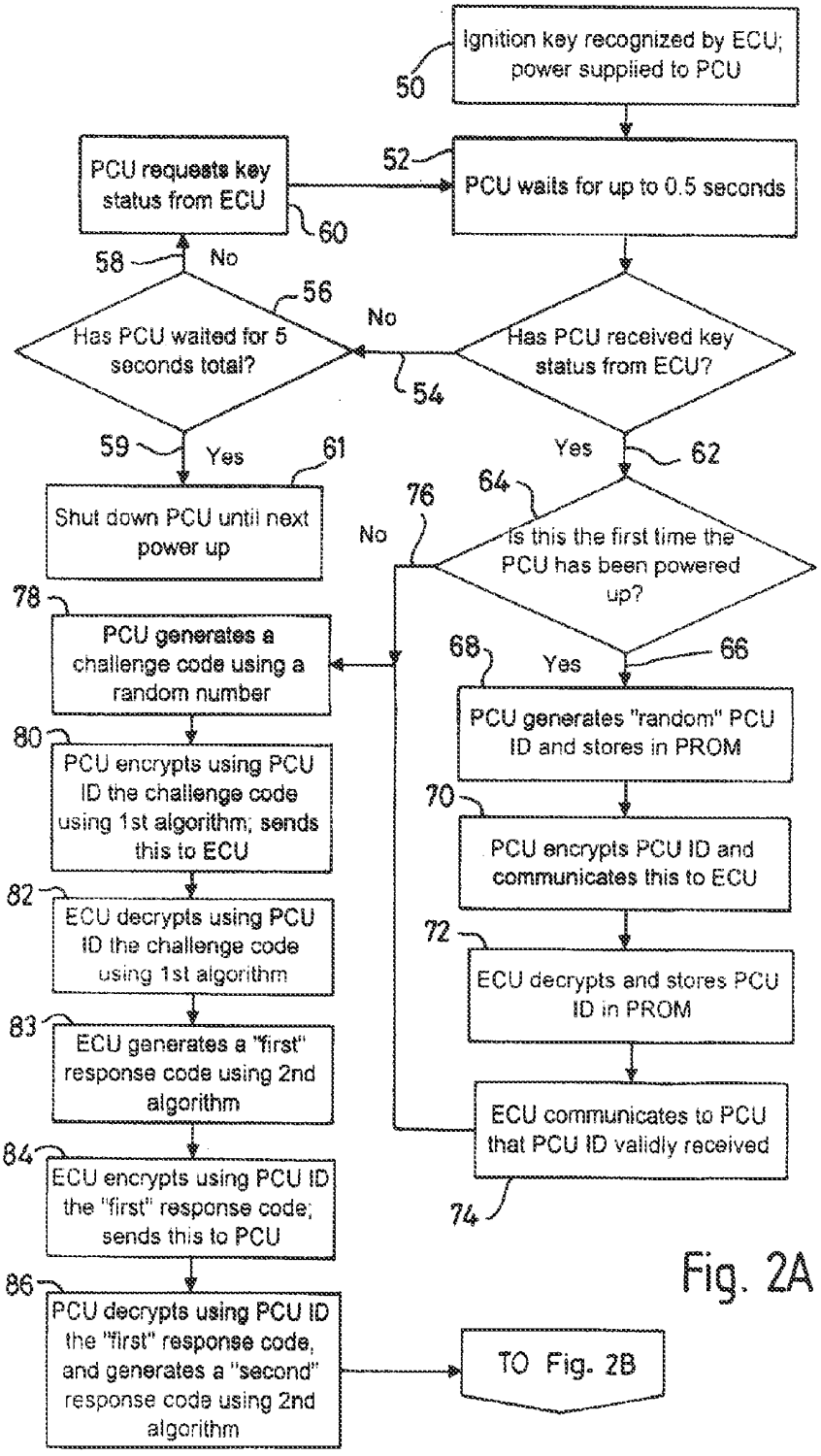

Ignition key recognized by ECU; power supplied to PCU
50
PCU requests key status from ECU
60
52
PCU waits for up to 0.5 seconds
58
No
56
Has PCU waited for 5 seconds total?
No
54
Has PCU received key status from ECU?
59
Yes
61
Yes
62
Shut down PCU until next power up
64
76
No
Is this the first time the PCU has been powered up?
78
PCU generates a challenge code using a random number
68
Yes
66
PCU generates "random" PCU ID and stores in PROM
80
PCU encrypts using PCU ID the challenge code using 1st algorithm; sends this to ECU
70
PCU encrypts PCU ID and communicates this to ECU
82
ECU decrypts using PCU ID the challenge code using 1st algorithm
72
ECU decrypts and stores PCU ID in PROM
83
ECU generates a "first" response code using 2nd algorithm
ECU communicates to PCU that PCU ID validly received
84
ECU encrypts using PCU ID the "first" response code; sends this to PCU
74
86
PCU decrypts using PCU ID the "first" response code, and generates a "second" response code using 2nd algorithm
TO Fig. 2B

Fig. 2A

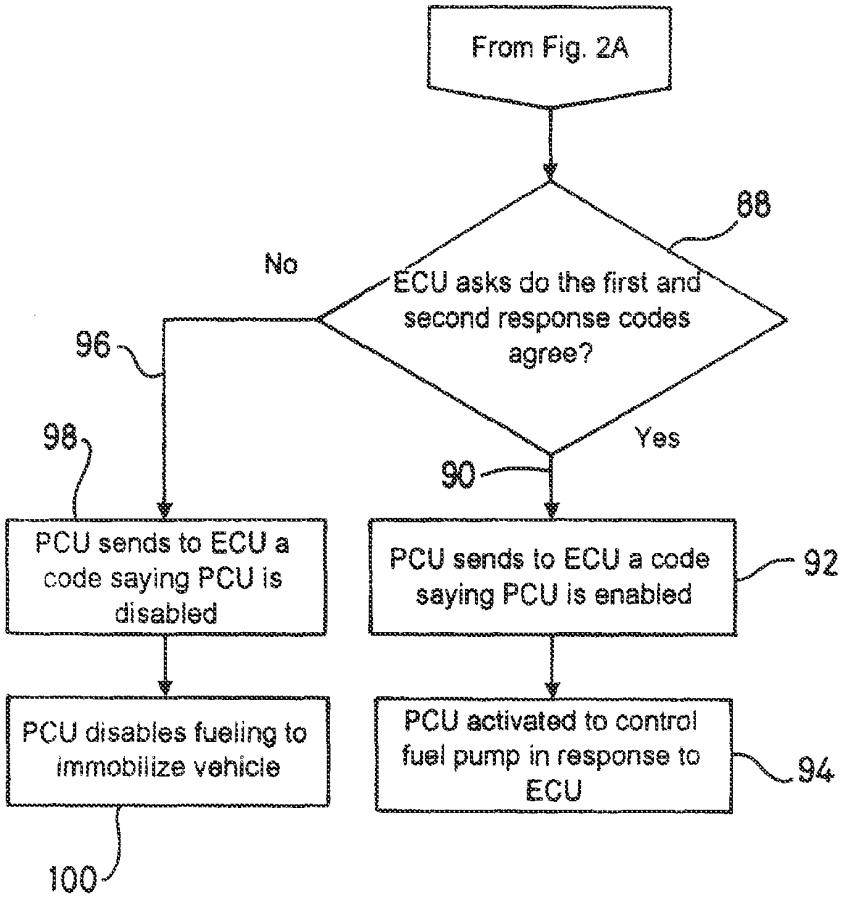

From Fig. 2A
88
ECU asks do the first and second response codes agree?
No
Yes
96
98
90
PCU sends to ECU a code saying PCU is disabled
PCU sends to ECU a code saying PCU is enabled
92
PCU disables fueling to immobilize vehicle
PCU activated to control fuel pump in response to ECU
94
100

Fig. 2B

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 977 145 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.02.2000 Bulletin 2000/05

(51) Int.Cl.⁷: G06K 19/077

(21) Application number: 99114603.3

(22) Date of filing: 26.07.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 28.07.1998 JP 21296398
30.11.1998 JP 33693498
24.02.1999 JP 4639299

(71) Applicant: KABUSHIKI KAISHA TOSHIBA
Kawasaki-shi, Kanagawa-ken 210-8572 (JP)

(72) Inventors:
- Karasawa, Jun, c/o Kabushiki Kaisha Toshiba
  Tokyo 105-8001 (JP)
- Segawa, Masao, c/o Kabushiki Kaisha Toshiba
  Tokyo 105-8001 (JP)
- Saito, Yasuhito c/o Kabushiki Kaisha Toshiba
  Tokyo 105-8001 (JP)

(74) Representative: Henkel, Feiler, Hänzel
Möhlstrasse 37
81675 München (DE)

(54) Radio IC card

(57) A first antenna coil (22) is formed on a surface of an IC chip (23). A second coil (31) and a third coil (32) are formed on a module board (30). The IC chip (23) is mounted on the module board (30) such that the first antenna coil (22) of the IC chip (23) is opposed to the second antenna coil (21).

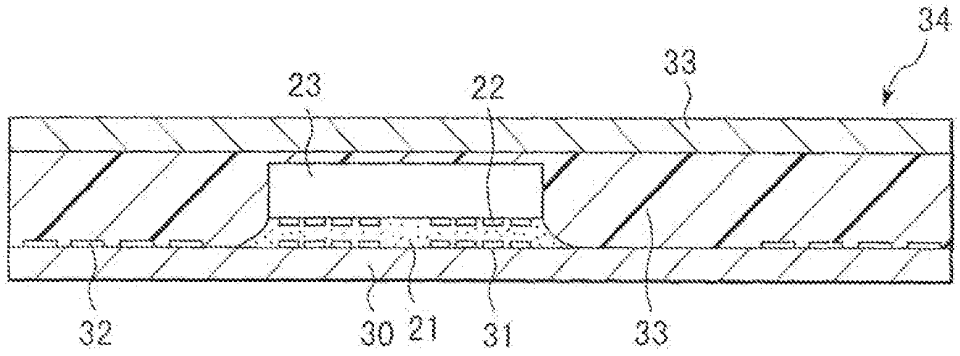


FIG. 14

EP 0 977 145 A2

Description

[0001] The present invention relates to an improvement of a radio IC card wherein an IC (integrated circuit) is buried in a plastic card, etc., a method of manufacturing the radio IC card, a data read/write apparatus for the radio IC card, a radio tag and a method of manufacturing the radio tag.

[0002] There are known non-contact type data carrier modules such as a radio IC card and a radio tag. The data carrier module comprises an IC chip functioning as a semiconductor device and a wound antenna (hereinafter referred to as "antenna coil"). There are various types of data carrier modules having different structures. Depending on the type of the structure, the data carrier module may include a capacitor for synchronization or a capacitor for power supply.

[0003] The antenna coil functions both for data communication and for power supply from the outside. There are various types of antenna coils, for example, a winding coil, a coil formed on a board by means of etching, and a coil formed on a board by means of printed wiring. The number of turns of the antenna coil varies in accordance with the communication frequency, communication distance, etc.

[0004] With recent development in the reduction in size, data carrier modules have widely been used and there is a demand for techniques for mass-producing them at low cost.

[0005] Under the circumstances, research and development has been made for methods of mass-producing data carrier modules by physically and electrically connecting IC chips and antenna coils. In such methods, for example, semiconductor devices are directly mounted on boards by flip-chip bonding, or semiconductor devices are connected to module boards by wire bonding.

[0006] FIG. 1 shows a perspective view of a conventional radio IC card, and FIG. 2 is a cross-sectional view of the same.

[0007] A rectangular-spiral coil pattern 2 is formed on a wiring board 1. An IC chip 3 used as a semiconductor device is mounted on the wiring board 1. An electrode 4 of the IC chip 3 is electrically connected to an electrode 5 on the wiring board 1 by means of a gold ball bump 6.

[0008] A method of manufacturing the radio IC card will now be described.

[0009] The IC chip 3 is first mounted on the wiring board 1 by means of bonding.

[0010] Then a thermoplastic sheet 7 is provided on both sides of the wiring board 1 by thermal fusion.

[0011] The sheet 7 is formed of, e.g. vinyl chloride or PET (polyethylene terephthalate). The entirety of the wiring board 1 is resin-molded by the thermal fusion of sheet 7.

[0012] The thus formed radio IC card is, for example, about 0.2 to 0.7 mm thick.

[0013] FIG. 3 is an electric circuit diagram of this radio IC card. The IC chip 3 is connected to the coil pattern 2. The IC chip 3 has functions of data control, data storage, etc. The IC chip 3 performs data transmission between itself and the outside and receives power through the coil pattern 2.

[0014] However, in the above method, when the IC chip 3 and coil pattern 2 are physically and electrically connected, the IC chip 3 is mounted on the wiring board 1. This method requires expensive equipment such as a flip-chip bonder or a wire-bonder.

[0015] In the order of the manufacturing steps, the step of mounting the IC chip 3 must precede the others. Thus there are many restrictions on the manufacturing steps, and the manufacturing steps are complicated.

[0016] In addition, in the case of the resin-molding, a process management, for example, for considering heat-resistance, is needed and the reliability lowers.

[0017] FIG. 4 is a structure of another radio IC card.

[0018] An IC chip 2 and a communication antenna 9 connected to the IC chip 2 are mounted on a card body 8, and a button cell 10 is built in.

[0019] FIG. 5 is a structure of another radio IC card and FIG. 6 is a cross-sectional view of the IC card.

[0020] An IC chip 2, a communication antenna 9 connected to the IC chip 2, and a power supply coil 10 are mounted on the card body 8.

[0021] In order to ensure security and reliability, the radio IC card is formed in a shape which does not permit easy dissembling, for example, by mold-sealing or thermal-pressing.

[0022] In the case of the radio IC card including the cell, however, the life of the radio IC card is limited by the life of the cell and this is very economically disadvantageous.

[0023] There is also known an electromagnetic-induction-type radio IC card to which power is supplied from a radio IC card reader in the form of electromagnetic waves. In the case of this IC card, the reader needs to constantly send signals. This is not preferable from the standpoint of energy saving.

[0024] For example, in a gate entrance/exit system, incoming/outgoing persons with radio IC cards pass through the gate. The time of entrance/exit of persons is irregular.

[0025] Consequently, the frequency of communication of data read from the radio IC card by the card reader becomes irregular, and the time of wait until the beginning of data communication increases.

[0026] Even if the frequency of data communication is irregular, the card reader is required to constantly send signals

and to always wait for data from the radio IC card.

[0027] An object of the present invention is to provide a radio IC card and a method of manufacturing the same, wherein a semiconductor element is electrically connected to an antenna coil and the radio IC card can be obtained at low cost without the need to use an expensive mounting apparatus.

[0028] Another object of the invention is to provide a radio IC card and a method of manufacturing the same, as well as a data read/write apparatus, wherein energy saving can be achieved irrespective of the life of a cell.

[0029] Still another object of the invention is to provide a radio tag and a method of manufacturing the same, wherein a semiconductor element is electrically connected to an antenna coil and the radio tag can be obtained at low cost without the need to use an expensive mounting apparatus.

[0030] Still another object of the invention is to provide a radio tag and a method of manufacturing the same, wherein energy saving can be achieved irrespective of the life of a cell.

[0031] According to an aspect of the present invention, there is provided a radio IC card comprising: a board having at least two rectangular-spiral antennas formed thereon; and a semiconductor element having a rectangular-spiral antenna formed on a surface thereof, the semiconductor element being mounted on the board such that the antenna on the semiconductor element is situated opposed to one of the at least two antennas on the board.

[0032] In this radio IC card, the antenna on the semiconductor element is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0033] The antenna on the semiconductor element is formed of a metallic film.

[0034] A layer of the antenna formed of the metallic film and a layer of an insulating film are laminated on the surface of the semiconductor element.

[0035] The antenna is provided on each of upper and lower surfaces of the semiconductor element.

[0036] The semiconductor element is provided with a layer for formation of an electric element.

[0037] One of the antennas formed on the board has substantially the same shape as the antenna formed on the semiconductor element, and the other of the antennas on the board is greater in size than the one of the antennas on the board.

[0038] One of the antennas on the board and the other of the antennas on the board are electrically connected.

[0039] One of the antennas on the board and the antenna on the semiconductor device are electromagnetically connected.

[0040] The antenna is formed over the semiconductor element, with an insulating film interposed.

[0041] The antenna is formed over the semiconductor element, with a magnetic film interposed.

[0042] An insulating film is formed on each of the antennas on the board.

[0043] An insulating film, in which magnetic particles are dispersed, is formed on each of the antennas on the board.

[0044] The semiconductor element and the substrate are integrally sealed with resin.

[0045] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: forming a rectangular-spiral antenna on a surface of a semiconductor element; forming at least two rectangular-spiral antennas on a board; and disposing the antenna formed on the semiconductor element such that the antenna formed on the semiconductor element is opposed to one of the antennas formed on the board.

[0046] In this method, the antenna on the surface of the semiconductor element is formed by a thin-film patterning process.

[0047] The antenna on the surface of the semiconductor element is formed by a printing process.

[0048] The antenna on the surface of the semiconductor element is formed such that a plurality of electrode pads are provided on the surface of the semiconductor element and the electrode pads are connected by means of wire bonding.

[0049] The at least two antennas on the board are integrally formed.

[0050] The method includes a step of integrally sealing the semiconductor element and the board with resin.

[0051] According to another aspect of the invention, there is provided a radio IC card having at least one rectangular-spiral antenna and one semiconductor element mounted thereon, wherein a cavity portion is provided near the antenna and a permanent magnet is movably provided within the cavity portion.

[0052] The permanent magnet is movable in a direction of a central axis of the antenna.

[0053] The permanent magnet is rotatably provided within the cavity portion.

[0054] The antenna serves both for power supply to the semiconductor element and for data communication.

[0055] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: mounting at least one semiconductor element and one rectangular-spiral antenna on a first casing body in which a recess portion is formed in advance; inserting a permanent magnet movably in the recess portion; and attaching a second casing body to the first casing body provided with the at least one semiconductor element and one antenna and the permanent magnet.

[0056] According to another aspect of the invention, there is provided a data reader/writer apparatus comprising: a

radio IC card on which at least one rectangular-spiral antenna and a semiconductor element are mounted; and read/write means for performing data communication with the semiconductor element mounted on the radio IC card, the read/write means having a permanent magnet for inducing an electromotive force in the antenna mounted on the radio IC card by crossing a magnetic field over the antenna.

[0057] According to another aspect of the invention, there is provided a radio IC card having at least one data communication antenna and one semiconductor element mounted thereon, the radio IC card comprising a piezoelectric element connected to the semiconductor element.

[0058] The piezoelectric element is used as a board, and the at least one antenna and one semiconductor element are mounted on the piezoelectric element.

[0059] Electrodes are provided on both sides of the piezoelectric element, and these electrodes are electrically connected to at least the semiconductor element.

[0060] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: attaching at least one data communication antenna and one semiconductor element to a first casing body; attaching a piezoelectric element to the first casing body; and adhering a second casing body to the first casing body.

[0061] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: attaching at least one data communication antenna and one semiconductor element on a board formed of a piezoelectric element; and applying an outer coating to the board on which the antenna and the semiconductor element are attached.

[0062] According to another aspect of the invention, there is provided a data read/write apparatus comprising: a radio IC card having at least one data communication antenna and one semiconductor element mounted thereon and including a piezoelectric element connected to the semiconductor element; and read/write means for performing data communication with the semiconductor element by means of the antenna, the read/write means including a pressing mechanism for pressing the piezoelectric element of the radio IC card, thereby producing an electric charge in the piezoelectric element.

[0063] According to another aspect of the invention, there is provided a radio IC card comprising: a semiconductor element having a rectangular-spiral antenna formed on a surface thereof; a board having at least three rectangular-spiral antennas formed thereon such that one of the at least three antennas is situated, opposed to the antenna of the semiconductor element; a cavity portion provided near one of the other antennas on the board; and a permanent magnet provided movably in the cavity portion.

[0064] In this radio IC card, on the board there are provided: an antenna situated to be opposed to the antenna on the semiconductor element; a communication antenna electrically connected to the antenna; and a power supply antenna electrically connected to the communication antenna, a magnetic flux of the permanent magnet being crossed over the power supply antenna.

[0065] The antennas are sealed with an insulating material in which magnetic particles are dispersed.

[0066] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: mounting at least one semiconductor element and at least three rectangular-spiral antennas on a first casing body in which a recess portion is formed in advance; inserting a permanent magnet movably in the recess portion; and attaching a second casing body to the first casing body.

[0067] In this method, the method includes the steps of: storing the permanent magnet movably in a case; and mounting the case in the recess portion.

[0068] The first and second casing bodies are formed of an insulating material in which magnetic particles are dispersed.

[0069] According to another aspect of the invention, there is provided a radio tag, wherein a rectangular-spiral antenna is formed on a surface of a semiconductor element.

[0070] In this radio tag, the antenna on the semiconductor element is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0071] The antenna on the semiconductor element is formed of a metallic film.

[0072] A layer of the antenna formed of the metallic film and a layer of an insulating film are laminated on the surface of the semiconductor element.

[0073] The antenna is provided on each of upper and lower surfaces of the semiconductor element.

[0074] The semiconductor element is provided with a layer for formation of an electric element.

[0075] The antenna is provided over the semiconductor element, with an insulating film interposed.

[0076] The antenna is formed over the semiconductor element, with a magnetic film interposed.

[0077] The antenna is formed on the semiconductor element, with an insulating film containing dispersed magnetic particles interposed.

[0078] The semiconductor element having the antenna formed on the surface thereof is sealed with resin.

[0079] According to another aspect of the invention, there is provided a method of manufacturing a radio tag, the

method comprising the steps of: forming an insulating film over a surface of a semiconductor wafer on which a plurality of semiconductor elements are formed; forming rectangular-spiral antennas on the insulating film at positions corresponding to the semiconductor elements; and dicing the semiconductor elements out of the semiconductor wafer.

[0080] In this method, the antenna formed on the surface of each of the semiconductor elements is formed by a thin-film patterning process.

[0081] The antenna formed on the surface of each of the semiconductor elements is formed by a printing process.

[0082] The antenna on each of the semiconductor elements is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0083] Each of the semiconductor elements, on the surface of which the antenna is formed, is sealed with resin.

[0084] According to the above radio IC card and the method of manufacturing the same, as well as the data read/write apparatus and the radio tag and the method of manufacturing the same, the semiconductor element and antenna coil are connected electrically, and not physically. Without using expensive mounting apparatuses, these can be manufactured cost-effectively. Furthermore, energy saving can be achieved irrespective of the life of the cell.

[0085] This summary of the invention does not necessarily describe all necessary features so that the invention may also be a sub-combination of these described features.

[0086] The invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a perspective view of a conventional radio IC card;
FIG. 2 is a cross-sectional view of the conventional radio IC card;
FIG. 3 is an electric circuit diagram of the conventional IC card;
FIG. 4 schematically shows the structure of another conventional IC card;
FIG. 5 schematically shows the structure of another conventional IC card;
FIG. 6 is a cross-sectional view of the radio IC card shown in FIG. 5;
FIG. 7A shows a step of manufacturing a radio tag according to a first embodiment of the present invention;
FIG. 7B shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 7C shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 7D shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 8A illustrates a process of manufacturing another example of the radio tag according to the first embodiment;
FIG. 8B is a cross-sectional view of the radio tag in FIG. 8A;
FIG. 8C is a partial cross-sectional view of the radio tag in FIG. 8B;
FIG. 8D is a cross-sectional view of the manufactured radio tag according to this process;
FIG. 9A shows a process of manufacturing the radio tag using a wire bonding method;
FIG. 9B is a side view of this radio tag;
FIG. 10 shows a modification of the radio tag according to the first embodiment;
FIG. 11 shows a modification of the radio tag according to the first embodiment;
FIG. 12 shows a modification of the radio tag according to the first embodiment;
FIG. 13A shows a step of manufacturing a radio IC card according to a second embodiment of the invention;
FIG. 13B shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13C shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13D shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13E shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 14 is a cross-sectional view of the manufactured IC card;
FIG. 15 is an electric circuit diagram of the radio IC card;
FIG. 16 is a view for describing electromagnetic induction coupling between first and second antenna coils;
FIG. 17A shows a structure of a radio IC card according to a third embodiment of the invention;
FIG. 17B is a cross-sectional view of the radio IC card;
FIG. 18 is an exploded perspective view of the radio IC card;
FIG. 19 is a flow chart of manufacture of the radio IC card;
FIG. 20A is a diagram illustrating the generation of induction electromotive force due to a permanent magnet;
FIG. 20B is a diagram illustrating the generation of induction electromotive force due to the permanent magnet;
FIG. 21A shows a structure of a radio IC card on which a permanent magnet is rotatably mounted;
FIG. 21B is a partial cross-sectional view of the radio IC card shown in FIG. 21A;
FIG. 22A shows a structure of a radio IC card in a data read/write apparatus according to a fourth embodiment of the invention;
FIG. 22B is a cross-sectional view of the radio IC card;
FIG. 23 schematically shows a structure of a reader/writer in the data read/write apparatus;
FIG. 24 is an exploded perspective view of the radio IC card;

FIG. 25 is a view for explaining supply of power from the reader/writer to the radio IC card;
FIG. 26 is a view for explaining the supply of power from the reader/writer to the radio IC card;
FIG. 27 shows a structure of a radio IC card according to a fifth embodiment of the invention;
FIG. 28 shows a structure of a modification of the radio IC card as applied to an automatic wicket;
FIG. 29A shows a structure of a radio IC card according to a sixth embodiment of the invention;
FIG. 29B is a cross-sectional view of the radio IC card;
FIG. 30 is a view for explaining a piezoelectric effect of a piezoelectric element;
FIG. 31 is an electric circuit diagram of the radio IC card;
FIG. 32 is an exploded perspective diagram of the radio IC card;
FIG. 33 is a flow chart of manufacture of the radio IC card;
FIG. 34A shows a structure of a radio IC card according to a seventh embodiment of the invention;
FIG. 34B is a cross-sectional view of the radio IC card;
FIG. 35 is an exploded perspective view of the radio IC card;
FIG. 36 is a flow chart of manufacture of the radio IC card;
FIG. 37A shows an example of dimensions of the manufactured IC card;
FIG. 37B shows an example of dimensions of the radio IC card;
FIG. 38 shows a structure of a data reader/writer apparatus according to an eighth embodiment of the invention;
FIG. 39 is a view for describing power supply to the radio IC card in the apparatus;
FIG. 40A shows a structure of a radio IC card according to a ninth embodiment of the invention;
FIG. 40B is a cross-sectional view of the radio IC card;
FIG. 41A shows a manufacturing step of the radio IC card;
FIG. 41B shows a manufacturing step of the radio IC card;
FIG. 41C shows a manufacturing step of the radio IC card;
FIG. 41D shows a manufacturing step of the radio IC card;
FIG. 42 is a cross-sectional view of an IC chip portion in the radio IC card;
FIG. 43 is an exploded perspective view of the radio IC card; and
FIG. 44 is a flow chart of manufacture of the radio IC card.

(First Embodiment)

[0087] A first embodiment of the present invention will now be described with reference to the accompanying drawings.

[0088] FIGS. 7A to 7D illustrate steps of manufacturing a radio tag.

[0089] FIG. 7A shows a semiconductor wafer 20 on which a plurality of ICs are formed.

[0090] An insulating protection film 21 is formed on the surface of the semiconductor wafer 20, as shown in FIG. 7B. The insulating protection film 21 is formed of, e.g. P-SiN (PSG: Phosphosilicate Glass). The thickness of the insulating protection film 21 is in a range from 0.75 μm to 0.4 μm. The insulating protection film 21 may be formed of, for example, a metal oxide such as silicon dioxide, a resin such as polyimide, or air gap.

[0091] As is shown in FIG. 7C, a number of wound antennas (hereinafter referred to as "antenna coils") 22 are formed on the insulating protection film 21. The antenna coils 22 are formed of, e.g. gold-plated wire. Alternatively, the antenna coils 22 may be formed of thin-film patterns of Cu, Al, etc., or by printing conductive paste of Cu, etc.

[0092] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0093] Thus, radio tags provided with antenna coils are manufactured. The size of each radio tag is, for example, 4 mm (length) × 3 mm (width) × 0.3 mm (height).

[0094] The above-described radio tag has a data control function and a memory function which are achieved by the IC chip 23. Data transmission with the outside or power supply from the outside can be effected through the antenna coil 22.

[0095] According to the first embodiment, as described above, the insulating protection film 21 is formed on the surface of the semiconductor wafer 20, and the antenna coil 22 is formed on the insulating protection film 21. The semiconductor wafer 20 is then diced and the radio tags are formed. Thus, the IC chips 23 are electrically connected to the antenna coils 22 without physical connection. There is no need to use expensive apparatuses, such as flip-chip bonders or wire bonders, in order to mount the IC chips.

[0096] There is no need to conduct a process management, for example, for considering heat-resistance in resin-molding, and the reliability is enhanced.

[0097] The antenna coil 22 is formed on the IC chip 23, and the resultant structure is merely mounted. Therefore, the small-sized, inexpensive radio tag can be obtained.

[0098] A description will now be given of another example of the manufacture of the radio tag according to the first embodiment.

[0099] FIGS. 8A to 8D schematically illustrate manufacturing steps of the radio tag. FIG. 8A shows a plan view and a cross-sectional view. FIG. 8B is a cross-sectional view of the radio tag. FIG. 8C is an enlarged view of portion 8C in FIG. 8B, and FIG. 8D is a cross-sectional view of the manufactured radio tag.

[0100] An IC chip 23 applied to this example has a square shape with each side of, e.g. about 10 mm, and a thickness of about 20 μm at a minimum.

[0101] An insulating protection film 21 is formed on the surface of the IC chip 23. The insulating protection film 21 is formed of, e.g. silicon dioxide or a polyimide resin. The thickness of the insulating protection film 21 is about 10 to 100 μm. The insulating protection film 21 may be formed of a magnetic film such as ferrite, instead of silicon dioxide or a polyimide resin.

[0102] Magnetic particles may be dispersed in the insulating protection film 21. With the formation of the magnetic film, an inductance component of the antenna coil 22 which is to be formed subsequently can be increased. The insulating protection film 21 may be an air gap formed by etching silicon dioxide.

[0103] A conductive via-hole 24, which is a through-hole, is formed in the insulating protection film 21, as shown in FIG. 8B.

[0104] A rectangular spiral antenna coil (pattern coil) 22 is formed on the insulating protection film 21. The antenna coil 22 is formed of a conductive film of Al, Cu, Au, etc. The antenna coil 22 is thinly formed, with a pattern width and a pattern interval being in a range of several μm to several-ten μm. The antenna coil 22 may be formed by means of printing of a conductive paste of, e.g. Ag, Cu, etc.

[0105] Subsequently, the IC chip 23 is molded with a mold resin 25, as shown in FIG. 8D. For example, if the mold resin 25 is an epoxy resin, etc., transfer molding is adopted. If the mold resin 25 is PP (polypropylene), PPS (polyphenylsulfone), etc., injection molding is adopted. Thus, a radio tag with an outside shape of about 10 mm × 10 mm and a thickness of about 1 mm.

[0106] FIGS. 9A and 9B are schematic views showing another example of the radio tag which is manufactured by using wire bonding. FIG. 9A is a plan view and a FIG. 9B is a side view.

[0107] As is shown in FIG. 9A, electrodes 26 are formed at four corner portions on the surface of the IC chip 23. Each electrode 26 has a square shape with each side about 30 μm to 100 μm long.

[0108] The electrodes 26 are interconnected by a bonding wire element 27. The bonding of electrodes 26 is performed from the outer peripheral side toward the central side. As a result, a rectangular-helical antenna coil is formed. The bonding wire element 27 has a diameter of, e.g. about 10 μm to 100 μm and is formed of Au, Al or Cu.

[0109] The radio tag is thus manufactured.

[0110] In the process of manufacturing this radio tag, the formation of an insulating protection film is not needed, as shown in FIG. 9B, and the pattern resistance can be reduced sine the bulk-type coil material is used.

[0111] A modification of the manufacture of the radio tag according to the first embodiment will now be described.

[0112] FIG. 10 shows a multi-layer structure in which antenna coils 22 and insulating protection films 21 are formed in two tiers on the surface of the IC chip 23. By virtue of this structure, the number of turns of the antenna coils 22 is increased.

[0113] FIG. 11 shows a structure in which through-holes 28 are formed in the IC chip 23. Antenna coils 22 are formed on upper and lower surfaces of the IC chip 23. The antenna coils 22 are electrically connected through the through-holes 28.

[0114] FIG. 12 shows a radio tag with multi-functions, wherein various electric elements such as a capacitor 29, in addition to antenna coils 22, are provided on the IC chip 23. In the capacitor 29, an induction-type thick-film material of, e.g. titanium dioxide, lead perovskite, etc. is used.

[0115] Needless to say, with the above examples of the radio tag, too, the IC chip 23 and antenna coil 22 are connected electrically, and not physically. Without using expensive mounting apparatuses, the radio tags can be manufactured cost-effectively.

(2) A radio IC card (non-contact data carrier) according to a second embodiment of the invention will now be described with reference to FIGS. 13A to 13E.

[0116] A radio tag, like the first embodiment, is first manufactured.

[0117] An insulating protection film 21 is formed, as shown in FIG. 7B, on the surface of the semiconductor wafer 20 shown in FIG. 7A. The insulating protection film 21 is formed of, e.g. P-SiN (PSG: Phosphosilicate Glass). The thickness of the insulating protection film 21 is in a range from 0.75 μm to 0.4 μm. The insulating protection film 21 may be formed of, for example, a metal oxide such as silicon dioxide, a resin such as polyimide, or air gap.

[0118] As is shown in FIG. 7C, the antenna coil 22 (hereinafter referred to as "first antenna coil 22") is formed on the insulating protection film 21 by gold plating. The first antenna coils 22 may be formed of thin-film patterns of Cu, Al, etc , or by printing conductive paste of Cu, etc.

[0119] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0120] On the other hand, a second antenna coil 31 and a third antenna coil 32 are formed, as shown in FIG. 13B, on a surface of a module board 30 shown in FIG. 13A.

[0121] The second antenna coil 31 has substantially the same shape as the first antenna coil 32 formed on the radio tag.

[0122] Since the third antenna coil 32 is used for communication with the outside of the radio IC card or for power supply from the outside, it has a greater number of turns and a greater shape than the second antenna coil 31.

[0123] The second and third antenna coils 31 and 32 are electrically connected to constitute a closed loop circuit.

[0124] The second and third antenna coils 31 and 32 are simultaneously formed on the surface of the module board 30, for example, by a subtractive method, as in the formation of a regular printed circuit board.

[0125] The second and third antenna coils 31 and 32 may be formed by an additive method. The second and third antenna coils 31 and 32 may be formed by fixing coils of coated wire on the module board 30. Alternatively, the antenna coils may be formed of a combination of printed wire and wire coils.

[0126] Specifically, the second and third antenna coils 31 and 32 are both formed by etching Ag, Al, etc.

[0127] Alternatively, the second and third antenna coils 31 and 32 may both be formed by a printing method using Ag paste, or formed of coils of Cu. Furthermore, the second antenna coil 31 may be formed by printing or etching, while the third antenna coil 32 may be formed of coils.

[0128] In a subsequent step shown in FIG. 13C, an insulating film 33 is formed on the second antenna coil 31. The insulating film 33 is formed of a semi-hardened epoxy resin with a thickness of, e.g. 20 μm. For example, the insulating film 33 is formed by attaching an insulating adhesive film of a semi-hardened epoxy resin. The insulating film 33 may be formed of some other insulative resin such as polyimide or a metal oxide.

[0129] In the next step illustrated in FIG. 13D, the IC chip 23 (see FIG. 7D) is opposed to, and disposed on, the second antenna coil 31 on the module board 30.

[0130] In this case, the IC chip 23 is mounted in a face-down fashion. The mounting is performed under a suitable pressure such that the second antenna coil 31 is opposed to the first antenna coil 22 of the IC chi 23 with the insulating film 33 interposed.

[0131] In addition, the mounting is performed such that the gap between the first antenna coil 22 and second antenna coil 31 is mechanically controlled and the gap is set at about 20 μm or less.

[0132] In the mounting step, in order to completely harden the insulating adhesive film of, e.g. semi-hardened epoxy resin, which forms the insulating film 33, it is heated at about 200°C to 120°C for 10 to 120 seconds and fixed on the module board 30.

[0133] For example, the material of the insulating adhesive film may be applied in a viscous liquid phase. In this case, where the maintenance of the insulating film 33 is difficult under pressure, the height of the film may be controlled. For example, the insulating film 33 may be maintained by using a spacer of a polyester film with a thickness of, e.g. 10 μm, which serves also as the insulating film 33.

[0134] Subsequently, as shown in FIG. 13E, the entire module board 30 with the IC chip 23 is sealed with resin and coated with the polyester film 33. At last, the radio IC card 34 is obtained after printing and punching.

[0135] FIG. 14 is a cross-sectional view of the manufactured radio IC card 34. The method of forming the radio IC card is, for example, injection molding (e.g. insertion molding) using, e.g. a polyester resin, or pressing molding using, e.g. a vinyl chloride sheet.

[0136] FIG. 15 is an electric circuit diagram of the radio IC card 34.

[0137] Since the first antenna coil 22 of the IC chip 23 is disposed to be opposed to the second antenna coil 31 of the module board 30, electromagnetic induction coupling is effected between the first antenna coil 22 and second antenna coil 31.

[0138] Accordingly, if the third antenna coil 32 receives electric waves from the outside, an electromotive force occurs in the third antenna coil 32. The electromotive force is supplied to the second antenna coil 31 connected to the third antenna coil 32.

[0139] At the time current begins to flow in the second antenna coil 31, an electric field is generated at the second antenna coil 31.

[0140] This electric field acts on the first antenna coil 22 located near and opposed to the second antenna coil 31, and an electromotive force is induced in the first antenna coil 22.

[0141] This electromotive force is supplied to the IC circuit 35. In this manner, external electric waves are converted to power to be supplied to the IC circuit 35, through the third, second and first antenna coils 32, 31 and 22.

[0142] On the other hand, if current is output from the IC circuit 35, the current is supplied to the first antenna coil 22. At the time the current begins to flow through the first antenna coil 22, an electric field is generated at the first antenna coil 22.

[0143] This electric field acts on the second antenna coil 31 located near and opposed to the first antenna coil 22, and an electromotive force is induced in the second antenna coil 31.

[0144] The induced electromotive force is supplied to the third antenna coil 32. This causes electric waves to be radiated from the third antenna coil 32.

[0145] The electromagnetic induction coupling between the first antenna coil 32 and second antenna coil 31 will now

be described with reference to FIG. 16.

[0146] Assume that there are two single-turn coils having loop planes parallel to an xz-plane, i.e. those corresponding to the first antenna coil 22 and second antenna coil 31. A distance between the first and second antenna coils 22 and 31 is d.

[0147] An intensity H, at a location of the first antenna coil 22, of a magnetic field produced by a current Ia flowing in the second antenna coil 31 can be found by considering a y-axis component Hy alone and given by the Biot-Savart's law as follows:

$$Hy = \frac{Ia(2\pi ra)\left\{ra / \sqrt{(ra^2 + d^2)}\right\}}{4\pi(ra^2 + d^2)}$$

$$= \frac{ra^2 \cdot Ia}{2(ra^2 + d^2)^{3/2}} \qquad \ldots(1)$$

$$= \alpha Ia$$

$$\alpha = \frac{ra^2}{2(ra^2 + d^2)^{3/2}} \qquad (2)$$

[0148] It is understood from above that the magnetic field Hy is proportional to the current Ia. An electromotive force Vb produced by electromagnetic induction in the first antenna coil 22 is expressed by

$$Vb = - (d\Phi b/dt) \qquad (3)$$

where Φb is the magnetic flux density of the first antenna coil 22.

[0149] The relationship between the magnetic flux density Φb of the first antenna coil 22 and the magnetic field Hy is expressed by

$$\Phi b = \mu \, Hy \ (\mu: \text{magnetic permeability}) \qquad (4)$$

[0150] Accordingly, using equations (1), (3) and (4), the electromotive force Vb is given by

$$Vb = - (d\Phi b/dt)$$
$$= -\mu \ (dHy/dt)$$
$$= -\alpha \mu \ (dIa/dt) \qquad \ldots(5)$$

where μ is a constant determined by material.

[0151] The electromotive force Vb occurs in the first antenna coil 22 due to a temporal variation in the current Ia flowing through the second antenna coil 31.

[0152] It is understood from the above equation (2) that α increases as the distance d between the first and second antenna coils 22 and 31 decreases and the sensitivity for communication becomes higher as the distance d between the first and second antenna coils 22 and 31 decreases.

[0153] According to the second embodiment, the first antenna coil 22 is formed on the surface of the IC chip 23, and the second and third antenna coils 31 and 32 are formed on the module board 30. The IC chip 23 is disposed on the module board 30 such that the first antenna coil 22 of the IC chip 23 is opposed to the second antenna coil 31. Thus, unlike the prior art, the radio IC card wherein the IC circuit 35 and third antenna coil 32 are electrically connected, without physical connection, can be obtained.

[0154] Accordingly, such an expensive mounting apparatus as a flip-chip bonder or a wire bonder is not required to mount the IC chip 23.

[0155] In addition, in the case of the resin-molding, a process management, for example, for considering heat-resistance, is needed and the reliability lowers.

[0156] Moreover, the degree of freedom for the manufacturing process is high, and the manufacturing cost is reduced.

[0157] In the manufacturing of the radio tag according to the second embodiment, the antenna coils 22 are formed of gold-plated wiring elements, thin-film patterns, or by printing conductive paste.

[0158] As shown in FIGS. 9A and 9B, however, the first antenna coil 22 may be formed by means of wire bonding.

[0159] Alternatively, the first antenna coil 22 may be formed with a multi-layer structure, as shown in FIG. 10.

[0160] Alternatively, antenna coils 22 may be formed on the upper and lower surfaces of the IC chip 23, as shown in FIG. 11.

[0161] Alternatively, the IC chip 23 may be provided with various electric elements such as capacitor 29 so as to have multi-functions, as shown in FIG. 12.

(3) A third embodiment according to the present invention will now be described.

[0162] FIGS. 17A and 17B show the structure of the radio IC card according to the third embodiment. FIG. 17A is a plan view and FIG. 17B is a cross-sectional view.

[0163] A carrier body 40 is provided with an IC chip 23, a communication antenna 41 and a power supply coil 42. The communication antenna 41 and power supply coil 42 are formed in rectangular spiral shapes.

[0164] The communication antenna 41 and power supply coil 42 are connected to the IC chip 23.

[0165] The carrier body 40 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride. The size of the carrier body is, e.g. 86 mm × 54 mm × 3 mm.

[0166] The communication antenna 41 and power supply coil 42 are formed, for example, by winding fine conductors twice or more, or by winding electric lines twice or more by means of deposition, etc. For example, coated copper-wire coils, copper-wire coils or aluminum-wire coils are used for the communication antenna 41 and power supply coil 42.

[0167] A space (hereinafter referred to as "cavity") 43 is defined inside the power supply coil 42. A permanent magnet 44 is movably provided within the cavity 43.

[0168] The permanent magnet 44 has a plate shape. One surface side of the permanent magnet 44 is magnetized with an N-pole, and the other surface side is magnetized with an S-pole. As is shown in FIG. 17B, the permanent magnet 44 is disposed to be movable in the direction of the central axis (S1) of the power supply coil 42. The permanent magnet 44 is formed of, e.g. an Alnico molded magnet, a Ba ferrite magnet, a rare-earth cobalt magnet, carbon steel, tungsten steel, KS steel, or Comfe. The size of the permanent magnet 44 is, e.g. 20 mm × 40 mm × 1 mm.

[0169] A method of manufacturing the above radio IC card will now be described with reference to an exploded perspective view of FIG. 18 and a flow chart of FIG. 19. In the flow chart of FIG. 19, triangular symbol ▽ denotes the provision of structural elements, and circular symbol ○ denotes manufacturing steps.

[0170] As is shown in FIG. 18, the carrier body 40 is a combination of a first casing body (lower card casing body) 40a and a second casing body (upper card casing body) 40b.

[0171] The lower card casing body 40a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0172] The upper card casing body 40b is provided with a cavity 43 for insertion of the permanent magnet 44.

[0173] To start with, as shown in FIG. 19, an IC chip 23 and a board 48 for the IC chip 23 are provided.

[0174] In step #1, the IC chip 23 is mounted on the board 48.

[0175] In step #2, the IC chip 23 mounted on the board 48 is set in the recess portion 45 in the lower card casing body 40a. In this step, the IC chip 23 is adhered to the recess portion 45.

[0176] The communication antenna 41 and power supply coil 42 are supplied to the manufacturing line.

[0177] Leads 41a and 42a for connection with the terminals of the board 48 extend from the communication antenna 41 and power supply coil 42.

[0178] In step #3, the communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 40a.

[0179] The leads 41a and 42a of the communication antenna 41 and power supply coil 42 are connected to the terminals of the board 48 by means of soldering.

[0180] The permanent magnet 44 is supplied to the manufacturing line. In step #4, the permanent magnet 44 is inserted in the cavity 43 in the upper card casing body 40b.

[0181] Subsequently, the lower card casing body 40a on which the IC chip 23, communication antenna 41 and power supply coil 42 are mounted is supplied to the manufacturing line, and the upper card casing body 40b in which the permanent magnet 44 is inserted are supplied to the manufacturing line.

[0182] In step #5, the lower card casing body 40a and upper card casing body 40b are combined and adhered to each other, whereby the carrier body 40 is formed.

[0183] In step #6, printing is effected on the surface of the carrier body 40.

[0184] At last, the manufactured radio IC card is examined.

[0185] The operation of the thus manufactured radio IC card will now be described.

[0186] If the radio IC card is carried by a person, etc., the entire body thereof moves. Thereby the permanent magnet 44 in the cavity 43 is moved.

[0187] The magnetic flux of the permanent magnet 44 crosses the power supply coil 42, and as a result an electromotive force is induced in the power supply coil 42. The induced electromagnetic force is supplied to the IC chip 23.

[0188] This operation will now be described more specifically with reference to FIGS. 20A and 20B which are enlarged partial views of the power supply coil 42.

[0189] If the radio IC card has moved, the permanent magnet 44 moves in the direction of the central axis s1 of the power supply coil 42 within the cavity 43.

[0190] Consider a case where the permanent magnet 44 is located at an end portion of the cavity 43, as shown in FIG. 20A, and a case where the permanent magnet 44 is located at a central portion of the cavity 43, as shown in FIG. 20B. Suppose that an upper surface of the permanent magnet 44 has an S-pole, and a lower surface thereof has an N-pole.

[0191] When the permanent magnet 44 is located at an end portion of the cavity 43, as shown in FIG. 20A, the flux density B within the power supply coil 42 takes a minimum value. When the permanent magnet 44 is located at a central portion of the cavity 43, as shown in FIG. 20B, the flux density takes a maximum value.

[0192] Accordingly, if the entire radio IC card is slightly moved, for example, by the hand of the user, the flux density B within the power supply coil 42 varies. The variation in the flux density B induces an electromotive force in the power supply coil 42. The electromotive force is supplied as power to the IC chip 23.

[0193] The permanent magnet 44 is movably provided within the cavity 43, but it may be provided, for example, in a rotatable manner.

[0194] FIGS. 21A and 21B show structures of the radio IC card. FIG. 21A is a partial plan view, and FIG. 21B is a partial cross-sectional view.

[0195] Both end portions of a plate-like permanent magnet 49 are rotatably supported by support members 50 and 51 within the cavity 43. The support member 51 is coupled to a dial 53. The dial 53 functions to rotate the permanent magnet 49 in the direction of arrow s2 from the outside, as shown in FIG. 21B.

[0196] In general, an induction electromotive force v occurs in a primary coil in such a direction as to cancel a temporal variation in magnetic flux within the coil. The electromotive force v is expressed by

$$v = -d\Phi/dt \quad (6)$$

where Φ is the flux, and t is time.

[0197] If the magnetic flux is B, the in-coil area is S, permeability is μ and magnetic field intensity is H,

$$\Phi = B \cdot S = \mu \cdot H \cdot S \quad \ldots(7)$$

[0198] The induction electromotive force v is expressed by

$$v = \mu \cdot S \cdot dH/dt \quad (8)$$

[0199] An example of calculation of induction electromotive force v is shown below. Since the cavity 43 is located within the power supply coil 42, the permeability of air is approximated on the basis of that of vacuum as follows:

$$\mu = 1.25 \times 10^{-6} \text{ [H/m]} \quad (9)$$

[0200] The permanent magnet 44 is rotatable within the radio IC card. The permanent magnet 44 has a plate shape and a size of 2 mm × 20 mm, and is formed of, e.g. $SmCo_5$.

[0201] The coercive force of the permanent magnet 44 is expressed by

$$H = 2.87 \times 10^{4} \text{ [Oe]} = 2.28 \times 10^{6} \text{ [A/m]} \quad \ldots(10)$$

[0202] If the permanent magnet 44 is rotated at 10 rps and the number of turns of the power supply coil 42 is set at 500, the electromotive force v is given by

$$v = 500\mu \cdot S \cdot 2\pi/10^{-1}$$
$$= 1.14 \text{ [V]} \quad \ldots(11)$$

[0203] In this example, an electromotive force of about 1 [V] is obtained.

[0204] According to the third embodiment, the cavity 43 is formed within the power supply coil 42 mounted on the radio IC card, and the permanent magnet 44 is movably provided within the cavity 43. Thus, electric energy due to induction electromotive force v can be supplied to the radio IC card by the permanent magnet 44 and, e.g. the manual operation, without using electric energy due to a cell or an electromagnetic coil.

[0205] Accordingly, exchange of a cell is not required, and power consumption in the standby state of the reader/writer can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured. For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced.

(4) A fourth embodiment of the present invention will now be described. The structural parts common to those shown in FIGS. 17A and 17B are denoted by like reference numerals, and a detailed description thereof is omitted.

[0206] The fourth embodiment relates to a data read/write apparatus using a radio IC card. FIGS. 22A and 22B show a structure of the radio IC card, and FIG. 23 schematically shows a structure of a radio IC card reader/writer 50.

[0207] In the radio IC card, the IC chip 23, communication antenna 41 and power supply coil 42 are mounted on the carrier body 40. The IC chip 23 is connected to the communication antenna 41 and power supply coil 42.

[0208] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 24.

[0209] The carrier body 40 is formed by combining a lower card casing body 40a and an upper card casing body 40b.

[0210] Like the radio IC card shown in FIG. 18, the lower card casing body 40a, the lower card casing body 40a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0211] To start with, the IC chip 23 and board 48 are prepared. The IC chip 23 is mounted on the board 48. The IC chip 23 is set in the recess portion 45 in the lower card casing body 40a.

[0212] Then, the communication antenna 41 and power supply coil 42 are prepared. These antennas 41 and 42 have leads 41a and 42a for connection with terminals of the board 48.

[0213] The communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 40a.

[0214] The leads 41a and 42a are connected to the terminals of the board 48 by means of, e.g. soldering.

[0215] The lower card casing body 40a, on which the IC chip 23, communication antenna 41 and power supply coil 42 have been mounted, is combined with the upper card casing body 40b. The lower card casing body 40a and the upper card casing body 40b are adhered to each other to constitute the carrier body 40.

[0216] Following the above, printing is effected on the surface of the carrier body 40.

[0217] At last, the manufactured radio IC card is inspected.

[0218] On the other hand, the reader/writer 50 reads/writes data from/in the radio IC card which is situated as shown in FIG. 23.

[0219] The reader/writer 50 includes a read/write antenna 51 which corresponds in position to the communication antenna 41 of the radio IC card. The reader/writer 50 also includes a permanent magnet 52 which corresponds in position to the power supply coil 42 of the radio IC card.

[0220] The power supply operation of the data read/write apparatus with the above construction, by which power is supplied to the radio IC card, will now be described.

[0221] If the carrier body 40 is moved toward the reader/writer 50, the power supply coil 42 in the radio IC card approaches the permanent magnet 52 in the reader/writer 50, as shown in FIGS. 25 and 26. With the power supply coil 42 approaching the permanent magnet 52, the flux density B within the power supply coil 42 varies and an electromotive force is induced in the power supply coil 42. The induced electromotive force is supplied to the IC chip 23.

[0222] According to the fourth embodiment, the reader/writer 50 is provided with the permanent magnet 52. By approaching the carrier body 40 to the reader/writer 50, the electromotive force is induced in the power supply coil 42 and it is supplied to the IC chip 23 of the radio IC card. Like the first embodiment, electric energy can be supplied to the radio IC card when data read/write is effected by the reader/writer 50, without using electric energy due to a cell or an electromagnetic induction coil. Therefore, no exchange of a cell is required, and power consumption in the standby state of the reader/writer 50 can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured.

(5) A fifth embodiment of the present invention will now be described. The structural parts common to those shown in

FIGS. 17A and 17B are denoted by like reference numerals, and a detailed description thereof is omitted.

[0223] FIG. 27 is an exploded perspective view of a radio IC card.

[0224] A method of manufacturing the radio IC card will now be described.

[0225] The carrier body 40 is formed by combining a lower card casing body 40a and an upper card casing body 40b.

[0226] The lower card casing body 40a is provided with recess portions 61 and 62 for receiving the IC chip 23 and a communication/power-supply coil 60.

[0227] The upper card casing body 40b is provided with the cavity 43 for receiving the permanent magnet 44.

[0228] To begin with, the IC chip 23 and board 48 are prepared.

[0229] The IC chip 23 is mounted on the board 48.

[0230] The IC chip 23 mounted on the board 48 is set in the recess portion 61 in the lower card casing body 40a.

[0231] The communication/power-supply coil 60 is prepared. The coil 60 has leads 60a for connection with terminals of the board 48. The communication/power-supply coil 60 is set in the recess portion 62 in the lower card casing body 40a. The leads 60a are connected to the terminals of the board 48 by means of, e.g. soldering.

[0232] Then the permanent magnet 44 is prepared. The permanent magnet 44 is inserted in the cavity 43 in the upper card casing body 40b.

[0233] The lower card casing body 40a, on which the IC chip 23 and communication/power-supply coil 60 are mounted, and the upper card casing body 40b, in which the permanent magnet 44 is inserted, are combined and adhered to each other. Thus the carrier body 40 is constituted.

[0234] Following the above, printing is effected on the surface of the carrier body 40. Finally, the radio IC card is inspected.

[0235] The operation of the radio IC card thus manufactured will now be described.

[0236] If the radio IC card is carried by the user and moved, the permanent magnet 44 in the cavity 43 is moved.

[0237] With the movement of the permanent magnet 44, the magnetic flux of the permanent magnet 44 crosses the communication/power-supply coil 60. Consequently, an electromotive force is induced in the communication/power-supply coil 60. The induced electromotive force is supplied to the IC chip 23.

[0238] Needless to say, according to the fifth embodiment, the same advantages as with the first embodiment can be obtained with use of the communication/power-supply coil 60.

[0239] The third to fifth embodiments may be modified as follows.

[0240] For example, as shown in FIG. 28, a plurality of permanent magnets 71 may be arranged in an automatic wicket 70. The radio IC card shown in FIGS. 22A and 22B is made to pass by the permanent magnets 71. At this time, the flux density B within the power supply coil 42 varies, and an electromotive force induced in the power supply coil 42 is supplied to the IC chip 23.

(6) A sixth embodiment of the present invention will now be described with reference to the accompanying drawings.

[0241] FIG. 29A shows a structure of a radio IC card, and FIG. 29B is a cross-sectional view of the radio IC card.

[0242] An IC chip 23 and a communication antenna 41 are mounted on a carrier body 80. The communication antenna 41 is electrically connected to the IC chip 23.

[0243] The carrier body 80 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET), vinyl chloride, etc.

[0244] The communication antenna 41 is formed of, e.g. a coated copper wire coil, a copper wire coil or an aluminum wire coil.

[0245] A piezoelectric element 81 electrically connected to the IC chip 23 is mounted on the carrier body 80. Electrodes 82a and 82b are provided at both ends of the piezoelectric element 81. The electrodes 82a and 82b are electrically connected to the IC chip 23.

[0246] The piezoelectric element 81 has such a piezoelectrical effect that when pressure is applied to the piezoelectric element 81, as shown in FIG. 30, it is polarized to have positive and negative charges (+,-). The piezoelectric element 81 is formed of, e.g. Rochelle salt, barium titanate, potassium dihydrogenphosphate, ammonium hydrogenphosphate, lithium sulfate, lithium niobate, zinc oxide, polyvinyl difluoride, antimony iodide-sulfide, or zinc zirconate-titanate.

[0247] FIG. 31 is an electric circuit diagram of the above radio IC card.

[0248] The communication antenna 41 and electrodes 82a and 82b are connected to the IC chip 23. The electrodes 82a and 82b are provided at both ends of the piezoelectric element 81. The piezoelectric element 81 serves as a power supply for the IC chip 23.

[0249] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 32 and a flow chart of FIG. 33.

[0250] The carrier body 80, as shown in FIG. 32, is formed by combining a first casing body (lower card casing body) 80a and a second casing body (upper card casing body) 80b.

[0251] A recess portion 83 for receiving the piezoelectric element 81 is formed in the lower card casing body 80a. Although not shown, the lower card casing body 80a is provided with recess portions for receiving the IC chip 23 and communication antenna 41.

[0252] To start with, as shown in FIG. 33, the IC chip 23 and board 84 are prepared. In step #10, the IC chip 23 is

mounted on the board 84. In the next step #11, the board 84 as a COB (chip-on-board) 85 is set in the recess portion 80 in the lower card casing body 80a.

[0253] The communication antenna 41 is supplied to the manufacturing line. The communication antenna 41 has leads 41a for connection with the terminals of the COB 85. In step #12, the communication antenna 41 is set in the recess portion in the lower card casing body 80a.

[0254] The leads 41a of the communication antenna 41 are connected to the terminals of the COB 85 by means of, e.g. soldering.

[0255] Subsequently, the piezoelectric element 81 and the terminals 82a and 82b to be provided at both ends of the piezoelectric element 81 are supplied. The electrodes 82a and 82b have leads 86 and 87 for connection with the terminals of the COB 85. The electrodes 82a and 82b are provided at both ends of the piezoelectric element 81.

[0256] In step #13, the piezoelectric element 81 with the electrodes is set in the recess portion in the lower card casing body 80a. The leads 86 and 87 of the electrodes 82a and 82b are connected to the terminals of the COB 85 by means of, e.g. soldering.

[0257] In step #14, the lower card casing body 80a on which the COB 85, communication antenna 41 and piezoelectric element 81 with electrodes are mounted, is combined with, and adhered to, the upper card casing body 80b. Thus, the carrier body 90 is constituted.

[0258] In step #15, printing is effected on the surface of the carrier body 90, and at last the manufactured radio IC card is inspected.

[0259] The size of the manufactured radio IC card is 85 mm × 54 mm, each side of the IC chip is 3 mm, each size of the communication antenna 41 is 45 mm, and the size of the piezoelectric element 81 is 30 mm × 45 mm × 2 mm.

[0260] The operation of the radio IC card will now be described.

[0261] If pressure is applied to the piezoelectric element 81 of the radio IC card, it is polarized to have positive and negative charges (+,-), as shown in FIG. 30. An electromotive force is produced at the electrodes 82a and 82b of the piezoelectric element 81, and it is supplied to the IC chip 23.

[0262] Accordingly, if pressure is applied to the piezoelectric element 81 of the radio IC card by a pressurizing mechanism or the hand of the user, the electromotive force produced by the piezoelectric element 81 is supplied to the IC chip 23.

[0263] As has been described above, according to the sixth embodiment, the electromotive force produced by the piezoelectric element 81 is supplied to the IC chip 23. Thus, like the third embodiment, no exchange of a cell is required, energy saving is realized, and the radio IC card with simple structure is obtained. For example, compared to the cell-built-in type non-contact data carrier, the energy saving ratio of power supply is 100% and no waste cell is produced. Therefore, the life of the apparatus can be increased while the apparatus can be operated with clean energy.

(7) A seventh embodiment of the present invention will now be described with reference to the accompanying drawings.

[0264] FIG. 34A shows the structure of a radio IC card and FIG. 34B is a cross-sectional view of the radio IC card.

[0265] An IC chip 23 and communication antenna 41 are mounted on the carrier body 90. The communication antenna 41 is electrically connected to the IC chip 23.

[0266] The carrier body 90 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride.

[0267] The communication antenna 41 is formed of, e.g. coated copper-wire coils, copper-wire coils or aluminum-wire coils.

[0268] The carrier body 90 incorporates a plate-like piezoelectric element (hereinafter referred to as "piezoelectric element board") 91. The piezoelectric element board 91 serves as a board of the radio IC card body.

[0269] The piezoelectric element board 91 has such a piezoelectrical effect that when pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-). Like the sixth embodiment, the piezoelectric element board 91 is formed of, e.g. Rochelle salt, barium titanate, potassium dihydrogenphosphate, ammonium hydrogenphosphate, lithium sulfate, lithium niobate, zinc oxide, polyvinyl difluoride, antimony iodide-sulfide, or zinc zirconate-titanate.

[0270] The IC chip 23 and communication antenna 41 are mounted on the piezoelectric element board 91.

[0271] The electrodes 92a and 92b are provided on both surfaces of the piezoelectric element board 91. The electrodes 92a and 92b are electrically connected to the IC chip 23. It is preferable to form the electrodes 92a and 92b as large as possible on both surfaces of the piezoelectric element board 91.

[0272] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 35 and a flow chart of FIG. 36.

[0273] As is shown in FIG. 35, the carrier body 90 is formed by providing the piezoelectric element board 91 with a lower outside sheet 90a and an upper outside sheet 90b.

[0274] The communication antenna 41 and electrodes 92a and 92b are formed on the piezoelectric element board 91.

[0275] To begin with, as shown in FIG. 35, the IC chip 23 and piezoelectric element board 91 are supplied to the manufacturing line. In step #20, the IC chip 23 is mounted on the piezoelectric element board 91.

[0276] In step #21, the lower outside sheet 70a and upper outside sheet 70b are attached, by means of pressing or

laminating, to both surfaces of the piezoelectric element board 91 on which the IC chip 23 is mounted. Thus, the carrier body 90 is formed.

[0277] In step #22, printing is effected on the surface of the carrier body 90.

[0278] At last, the manufactured radio IC card is inspected.

[0279] FIGS. 37A and 37B show an example of the size of the manufactured radio IC card. The size of the entire radio IC card is 86 mm × 54 mm × 3 mm.

[0280] The operation of the manufactured radio IC card will now be described.

[0281] If pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-), as shown in FIG. 30. An electromotive force is produced at the electrodes 92a and 92b of the piezoelectric element board 91, and it is supplied to the IC chip 23.

[0282] Accordingly, if pressure is applied to the piezoelectric element board 91 by a pressurizing mechanism or the hand of the user, the electromotive force produced by the piezoelectric element board 91 is supplied to the IC chip 23.

[0283] As has been described above, according to the seventh embodiment, the electromotive force produced by the piezoelectric element board 91 used as the board of the carrier body 90 is supplied to the IC chip 23. Thus, like the third embodiment, no exchange of a cell is required, energy saving is realized, and the radio IC card with simple structure is obtained.

[0284] For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced. Therefore, the life of the apparatus can be increased while the apparatus can be operated with clean energy.

(8) An eighth embodiment of the present invention will now be described with reference to the accompanying drawings.

[0285] FIG. 38 shows the structure of a data read/write apparatus.

[0286] The data read/write apparatus comprises, for example, the radio IC card 100 according to the seventh embodiment, as a radio IC card, and a reader/writer 101 for reading/writing data from/in the radio IC card 100.

[0287] Since the radio IC card 100 has the same structure as the radio IC card according to the seventh embodiment, a description thereof is omitted.

[0288] On the other hand, in the state in which the radio IC card 100 is set in position, the reader/writer 101 reads/writes data from/in the radio IC card 100.

[0289] The reader/writer 101 comprises a read/write antenna 102, which is so situated as to correspond in position to the communication antenna 41 of the radio IC card 100, and a data processing unit 103, connected to the read/write antenna 102, for controlling data read/write, processing data and storing data.

[0290] The reader/writer 101 has a carrier passage 105 communicating with a carrier insertion opening 104. A pair of rollers 106a and 106b are provided along the carrier passage 105.

[0291] When the radio IC card 100 is set in the reader/writer 101, the rollers 106a and 106b serve as a pressing mechanism for pressing the electrodes 92a and 92b provided on the piezoelectric element board 91 of radio IC card 100.

[0292] In addition to the rollers 106a and 106b, a plurality of rollers are provided along the carrier passage 105 in order to guide the radio IC card 100 through the carrier passage 105.

[0293] A power supply operation in the data read/write apparatus with the above structure, by which power is supplied to the radio IC card 100, will now be described.

[0294] If the radio IC card 100 is inserted into the carrier insertion opening 104 in the reader/writer 101, the radio IC card 100 is automatically guided into the carrier passage 105 and set in a data read/write position.

[0295] At this time, the rollers 106a and 106b press the electrodes 92a and 92b provided on the piezoelectric element board 91 of radio IC card 100, as shown in FIG. 39.

[0296] If pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-). An electromotive force is produced at the electrodes 92a and 92b of the piezoelectric element board 91, and it is supplied to the IC chip 23.

[0297] Thereby, data is transmitted between the radio IC card 100 and reader/writer 101 by means of their communication antennas 41 and 102.

[0298] In the eighth embodiment of the invention, the piezoelectric element board 91 of radio IC card 100 is pressed by the paired rollers 106a and 106b of reader/writer 101 to produce an electromotive force, and the electromotive force is supplied to the IC chip 23. Accordingly, like the fourth embodiment, electric energy can be supplied to the radio IC card 100 when data read/write is effected by the reader/writer 101, without using electric energy due to a cell or an electromagnetic induction coil.

[0299] Therefore, no exchange of a cell is required, and power consumption in the standby state of the reader/writer 101 can be reduced to achieve energy saving. Thus, the radio IC card 100 with simple structure can be manufactured.

(9) A ninth embodiment of the invention will now be described with reference to the accompanying drawings.

[0300] FIGS. 40A and 40B show the structure of a radio IC card. FIG. 40A is a plan view and FIG. 40B is a cross-sectional view.

[0301] An IC chip 23, a communication antenna 41 and a power supply coil 42 are mounted on a carrier body 110.

The communication antenna 41 and power supply coil 42 are formed in a rectangular spiral shape, respectively.

[0302] The communication antenna 41 is electrically connected to an antenna coil 31 situated opposed to an antenna coil 22 of the IC chip 23.

[0303] The power supply coil 42 is electrically connected to the communication antenna 41.

[0304] The power supply coil 110 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride.

[0305] The communication antenna 41 and power supply coil 42 are formed, for example, by winding fine conductors twice or more, or by winding electric lines twice or more by means of deposition, etc. For example, coated copper-wire coils, copper-wire coils or aluminum-wire coils are used for the communication antenna 41 and power supply coil 42.

[0306] A cavity 43 is defined inside the power supply coil 42. A permanent magnet 44 is movably provided within the cavity 43.

[0307] The permanent magnet 44 has a plate shape.

One surface side of the permanent magnet 44 is magnetized with an N-pole, and the other surface side is magnetized with an S-pole. As is shown in FIG. 40B, the permanent magnet 44 is disposed to be movable in the direction of the central axis (S1) of the power supply coil 42. The permanent magnet 44 is formed of, e.g. an Alnico molded magnet, a Ba ferrite magnet, a rare-earth cobalt magnet, carbon steel, tungsten steel, KS steel, or Cunife.

[0308] A method of manufacturing the radio IC card will now be described with reference to FIGS. 41A to 41D illustrating the respective manufacturing steps.

[0309] The IC chip 23 is formed, as in the first embodiment.

[0310] In brief, the insulating protection film 21 shown in FIG. 7B is formed on the surface of the semiconductor wafer 20 shown in FIG. 7A.

[0311] As is shown in FIG. 7C, the antenna coil 22 of, e.g. gold-plated wire, is formed on the insulating protection film 21.

[0312] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0313] On the other hand, as shown in FIG. 41B, the communication antenna coil 41 and antenna coil 31 are formed on a surface of a module board 111.

[0314] The shape of the antenna coil 31 is substantially the same as that of the antenna coil 22 formed on the IC chip 23.

[0315] Since the communication antenna coil 41 is used for communication with the outside, the number of turns of the coil 41 is made greater than that of the antenna coil 31 and the coil 41 is made larger than the coil 31. The communication antenna coil 41 and antenna coil 31 are electrically connected to each other.

[0316] The communication antenna coil 41 and antenna coil 31 are simultaneously formed on the surface of the module board 111, for example, by a subtractive method, as in the formation of a regular printed circuit board. These antenna coils 41 and 31 may be formed by an additive method.

[0317] These antenna coils 41 and 31 may be formed by fixing coils of coated wire on the module board 111. Alternatively, the antenna coils may be formed of a combination of printed wire and wire coils.

[0318] Specifically, the communication antenna coil 41 and antenna coil 31 are both formed by etching Ag, Al, etc. Alternatively, the antenna coils 41 and 31 may both be formed by a printing method using Ag paste, or formed of coils of Cu. Furthermore, the antenna coil 31 may be formed by printing or etching.

[0319] In a subsequent step, an insulating film 21 is formed on the antenna coil 31, as shown in FIG. 41C. The insulating film 21 is formed of a semi-hardened epoxy resin with a thickness of, e.g. 20 μm. For example, the insulating film 21 is formed by attaching an insulating adhesive film of a semi-hardened epoxy resin. The insulating film 21 may be formed of some other insulative resin such as polyimide or a metal oxide.

[0320] Thereafter, the IC chip 23 is opposed to, and disposed on, the antenna coil 31.

[0321] In this case, the IC chip 23 is mounted in a face-down fashion. The mounting is performed under a suitable pressure such that the antenna coil 31 is opposed to the antenna coil 22 of the IC chi 23 with the insulating film 21 interposed.

[0322] In addition, the mounting is performed such that the gap between the antenna coil 22 and antenna coil 31 is mechanically controlled and the gap is set at about 20 μm or less. In the mounting step, in order to completely harden the insulating adhesive film of, e.g. semi-hardened epoxy resin, which forms the insulating film 21, it is heated at about 200°C to 120°C for 10 to 120 seconds and fixed on the module board 111.

[0323] For example, the material of the insulating adhesive film may be applied in a viscous liquid phase. In this case, where the maintenance of the insulating film 21 is difficult under pressure, the height of the film may be controlled. For example, the insulating film 21 may be maintained by using a spacer of a polyester film with a thickness of, e.g. 10 μm, which serves also as the insulating film 21.

[0324] An insulating film 112 is then formed on the module board 111.

[0325] The power supply coil 42 is formed on the insulating film 112. The power supply coil 42 is formed, for example, by a subtractive method, as in the formation of a regular printed circuit board.

[0326] The power supply coil 42 may be formed by an additive method. The power supply coil 42 may be formed by fixing coils of coated wire on the module board 111. Alternatively, the coil 42 may be formed of a combination of printed wire and a wire coil.

[0327] A cavity portion 43 containing a permanent magnet 44 is provided. The permanent magnet 44 is movably provided within the cavity portion 43. The cavity portion 43 is mounted on the insulating film 112.

[0328] As is shown in FIG. 41D, the entire module board 111 with the IC chip 23 and cavity portion 43 is sealed with resin 113. Magnetic particles are dispersed in the resin 113.

[0329] The entire body of the module board 111 is coated with a polyester film 33. Finally, the radio IC card is obtained after printing and punching.

[0330] FIG. 42 is a cross-sectional view of the IC chip of the manufactured radio IC card. The method of forming the radio IC card is, for example, injection molding using, e.g. a polyester resin, or pressing molding using, e.g. a vinyl chloride sheet.

[0331] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 43 and a flow chart of FIG. 44.

[0332] As is shown in FIG. 43, the carrier body 110 is a combination of a first casing body (lower card casing body) 110a and a second casing body (upper card casing body) 110b.

[0333] The lower card casing body 110a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0334] The lower card casing body 110a is provided with a recess portion 120 for electrical connection between the communication antenna 41 and power supply coil 42.

[0335] The cavity portion 43 for insertion of the permanent magnet 44 is provided on the upper card casing body 110b.

[0336] Magnetic particles are dispersed in both the lower card casing body 110a and upper card casing body 110b.

[0337] To start with, as shown in FIG. 44, the IC chip 23 and the board 48 for the IC chip 23 are prepared.

[0338] In step #30, the IC chip 23 is mounted on the board 48.

[0339] In step #31, the IC chip 23 mounted on the board 48 is set in the recess portion 45 in the lower card casing body 110a. In this case, the IC chip 23 is adhered to the recess portion 45.

[0340] Next, the communication antenna 41 and power supply coil 42 are supplied. The communication antenna 41 has leads 41a for connection with the terminals of the substrate 48. The communication antenna 41 also has leads 41b for electrical connection with the power supply coil 42.

[0341] The power supply coil 42 has leads 42a for electrical connection with the communication antenna 41.

[0342] In step #32, the communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 110a. The leads 41a of the communication antenna 41 are connected to the terminals of the board 48 by means of, e.g. soldering.

[0343] The leads 41a of the communication antenna 41 and the leads 42a of the power supply coil 42 are electrically connected by means of, e.g. soldering.

[0344] The permanent magnet 44 is then supplied. In step #33, the permanent magnet 44 is inserted in the cavity portion 43 on the upper card casing body 110b.

[0345] Subsequently, the lower card casing body 110a, on which the IC chip 23, communication antenna 41 and power supply coil 42 are mounted, is supplied. In addition, the upper card casing body 110b in which the permanent magnet 44 is inserted is supplied.

[0346] In step #34, the lower card casing body 110a and upper card casing body 110b are combined and adhered to each other. Thus, the carrier body 110 is constituted.

[0347] In step #35, printing is effected on the surface of the carrier body 110, and at last the manufactured radio IC card is inspected.

[0348] The operation of the radio IC card thus manufactured will now be described.

[0349] If the radio IC card is carried by a person, etc., the entire body thereof is moved. Thereby, the permanent magnet 44 in the cavity 43 moves.

[0350] The magnetic flux of the permanent magnet 44 crosses the power supply coil 42, thus inducing an electromotive force in the power supply coil 42. The electromotive force is supplied to the IC chip 23 through the communication antenna 41.

[0351] As has been described above, according to the ninth embodiment of the invention, electric energy can be supplied to the radio IC card due to the induced electromotive force v, which is produced by, e.g. a manual operation of the permanent magnet 44, without using electric energy due to a cell or an electromagnetic coil.

[0352] In this case, since magnetic particles are dispersed in the seal resin 113 or the lower and upper card casing bodies 110a and 110b, the sensitivity of transmission between the communication antenna 41 and IC chip 23 can be enhanced.

[0353] Furthermore, since the magnetic particles are dispersed, the electromotive force induced in the power supply coil 42 can be increased and also the power to be supplied to the IC chip 23 increased.

[0354] Accordingly, exchange of a cell is not required, and power consumption in the standby state of the reader/writer can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured. For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced.

Claims

1. A radio IC card for data communication with outside, characterized by comprising:

   a board (30) having at least two rectangular-spiral antennas (31, 32) formed thereon; and
   a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof, the semiconductor element being mounted on the board such that the antenna (22) on the semiconductor element is situated opposed to one (31) of said at least two antennas on the board (30).

2. A radio IC card according to claim 1, characterized in that said antenna (23) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

3. A radio IC card according to claim 1, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

4. A radio IC card according to claim 1, characterized in that a layer of the antenna (22) formed of a metallic film and a layer of an insulating film (21) are laminated on the surface of the semiconductor element.

5. A radio IC card according to claim 1, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

6. A radio IC card according to claim 1, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (29).

7. A radio IC card according to claim 1, characterized in that one (31) of the antennas formed on the board (30) has substantially the same shape as the antenna (22) formed on the semiconductor element, and the other (32) of the antennas on the board is greater in size than said one (31) of the antennas on the board.

8. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the other (32) of the antennas on the board are electrically connected.

9. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the antenna (22) on the semiconductor device are electromagnetically connected.

10. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with an insulating film (21) interposed.

11. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

12. A radio IC card according to claim 1, characterized in that an insulating film (21) is formed on each of the antennas (31, 32) on the board.

13. A radio IC card according to claim 1, characterized in that an insulating film (21), in which magnetic particles are dispersed, is formed on each of the antennas (31, 32) on the board.

14. A radio IC card according to claim 1, characterized in that said semiconductor element (23) and said substrate (30) are integrally sealed with resin (25).

15. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

forming a rectangular-spiral antenna (22) on a surface of a semiconductor element (23);
forming at least two rectangular-spiral antennas (31, 32) on a board (30); and
disposing the antenna (22) formed on the semiconductor element such that the antenna formed on the semiconductor element is opposed to one (31) of said antennas formed on the board.

16. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a thin-film patterning process.

17. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a printing process.

18. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed such that a plurality of electrode pads (26) are provided on the surface of the semiconductor element and the electrode pads are connected by means of wire bonding.

19. A method of manufacturing a radio IC card, according to claim 15, characterized in that said at least two antennas (31, 32) on the board are integrally formed.

20. A method of manufacturing a radio IC card, according to claim 15, characterized in that the method includes a step of integrally sealing the semiconductor element (23) and the board (30) with resin (25).

21. A radio IC card having at least one rectangular-spiral antenna (42) and one semiconductor element (23) mounted thereon, characterized in that a cavity portion (43) is provided near the antenna and a permanent magnet (44) is movably provided within the cavity portion.

22. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is movable in a direction of a central axis of the antenna (42).

23. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is rotatably provided within the cavity portion (43).

24. A radio IC card according to claim 21, characterized in that the antenna (42) serves both for power supply to the semiconductor element (23) and for data communication.

25. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and one rectangular-spiral antenna (41, 42) on a first casing body (40a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (40b) to the first casing body provided with said at least one semiconductor element and one antenna and said permanent magnet.

26. A data reader/writer apparatus for reading/writing data from/in a radio IC card, the apparatus characterized by comprising:

a radio IC card on which at least one rectangular-spiral antenna (41, 42) and a semiconductor element (23) are mounted; and
read/write means for performing data communication with the semiconductor element mounted on the radio IC card, the read/write means having a permanent magnet (52) for inducing an electromotive force in the antenna mounted on the radio IC card by crossing a magnetic field over the antenna.

27. A radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon, characterized in that the radio IC card comprises a piezoelectric element (81) connected to the semiconductor element.

28. A radio IC card according to claim 27, characterized in that said piezoelectric element (81) is used as a board, and said at least one antenna (41) and one semiconductor element (23) are mounted on the piezoelectric element.

29. A radio IC card according to claim 27, characterized in that electrodes (92a, 92b) are provided on both sides of the piezoelectric element (91), and these electrodes are electrically connected to at least said semiconductor element (23).

30. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) to a first casing body (80a);
attaching a piezoelectric element (81) to the first casing body (80a); and
adhering a second casing body (80b) to the first casing body (80a).

31. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) on a board (91) formed of a piezoelectric element; and
applying an outer coating to the board (91) on which the antenna and the semiconductor element are attached.

32. A data read/write apparatus characterized by comprising:

a radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon and including a piezoelectric element (81) connected to the semiconductor element (23); and
read/write means for performing data communication with the semiconductor element (23) by means of the antenna (41), the read/write means including a pressing mechanism (106a, 106b) for pressing the piezoelectric element (81) of the radio IC card, thereby producing an electric charge in the piezoelectric element.

33. A radio IC card for data communication with outside, characterized by comprising:

a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof;
a board (111) having at least three rectangular-spiral antennas (31, 41, 42) formed thereon such that one (31) of said at least three antennas is situated, opposed to the antenna (22) of the semiconductor element;
a cavity portion (43) provided near one (42) of the other antennas on the board; and
a permanent magnet (44) provided movably in the cavity portion.

34. A radio IC card according to claim 33, characterized in that on said board (111) there are provided:

an antenna (31) situated to be opposed to the antenna (22) on the semiconductor element (23);
a communication antenna (41) electrically connected to said antenna; and
a power supply antenna (42) electrically connected to the communication antenna (41), a magnetic flux of the permanent magnet (44) being crossed over the power supply antenna.

35. An IC card according to claim 33, characterized in that said antennas are sealed with an insulating material (113) in which magnetic particles are dispersed.

36. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and at least three rectangular-spiral antennas (31, 41, 42) on a first casing body (100a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (110b) to the first casing body (110a).

37. A method of manufacturing a radio IC card according to claim 36, characterized in that the method includes the steps of:

storing the permanent magnet (44) movably in a case; and
mounting the case in the recess portion.

38. A method of manufacturing a radio IC card according to claim 36, characterized in that the first and second casing

bodies (110a, 110b) are formed of an insulating material in which magnetic particles are dispersed.

39. A radio tag for data communication with inside, characterized in that a rectangular-spiral antenna (22) is formed on a surface of a semiconductor element (23).

40. A radio tag according to claim 39, characterized in that said antenna (22) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

41. A radio tag according to claim 39, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

42. A radio tag according to claim 39, characterized in that a layer of the antenna (22) formed of a metallic film (21) and a layer of an insulating film (21) are laminated on the surface of the semiconductor element (23).

43. A radio tag according to claim 39, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

44. A radio tag according to claim 39, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (24).

45. A radio tag according to claim 39, characterized in that the antenna (22) is provided over the semiconductor element (23), with an insulating film (21) interposed.

46. A radio tag according to claim 39, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

47. A radio tag according to claim 39, characterized in that the antenna (22) is formed on the semiconductor element (23), with an insulating film (21) containing dispersed magnetic particles interposed.

48. A radio tag according to claim 39, characterized in that the semiconductor element (23) having the antenna (22) formed on the surface thereof is sealed with resin (25).

49. A method of manufacturing a radio tag for data communication with outside, the method characterized by comprising the steps of:

forming an insulating film (21) over a surface of a semiconductor wafer (20) on which a plurality of semiconductor elements (23) are formed;
forming rectangular-spiral antennas (22) on the insulating film at positions corresponding to the semiconductor elements; and
dicing the semiconductor elements (23) out of the semiconductor wafer (20).

50. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a thin-film patterning process.

51. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a printing process.

52. A method of manufacturing a radio tag according to claim 49, characterized in that said antenna (22) on each of the semiconductor elements is formed by bonding a piece of bonding wire among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

53. A method of manufacturing a radio tag according to claim 49, characterized in that each of the semiconductor elements (23) on the surface of which the antenna is formed is sealed with resin (25).

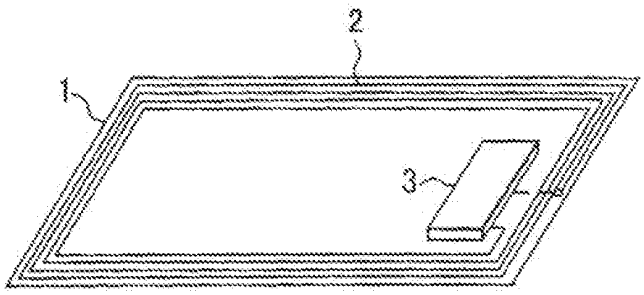


FIG. 1

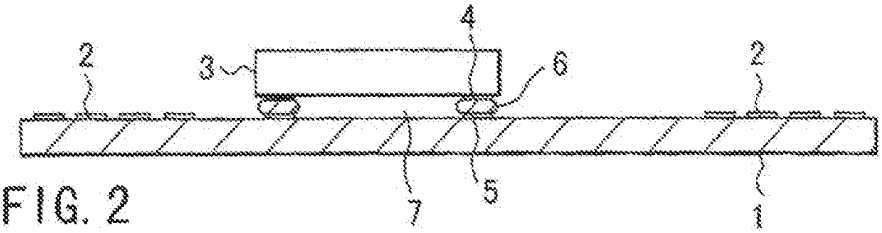


FIG. 2

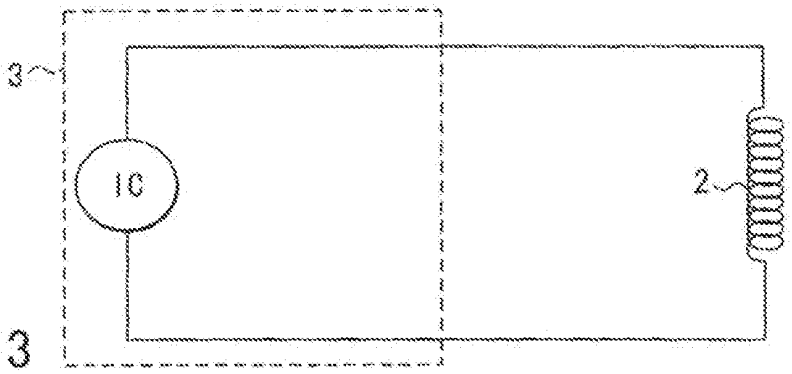


FIG. 3

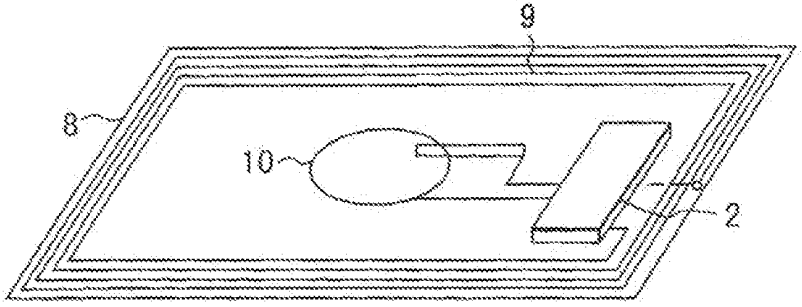


FIG. 4

FIG. 5

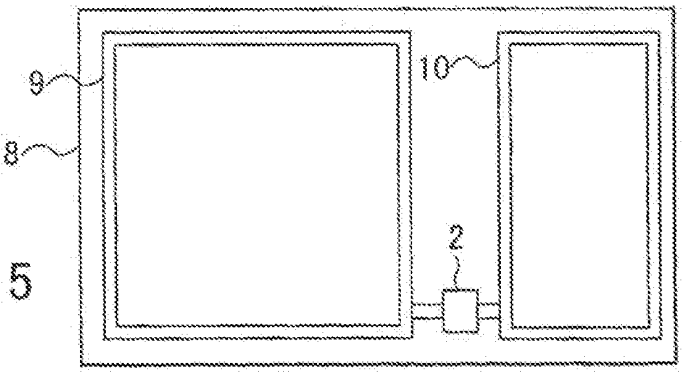


FIG. 6

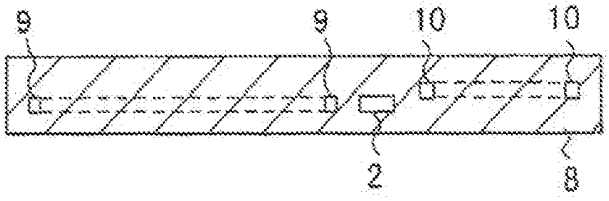


FIG. 7A

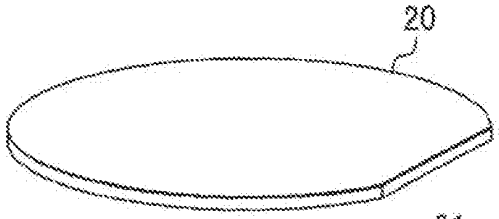


FIG. 7B

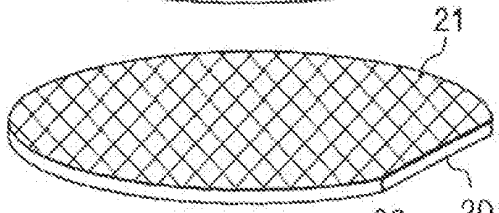


FIG. 7C

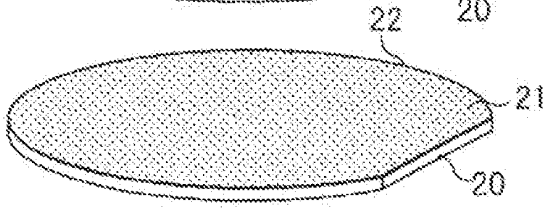
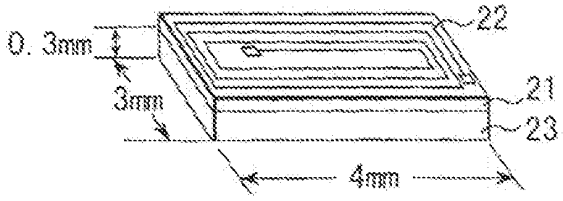


FIG. 7D



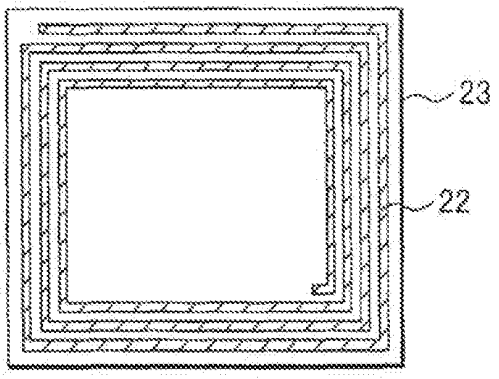


FIG. 8A

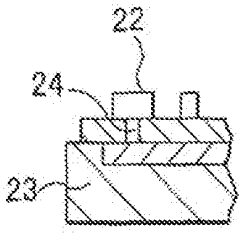
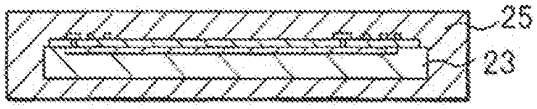


FIG. 8C



FIG. 8B

FIG. 8D



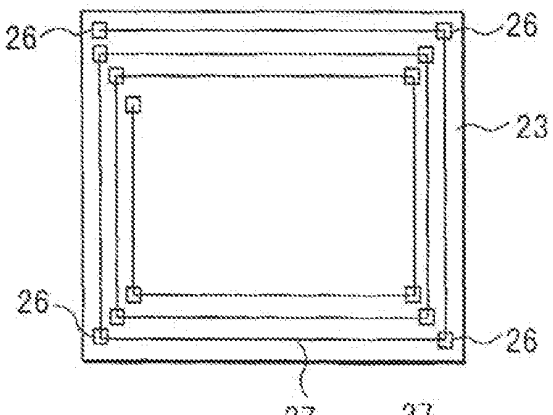


FIG. 9A

FIG. 9B

FIG. 10

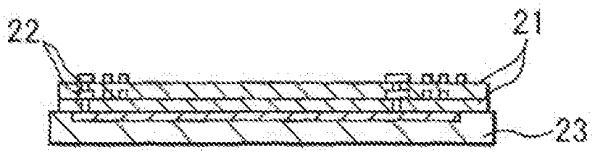


FIG. 11

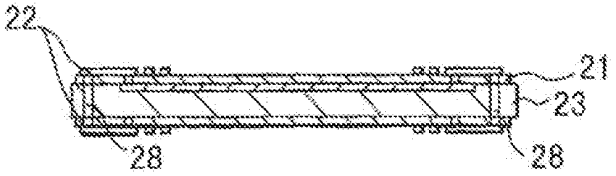


FIG. 12

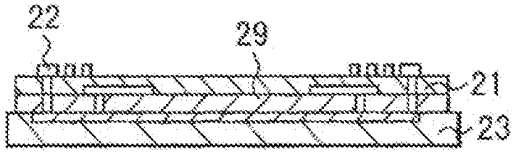


FIG. 13A

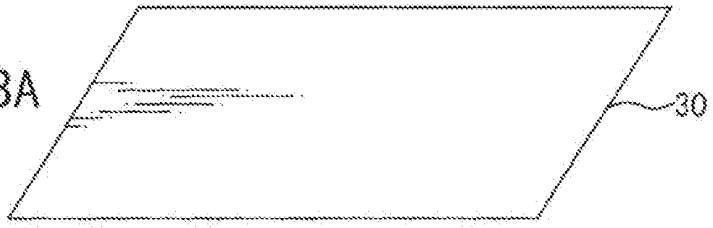


FIG. 13B

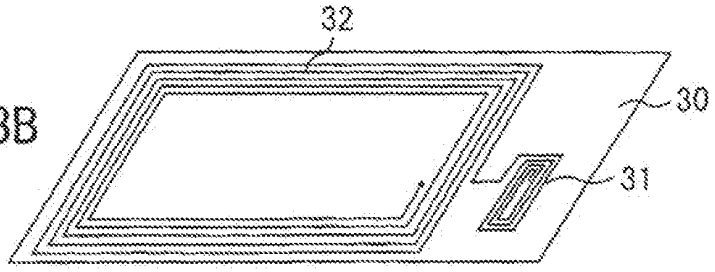
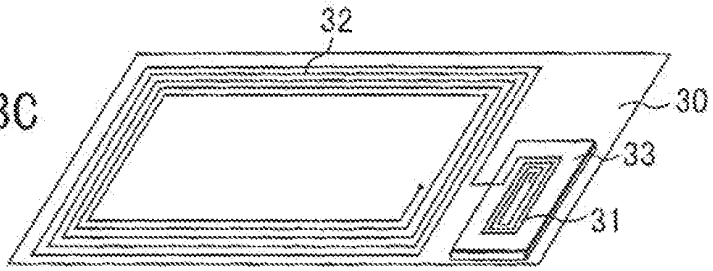


FIG. 13C



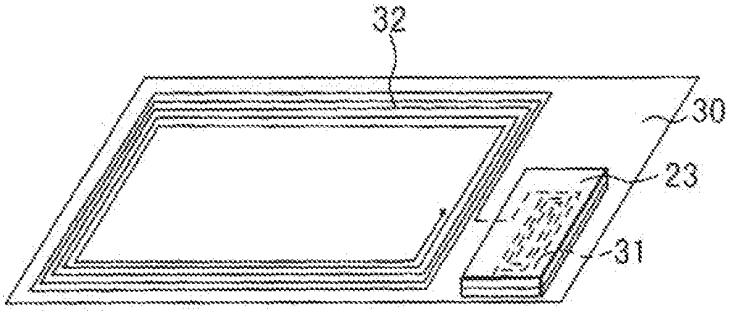


FIG. 13D

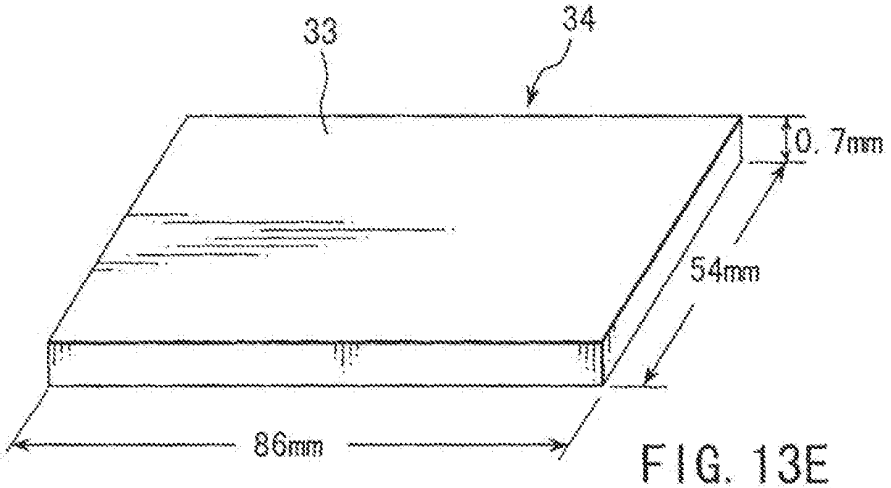


FIG. 13E

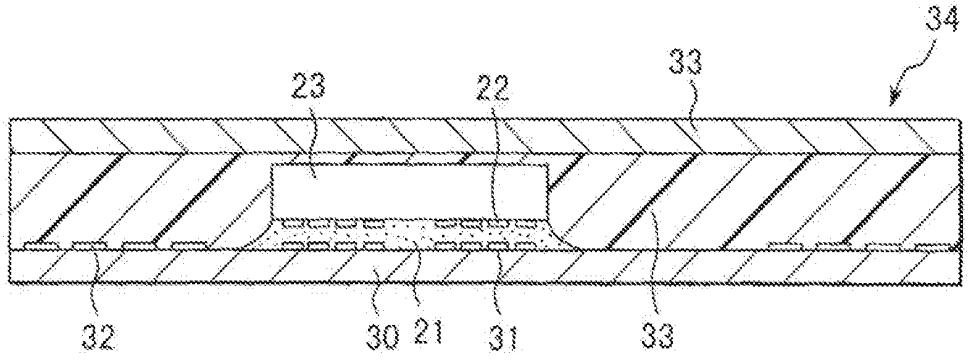


FIG. 14

FIG. 15

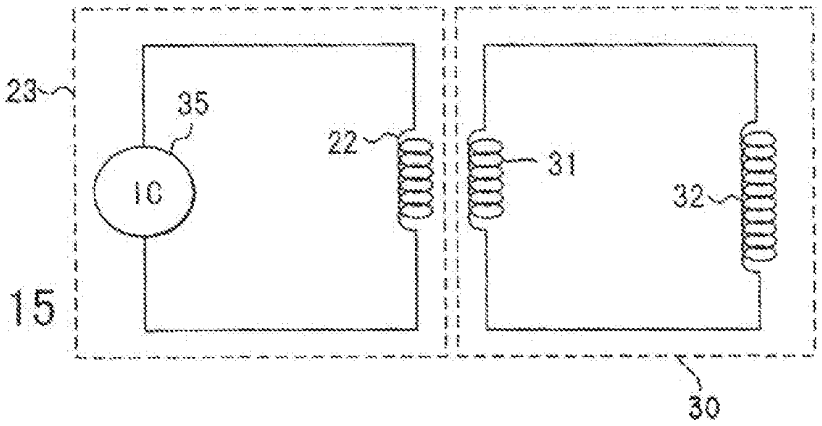


FIG. 16

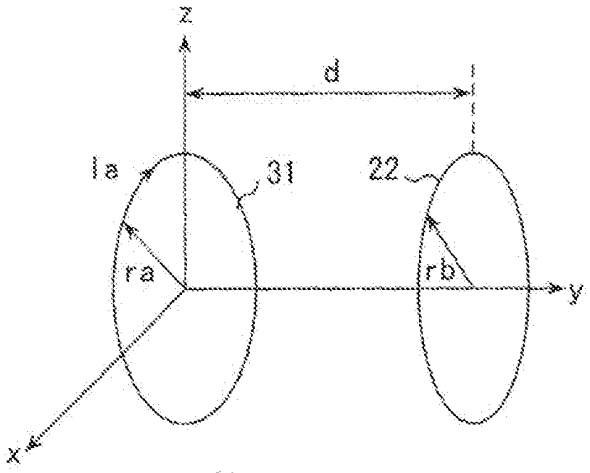


FIG. 17A

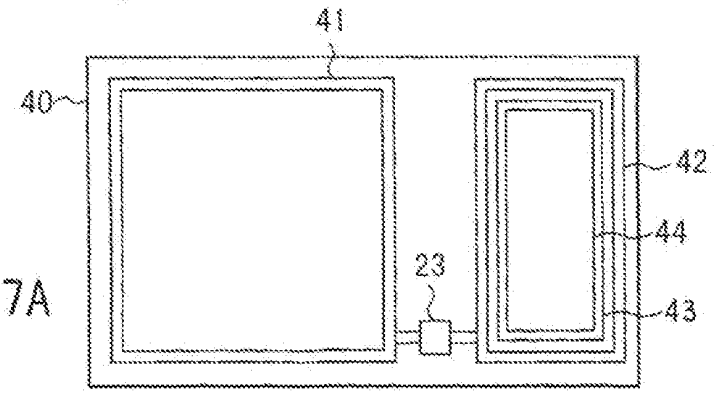
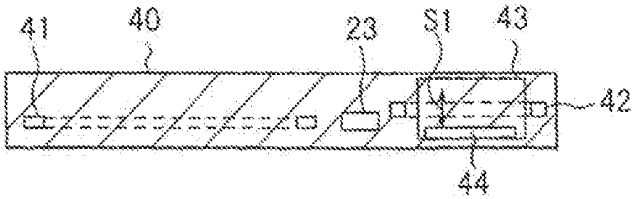


FIG. 17B



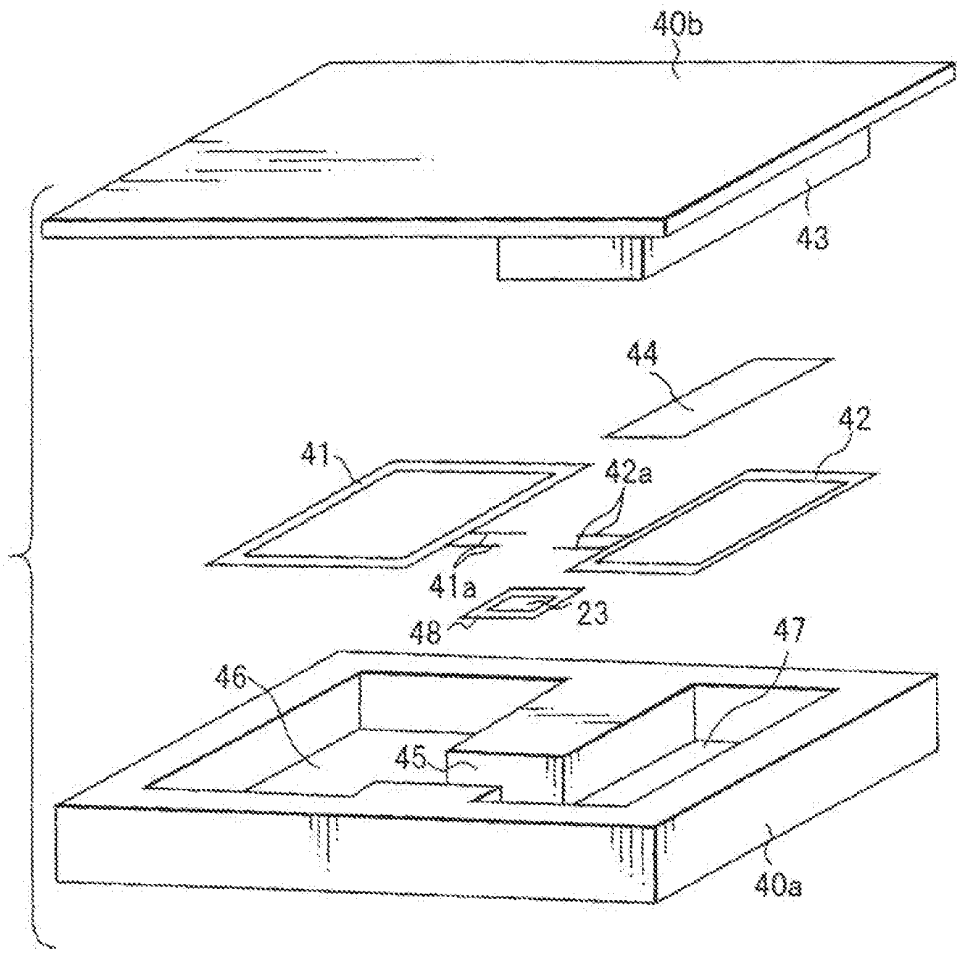


FIG. 18

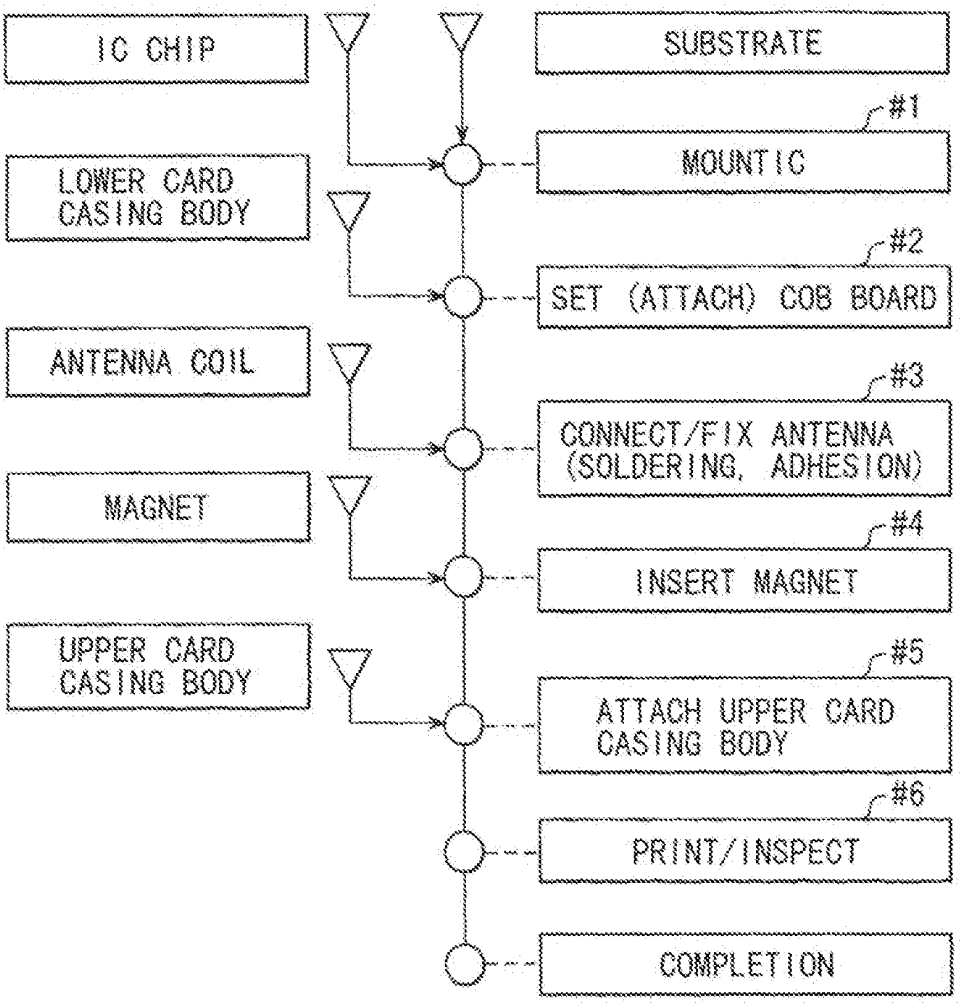

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#1
MOUNT IC
#2
SET (ATTACH) COB BOARD
#3
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#4
INSERT MAGNET
#5
ATTACH UPPER CARD CASING BODY
#6
PRINT/INSPECT
COMPLETION

FIG. 19

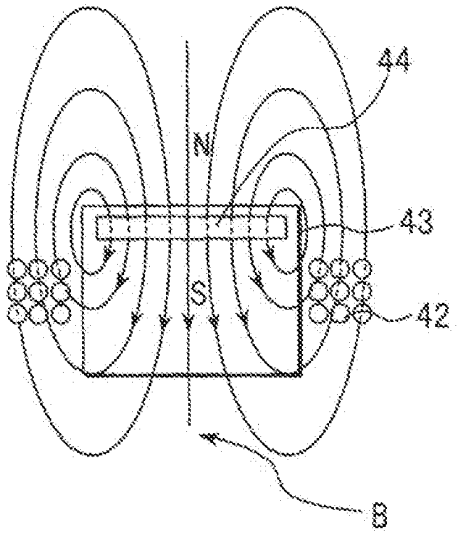


FIG. 20A

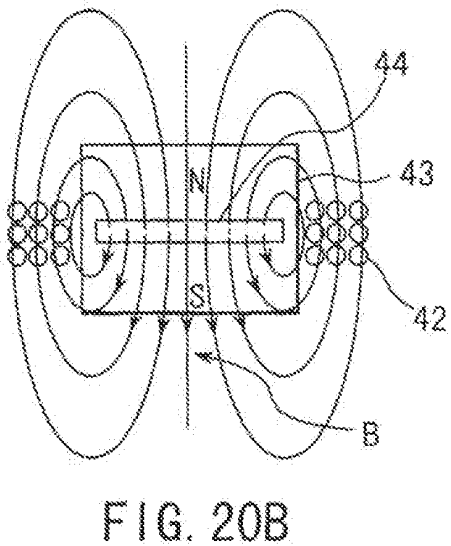


FIG. 20B

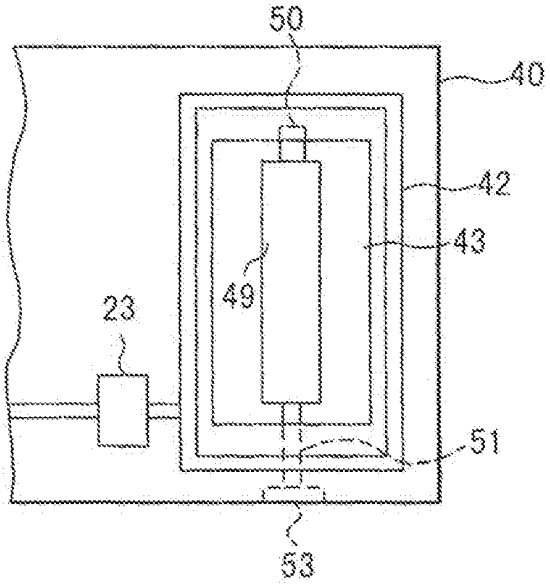


FIG. 21A

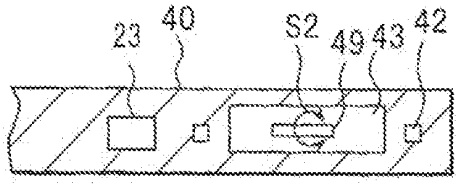


FIG. 21B

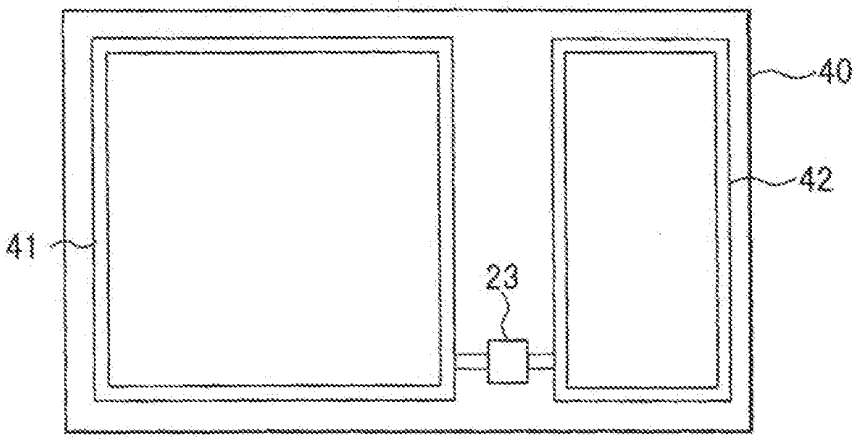


FIG. 22A

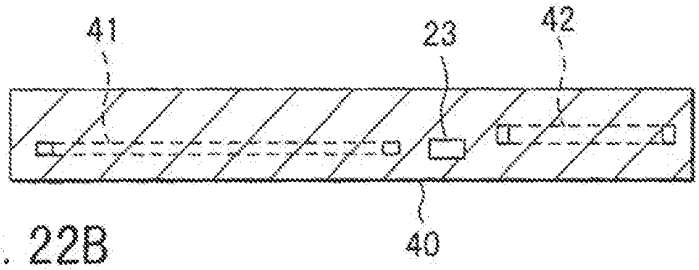


FIG. 22B

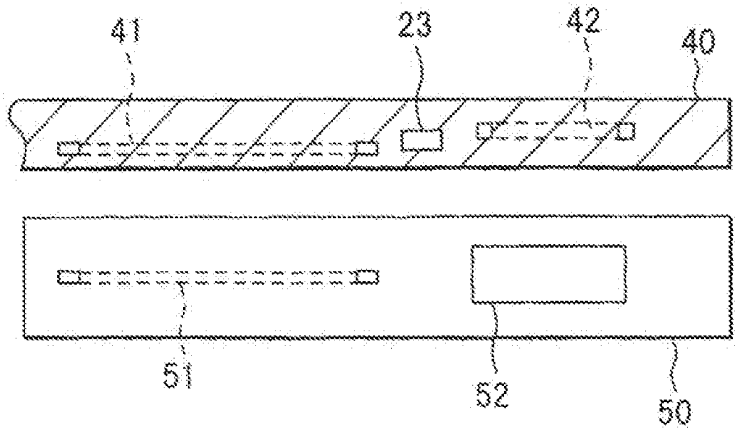


FIG. 23

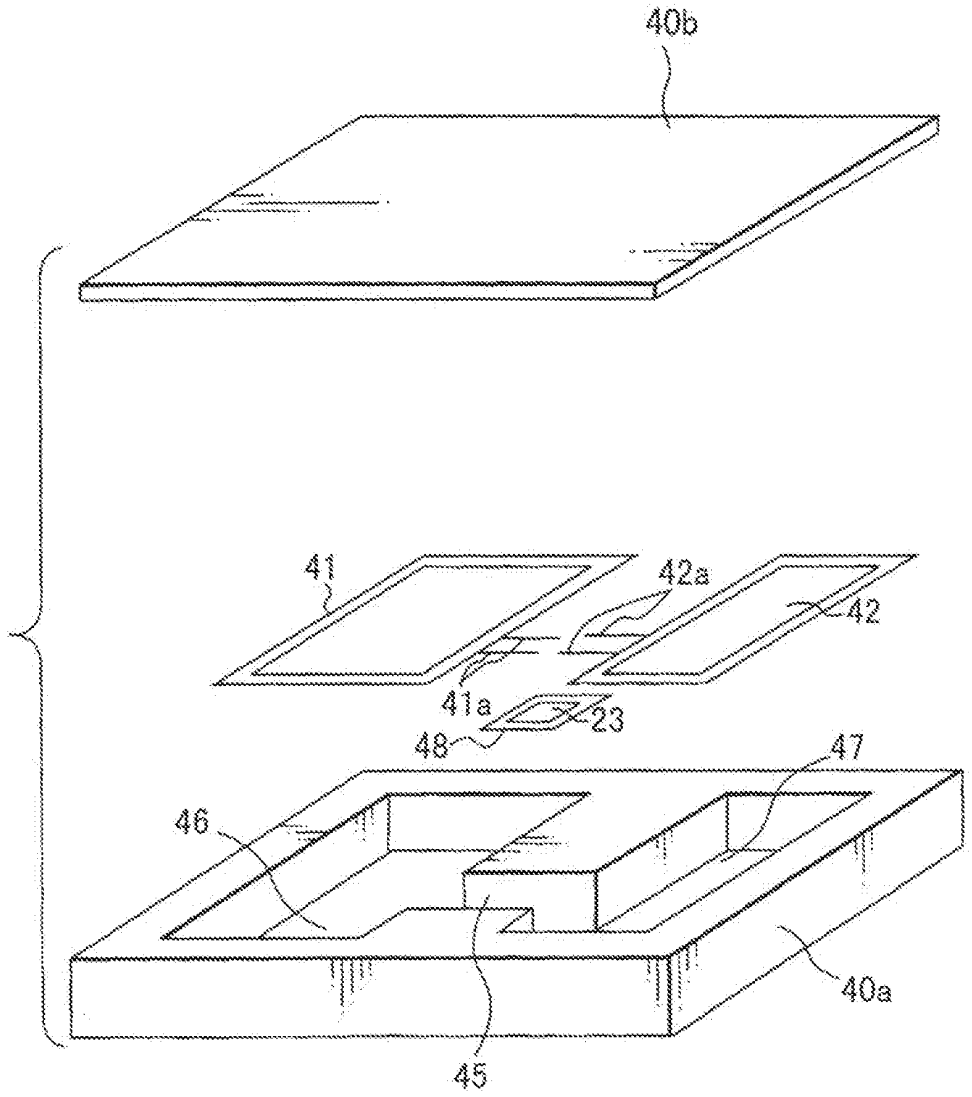


FIG. 24

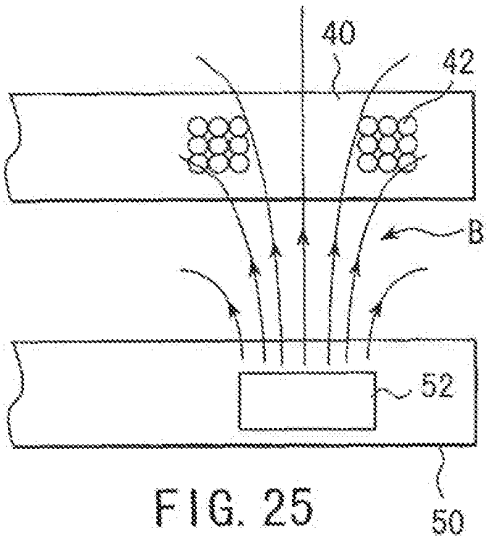


FIG. 25

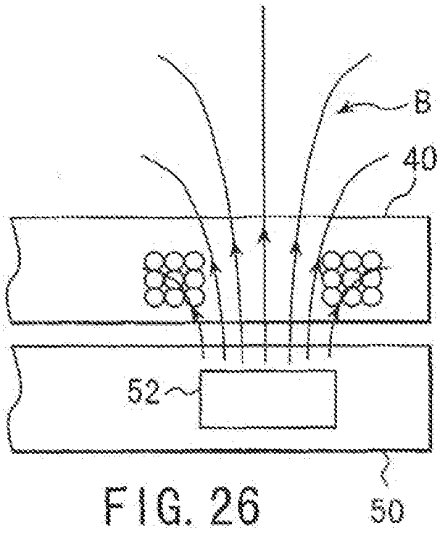


FIG. 26

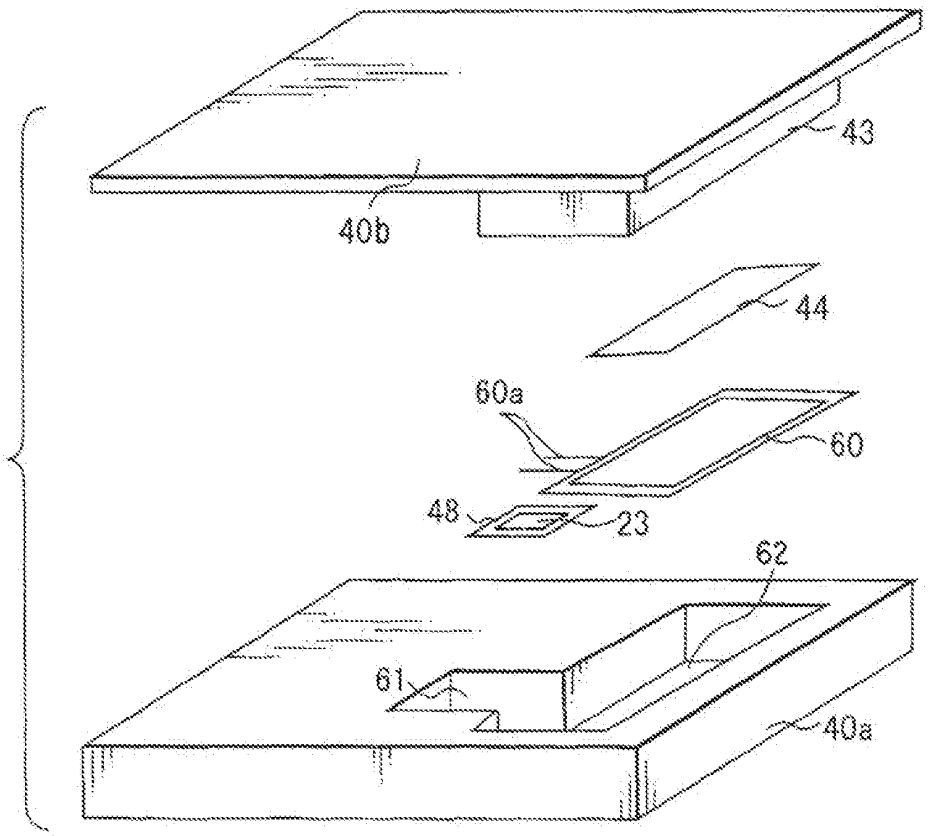


FIG. 27

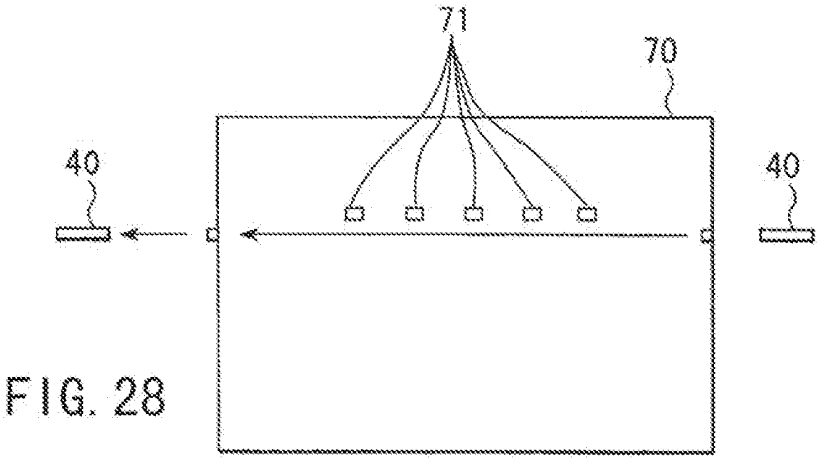


FIG. 28

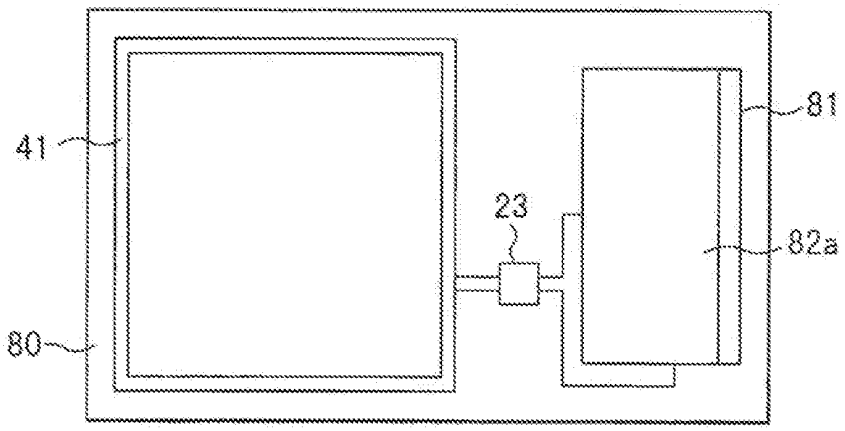


FIG. 29A

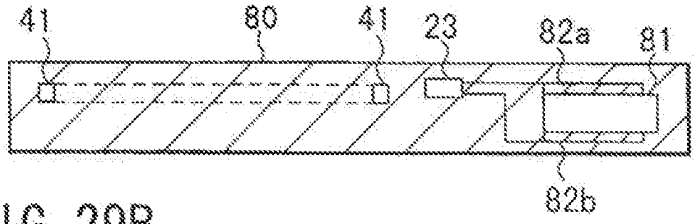


FIG. 29B

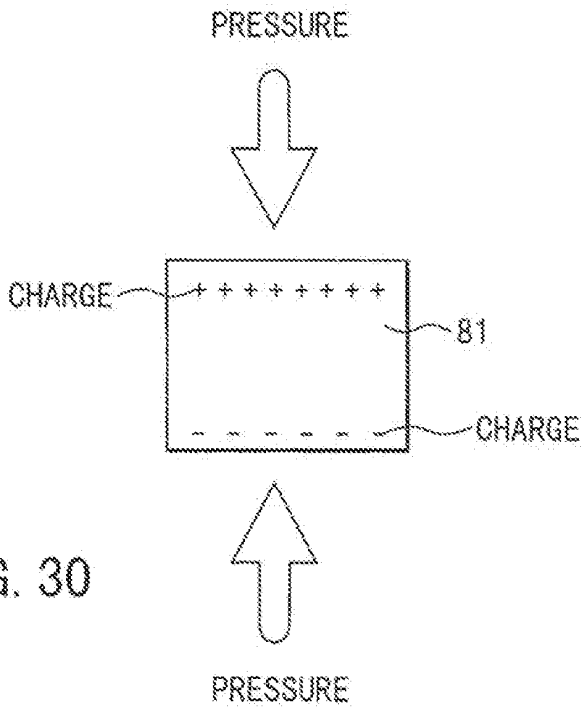


FIG. 30

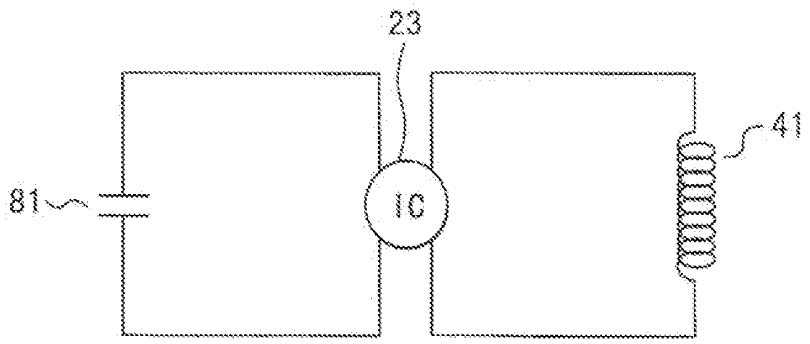


FIG. 31

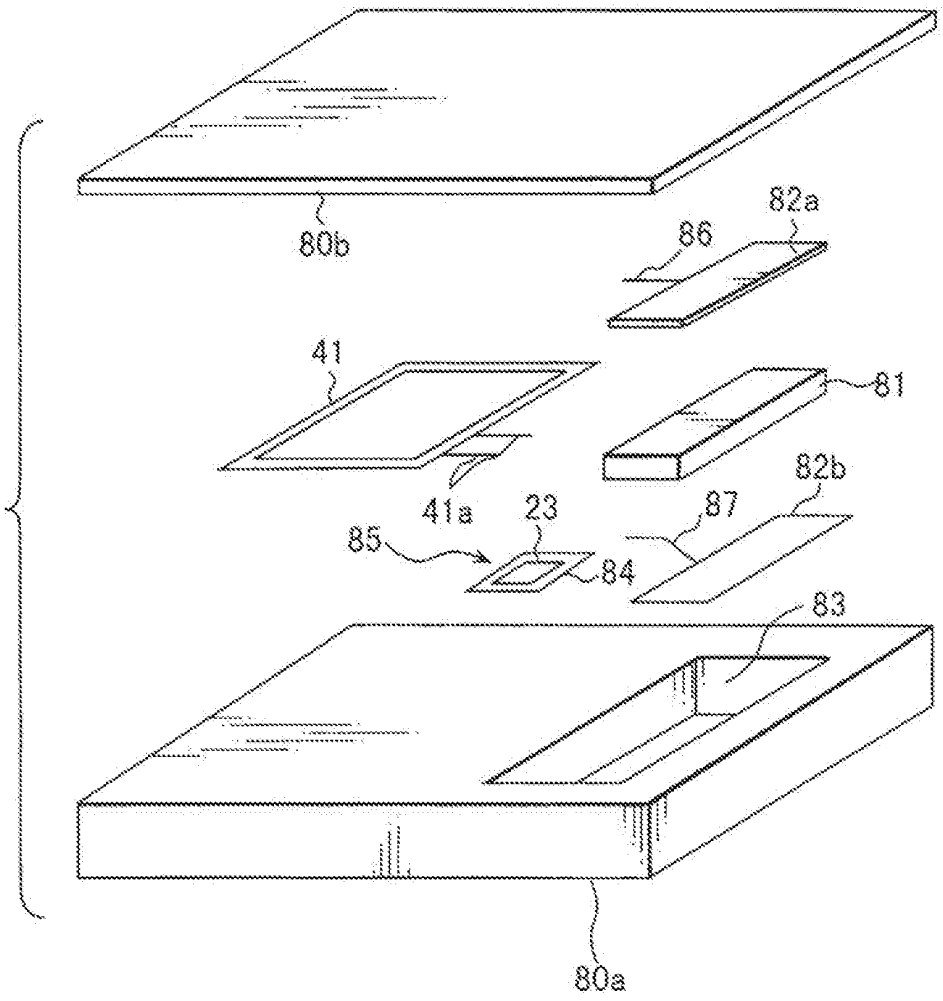


FIG. 32

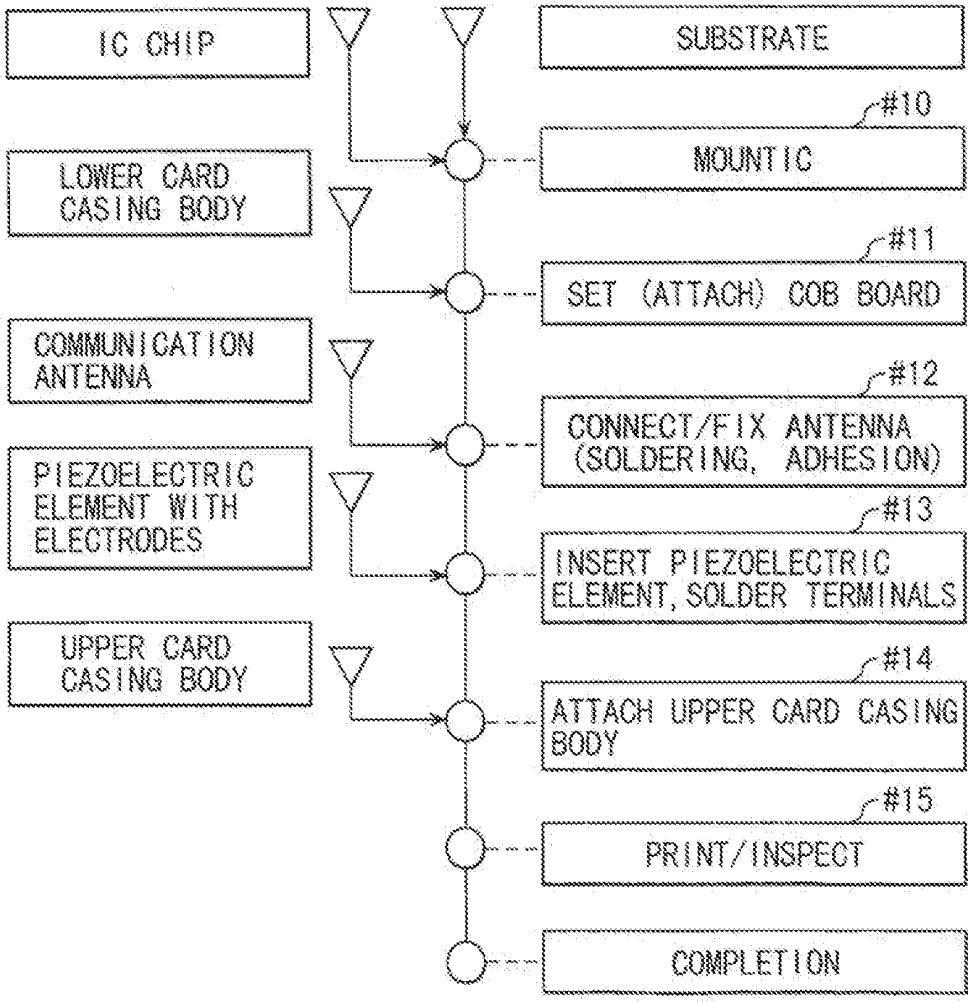

IC CHIP
LOWER CARD CASING BODY
COMMUNICATION ANTENNA
PIEZOELECTRIC ELEMENT WITH ELECTRODES
UPPER CARD CASING BODY
SUBSTRATE
#10
MOUNTIC
#11
SET (ATTACH) COB BOARD
#12
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#13
INSERT PIEZOELECTRIC ELEMENT, SOLDER TERMINALS
#14
ATTACH UPPER CARD CASING BODY
#15
PRINT/INSPECT
COMPLETION

FIG. 33

FIG. 34A

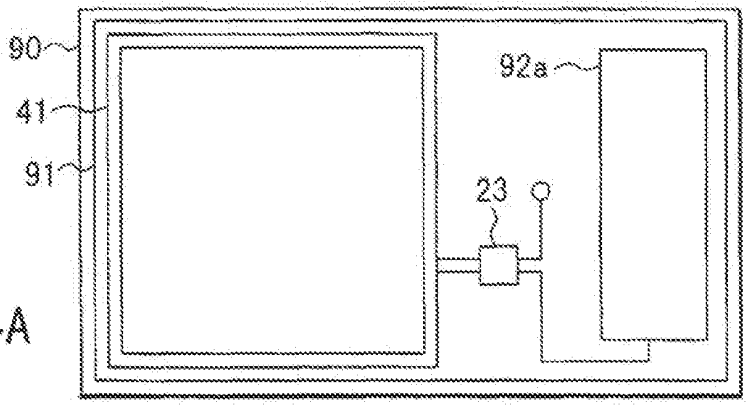


FIG. 34B

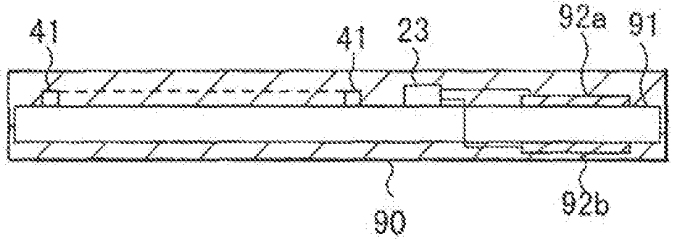
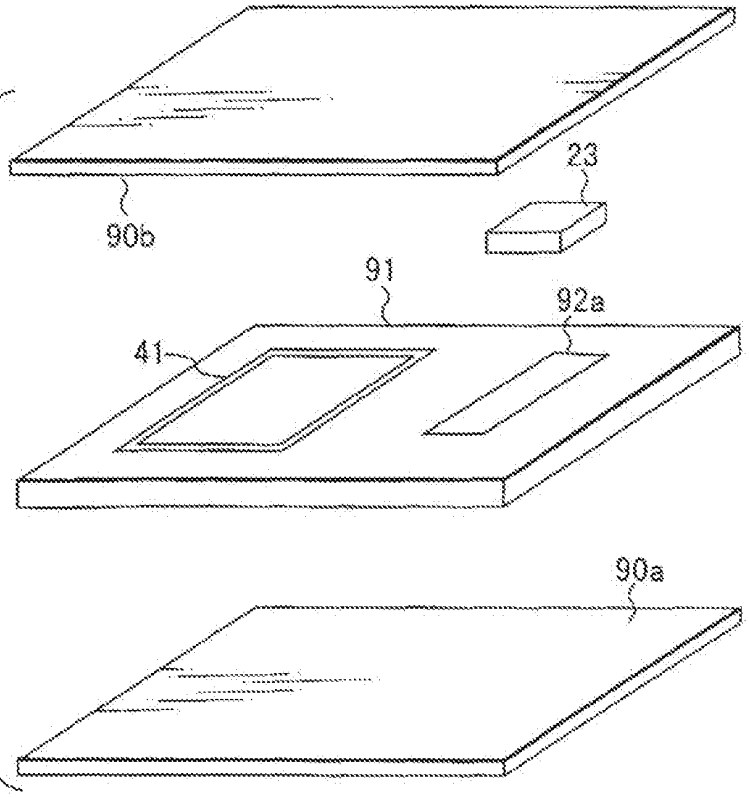


FIG. 35



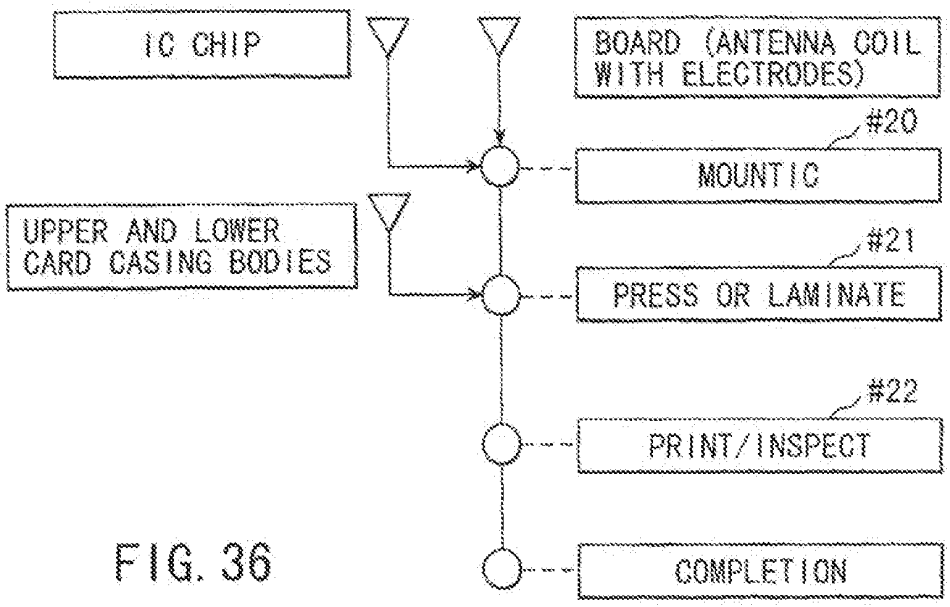


FIG. 36

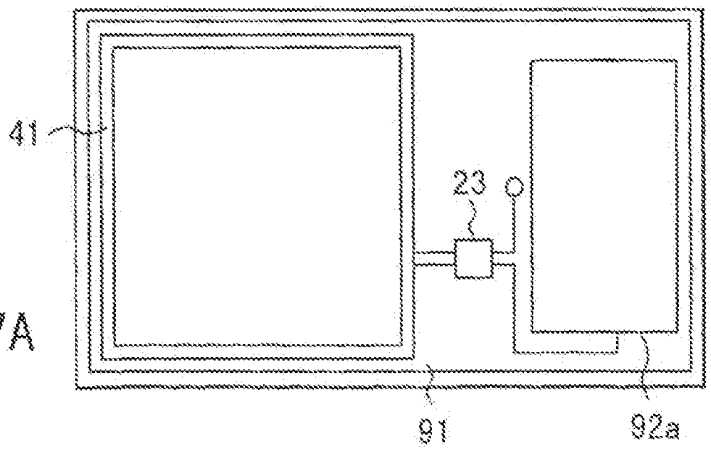


FIG. 37A

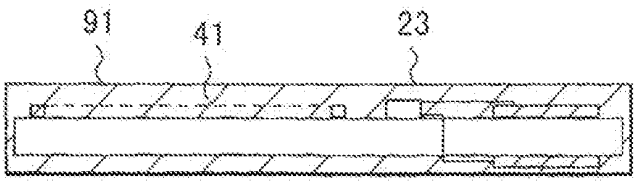


FIG. 37B

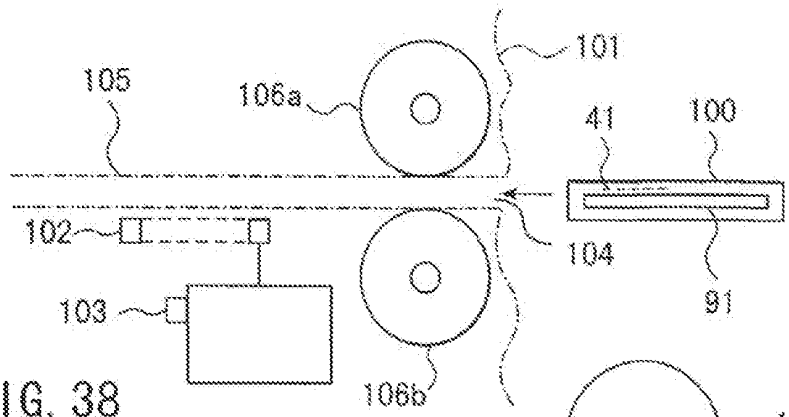


FIG. 38

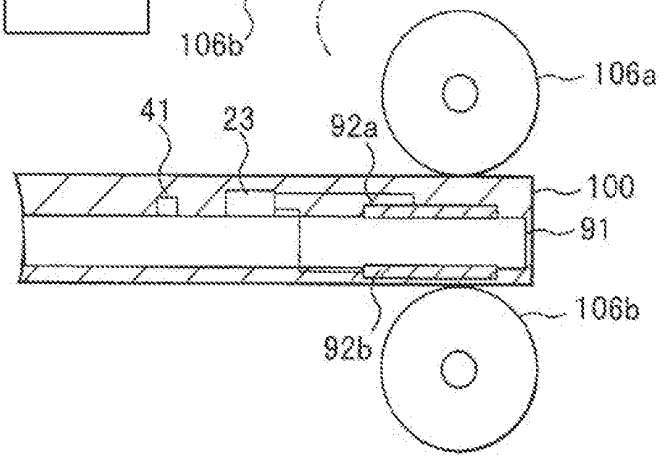


FIG. 39

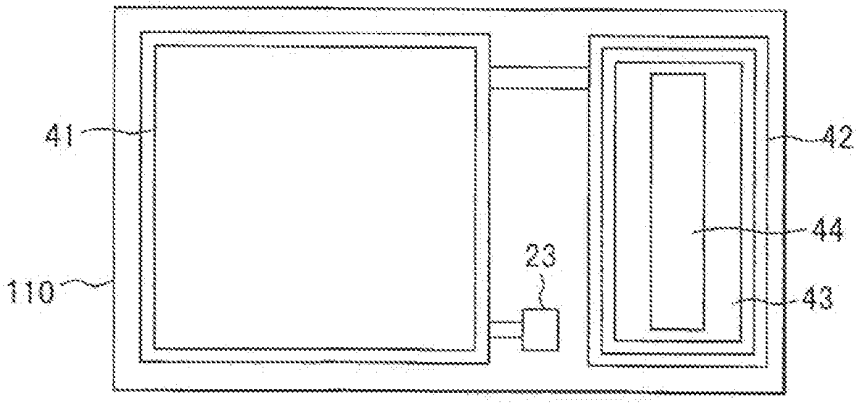


FIG. 40A

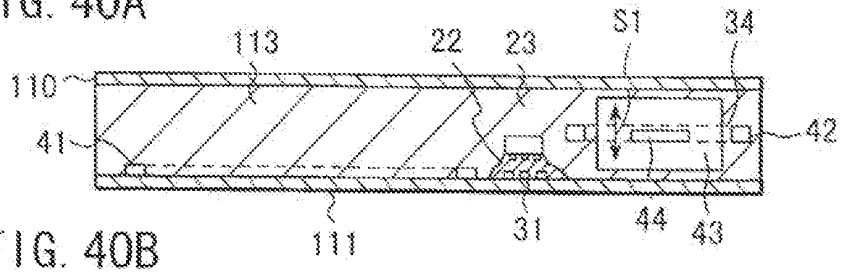


FIG. 40B

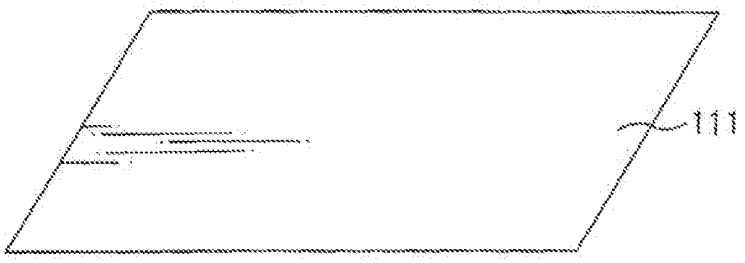


FIG. 41A

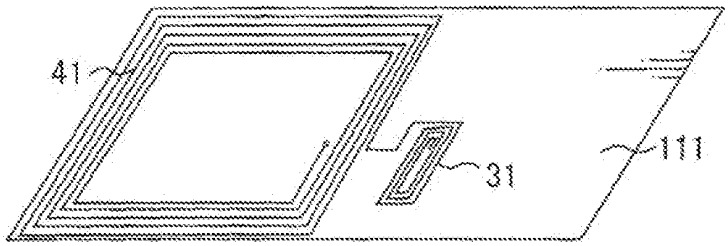


FIG. 41B

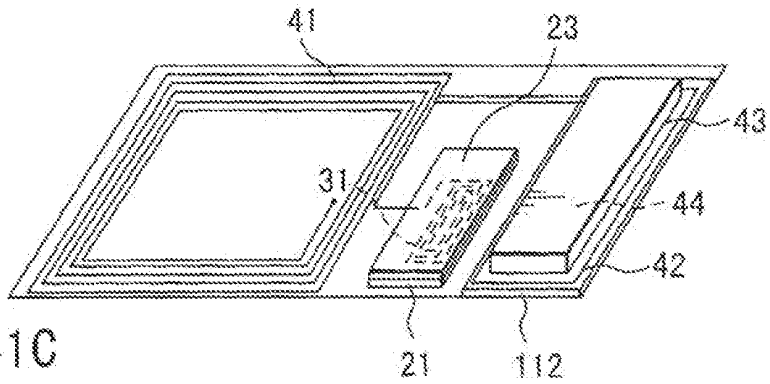


FIG. 41C

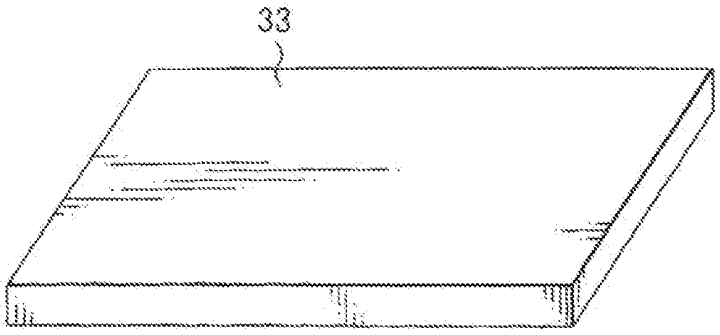
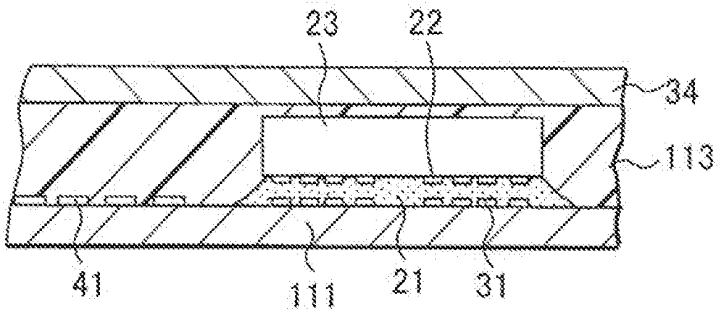


FIG. 41D

FIG. 42


23
22
34
113
41
111
21
31

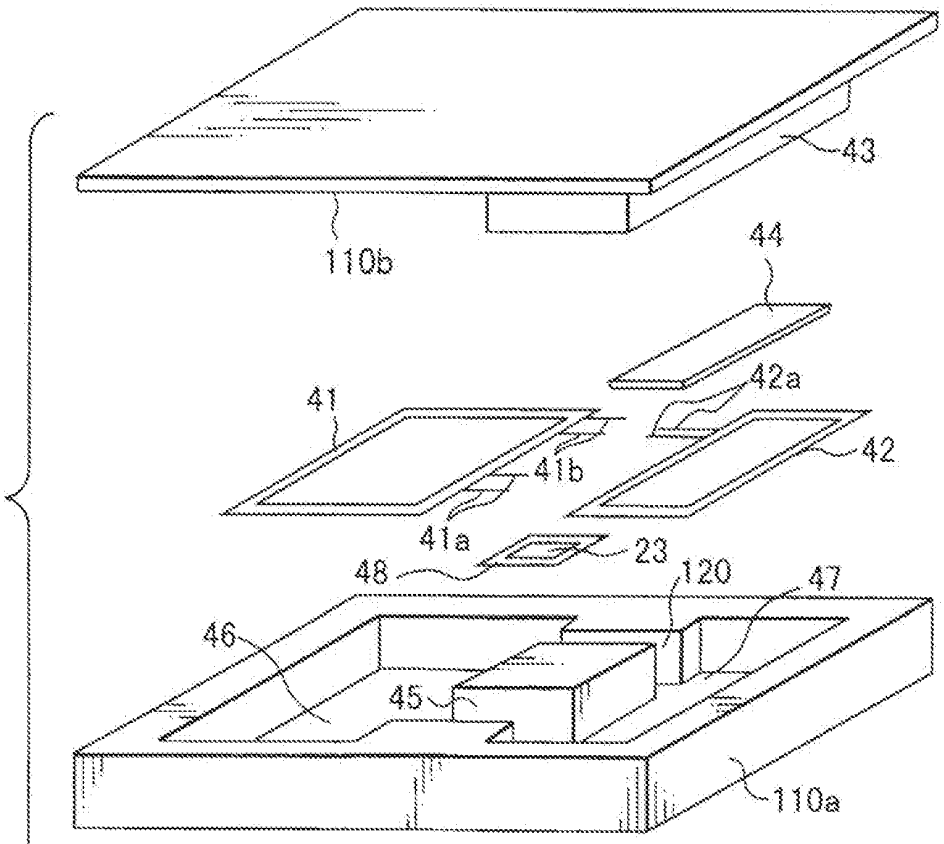

43
110b
44
42a
41
42
41b
41a
23
48
120
47
46
45
110a

FIG. 43

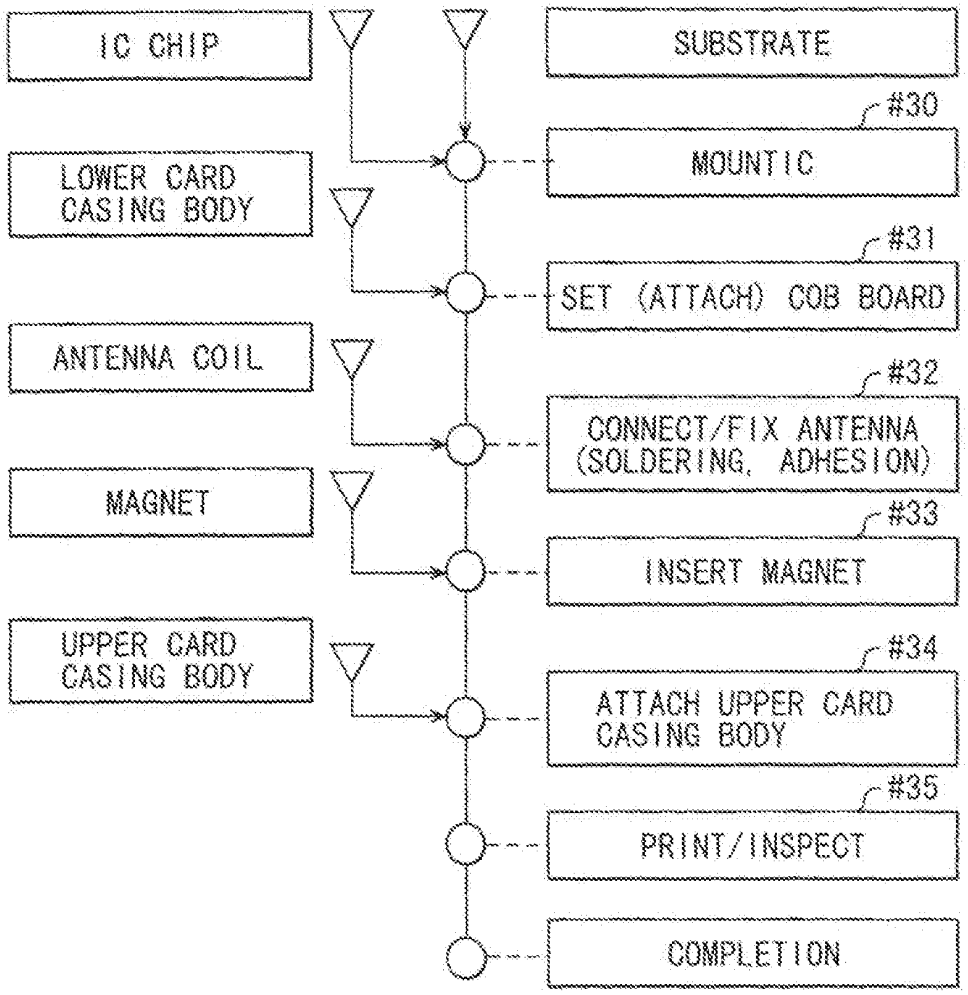

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#30
MOUNT IC
#31
SET (ATTACH) COB BOARD
#32
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#33
INSERT MAGNET
#34
ATTACH UPPER CARD CASING BODY
#35
PRINT/INSPECT
COMPLETION

FIG. 44

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Francisco Martinez de Velasco Cortina	Nonprovisional Application Number (if known):	
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /li zhang/	Date March 16, 2015
Name (Print/Typed) Li Zhang	Practitioner Registration Number 70902

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☐ *Total of _____ forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

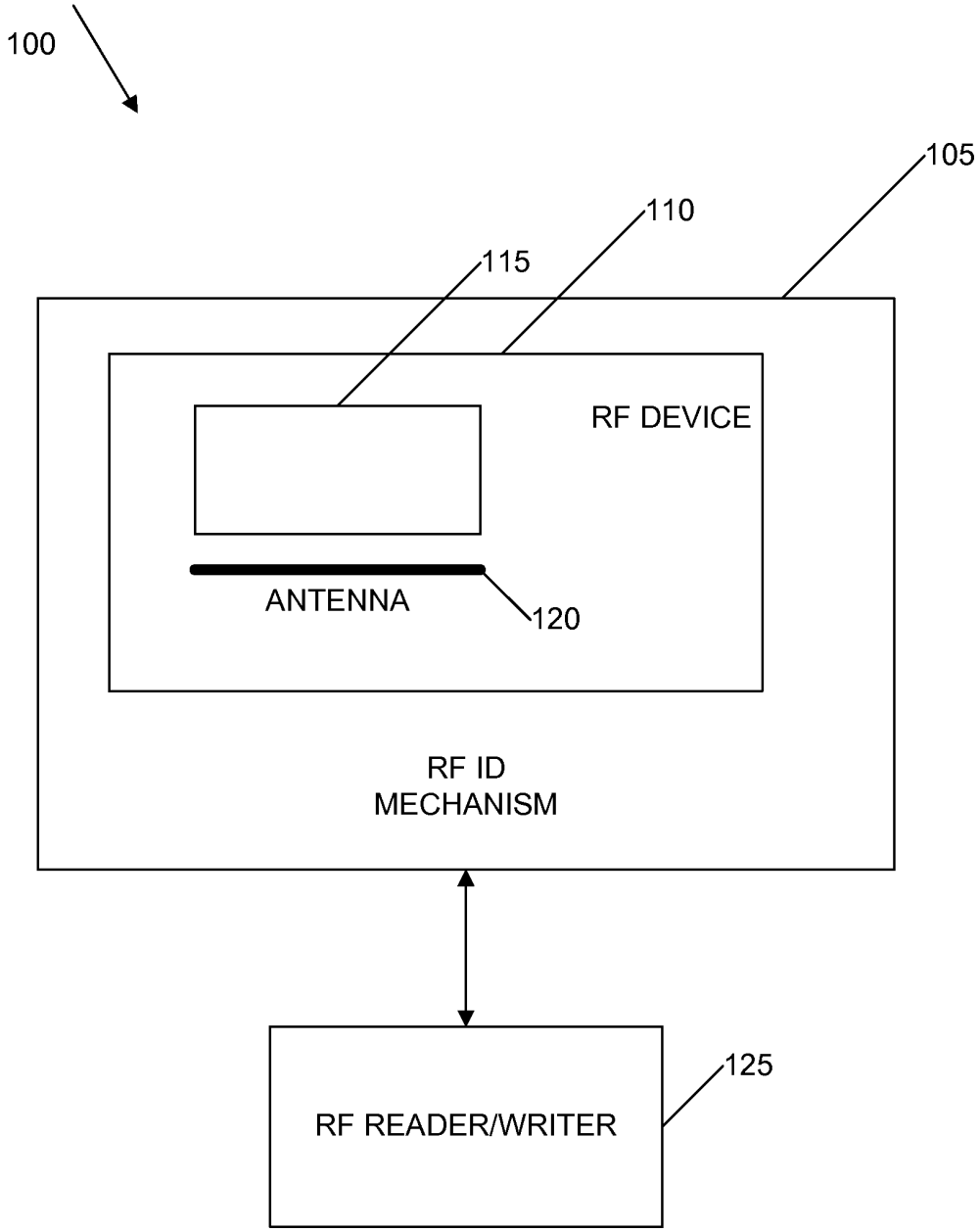

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

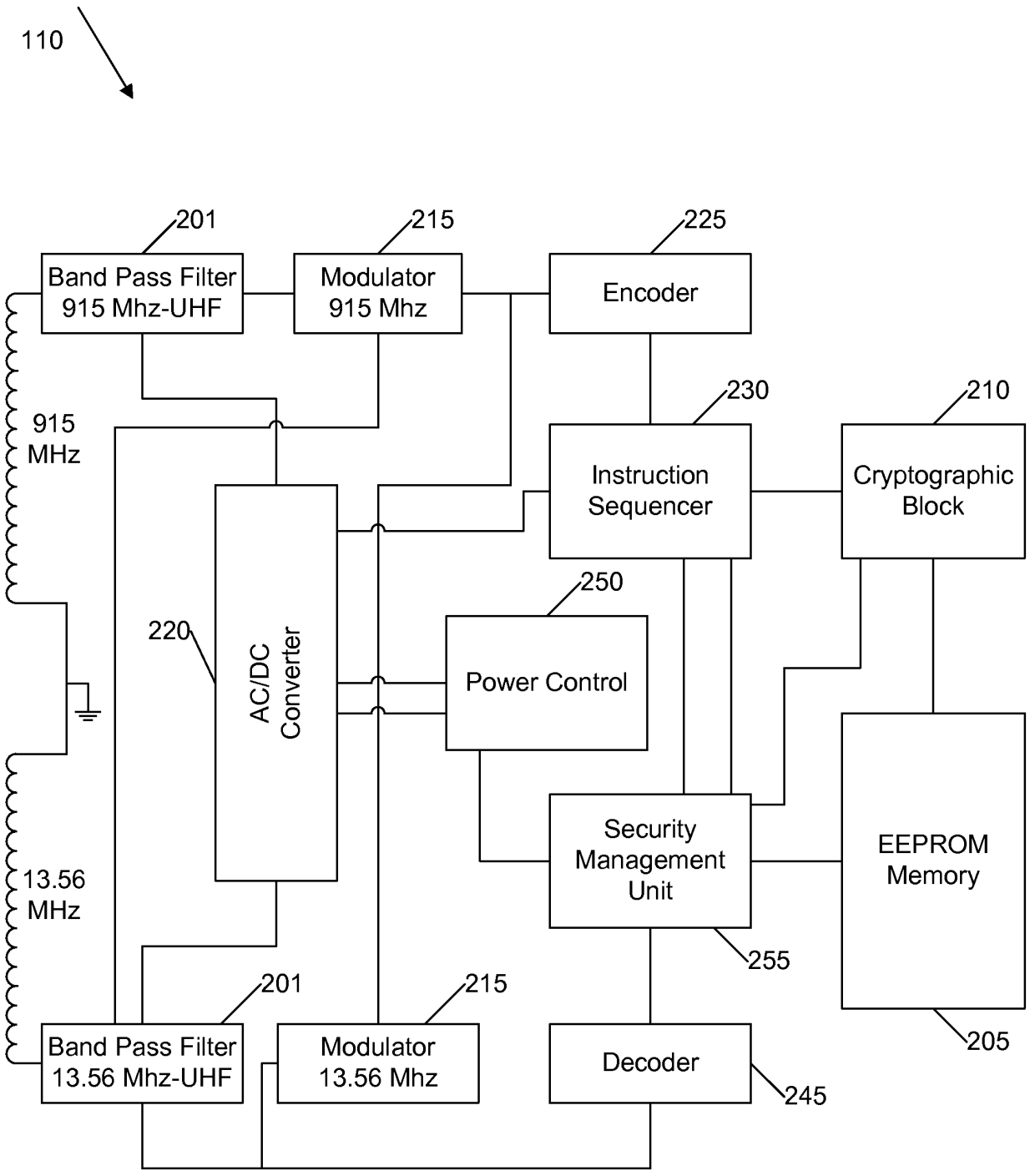

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
13.56
MHz
Security
Management
Unit
EEPROM
Memory
255
201
215
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
205
245

FIG. 2

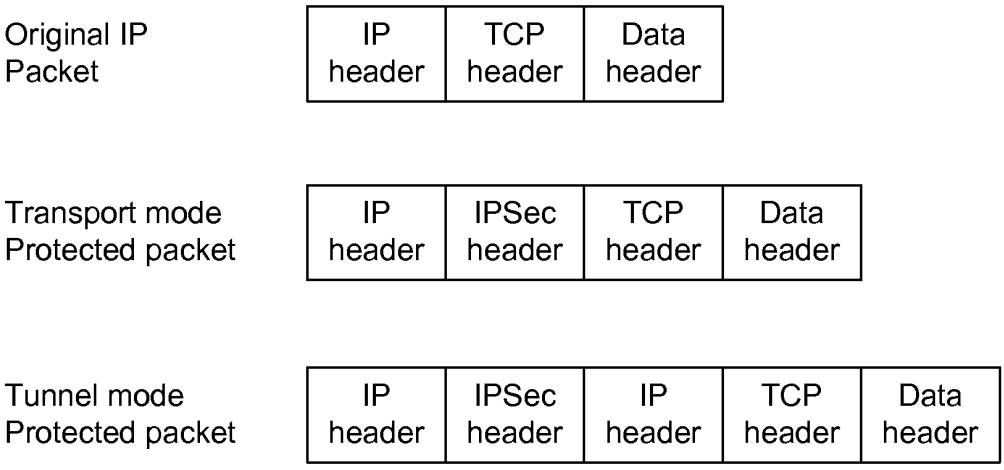

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

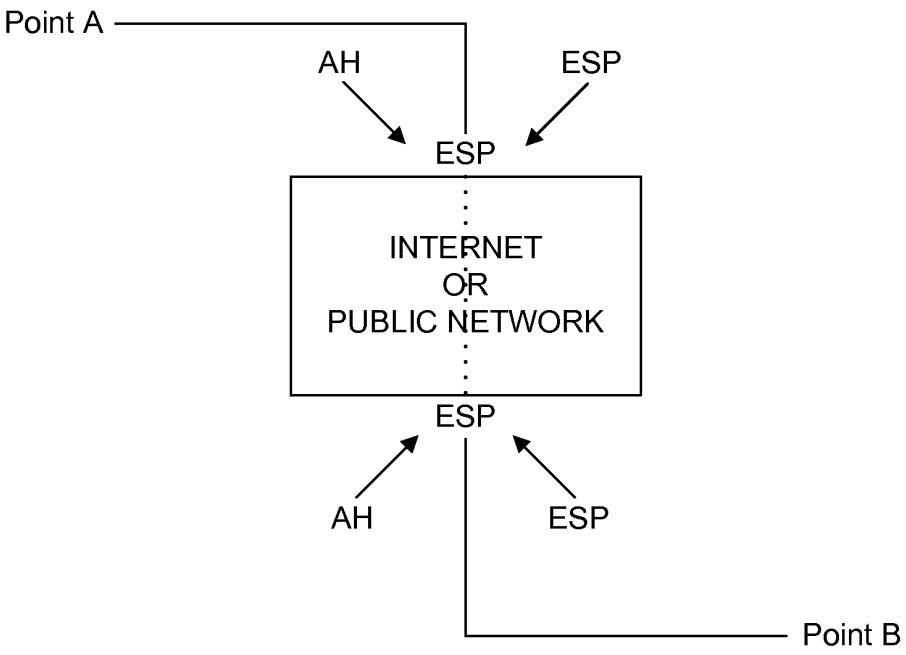

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

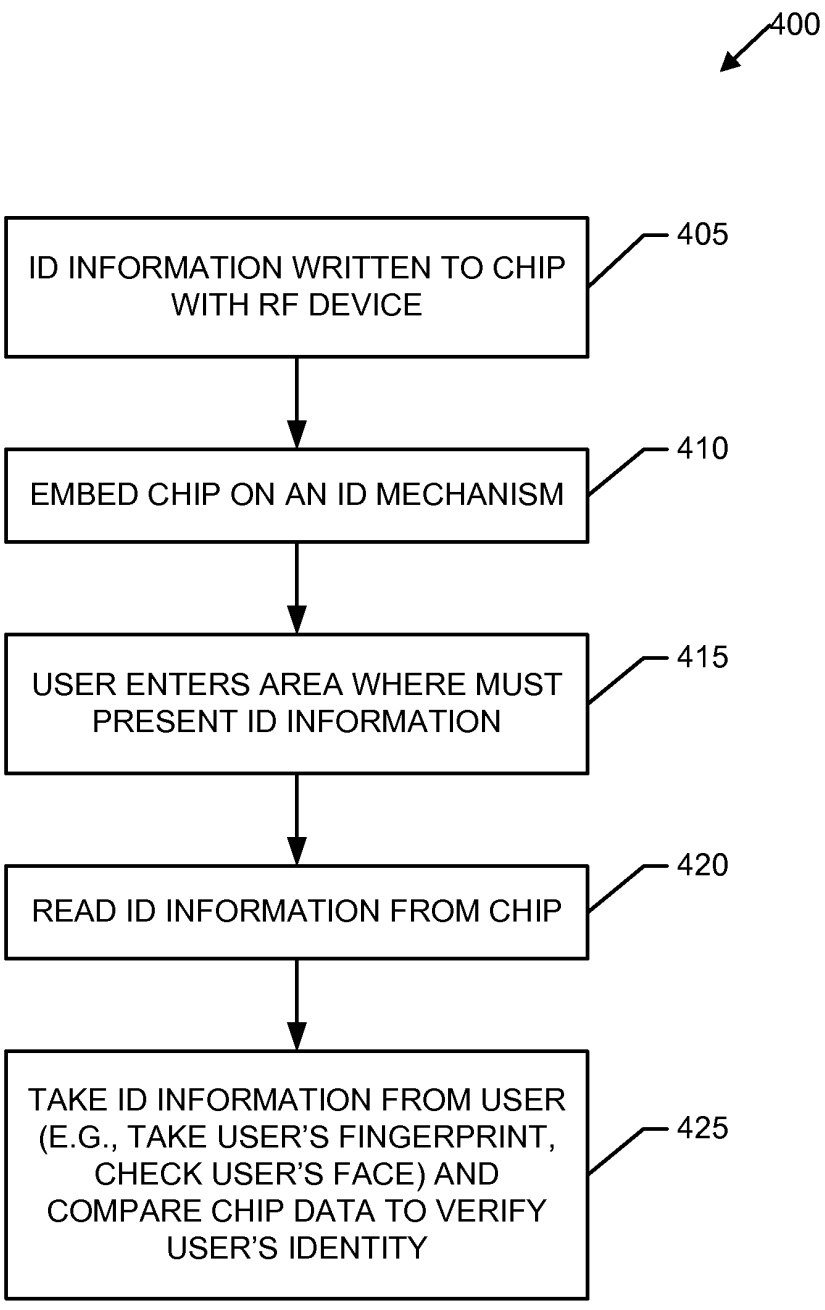

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY
425

FIG. 4

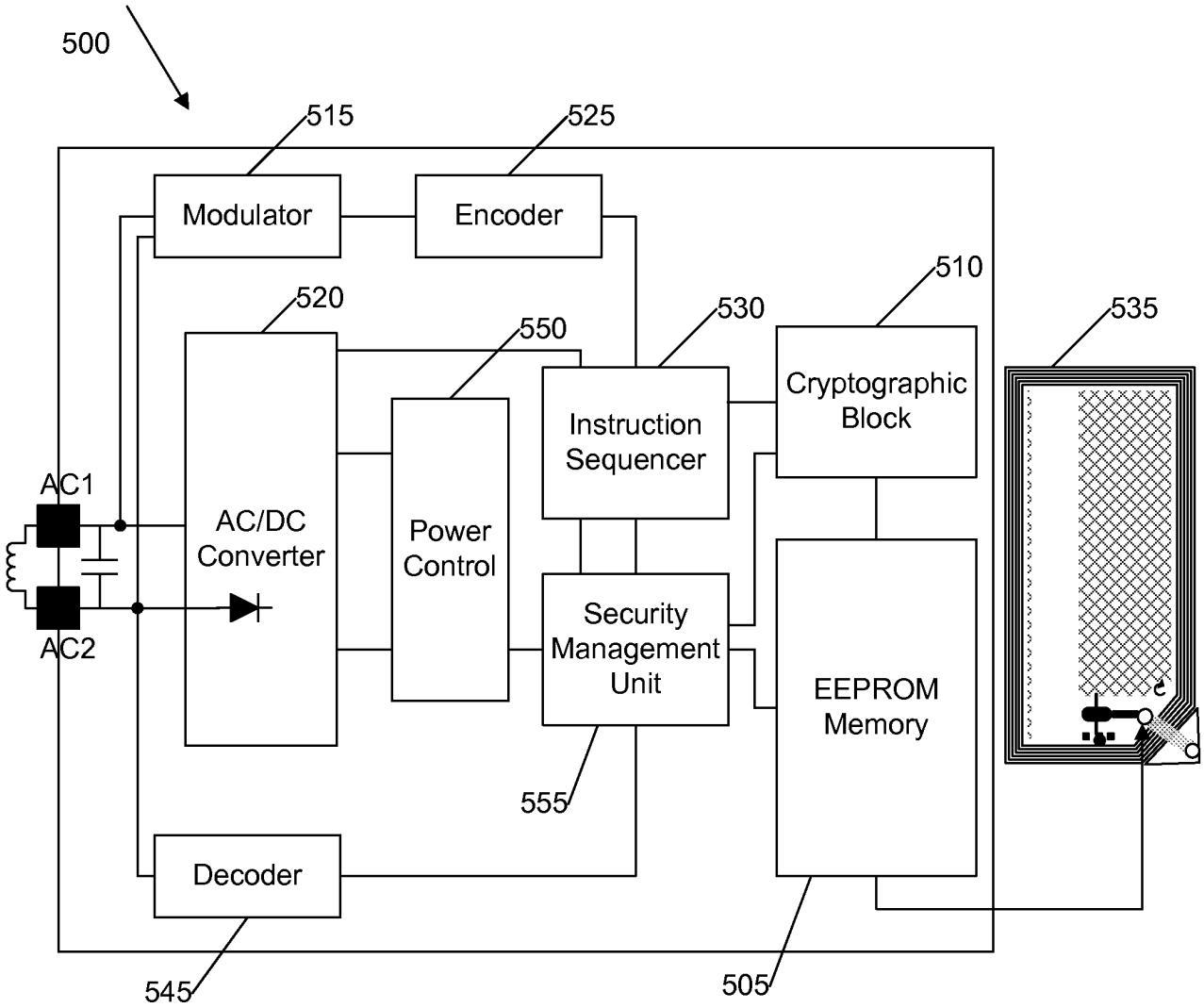

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

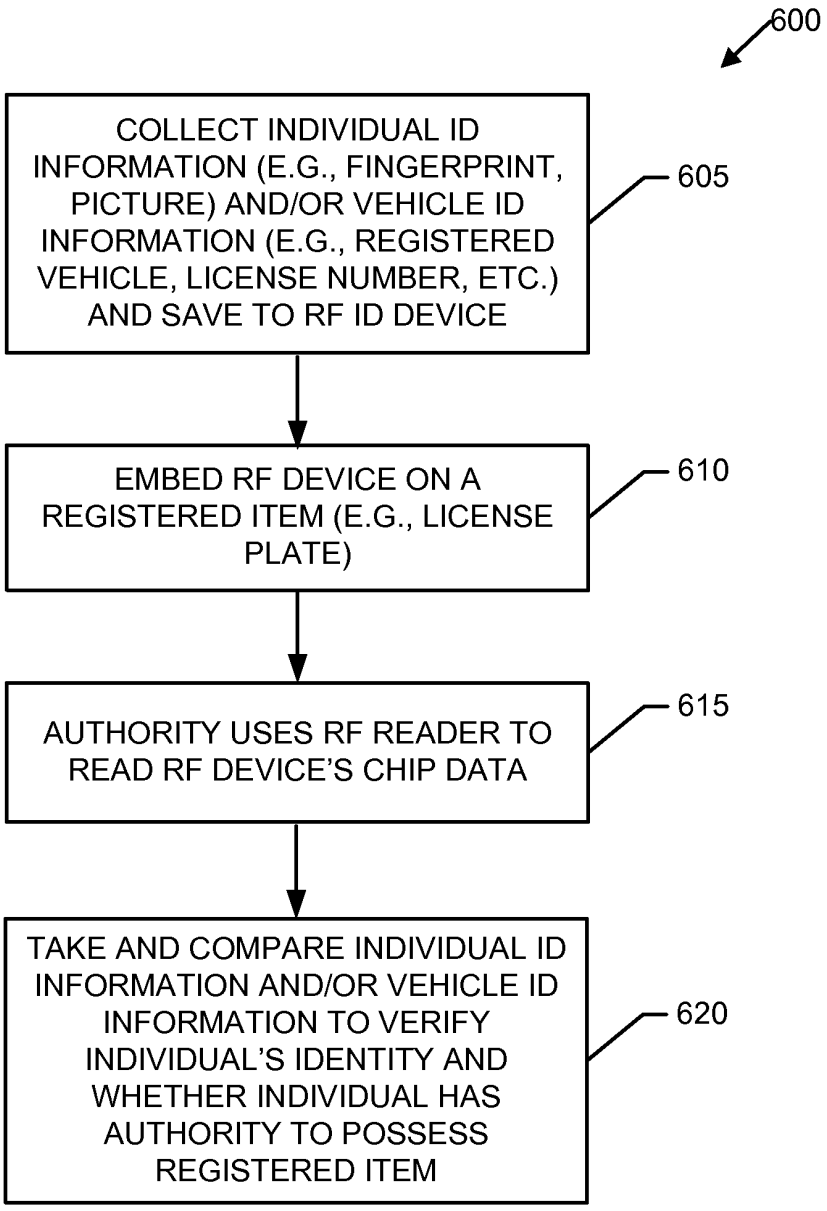

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE AND COMPARE INDIVIDUAL ID INFORMATION AND/OR VEHICLE ID INFORMATION TO VERIFY INDIVIDUAL'S IDENTITY AND WHETHER INDIVIDUAL HAS AUTHORITY TO POSSESS REGISTERED ITEM
620

FIG. 6

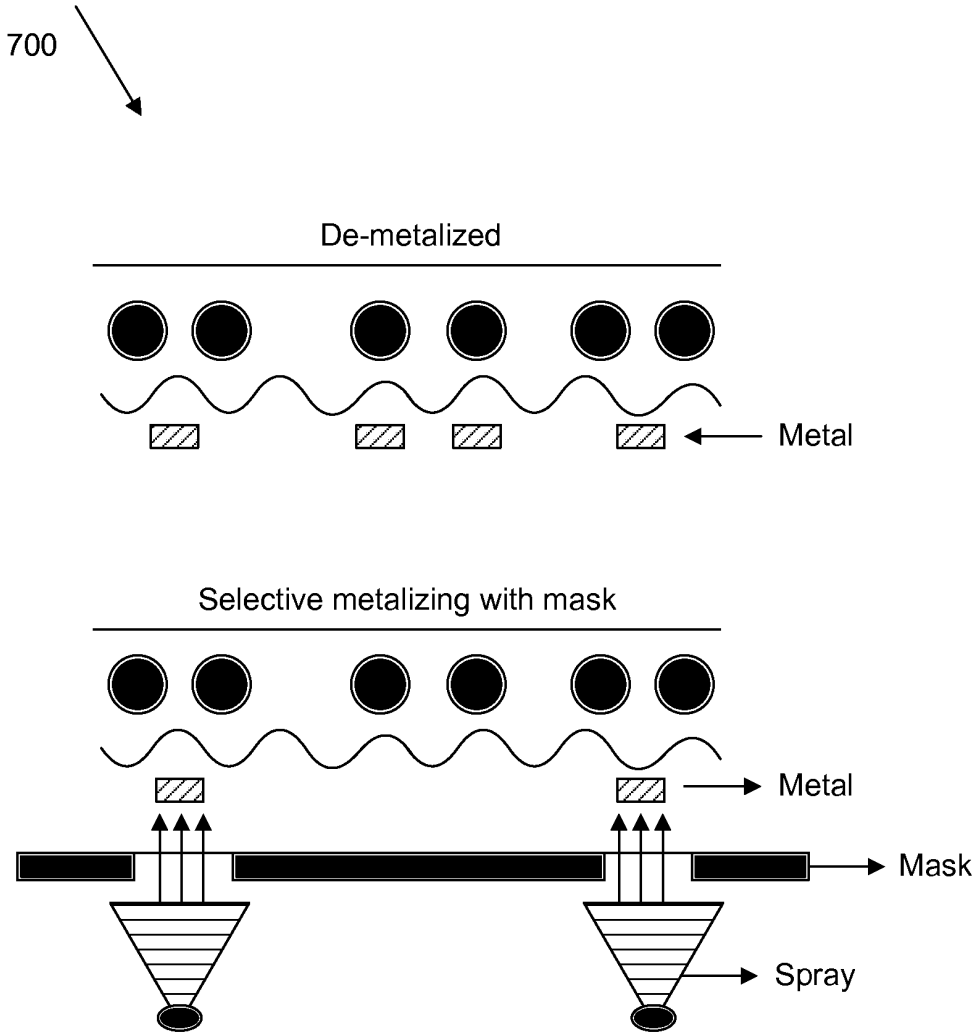

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

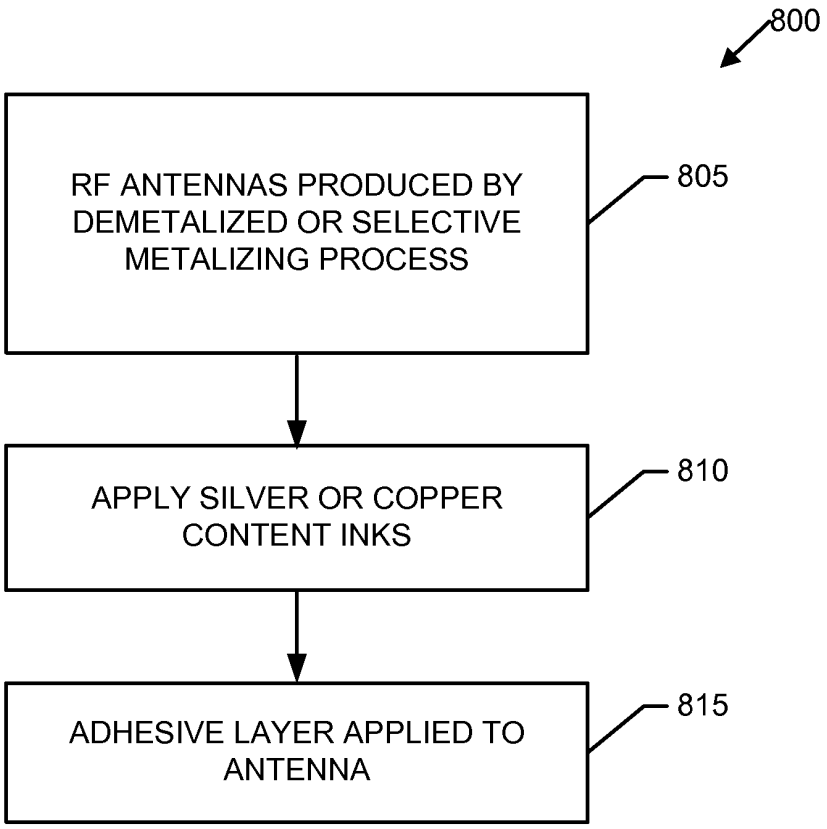

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

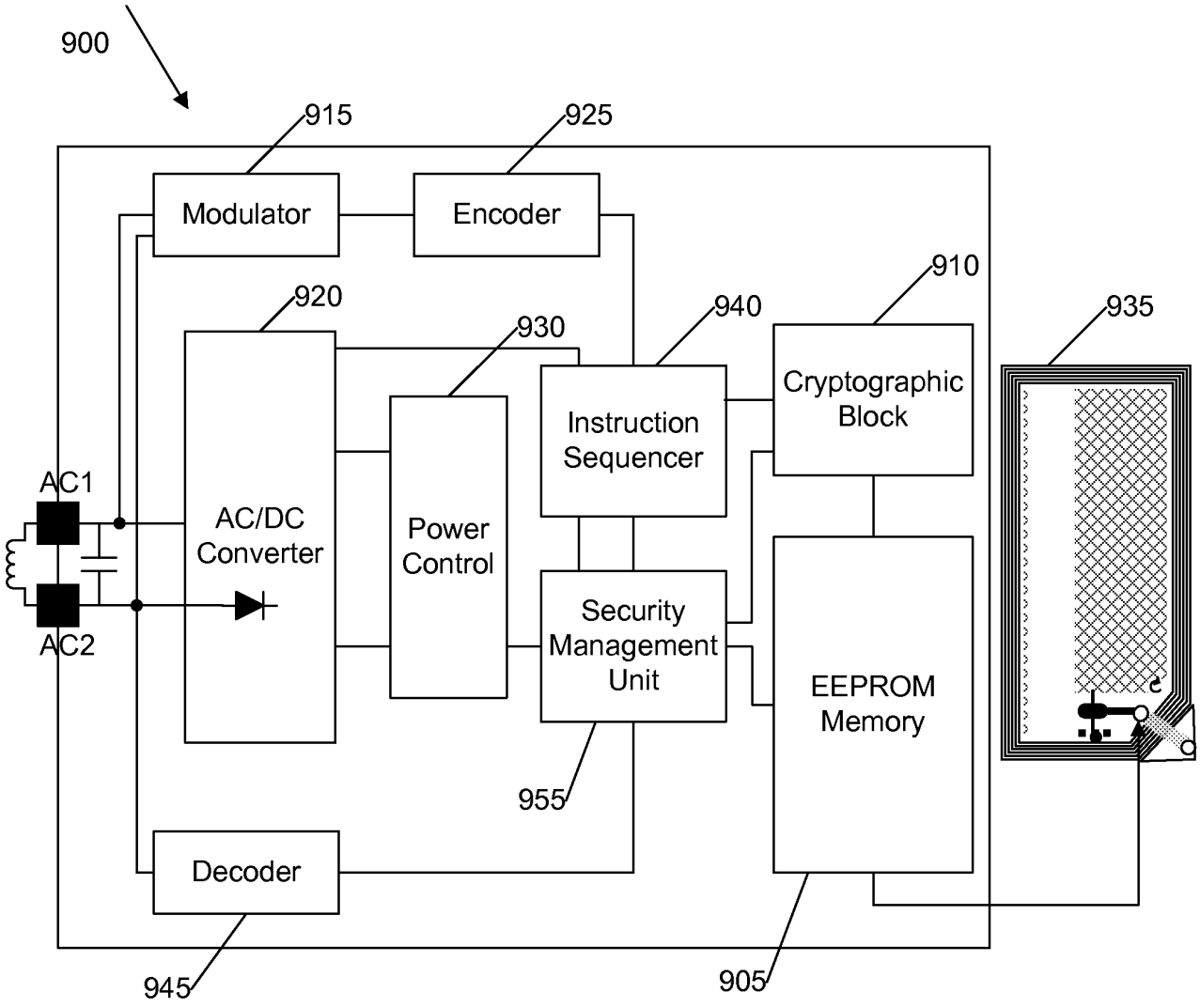

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

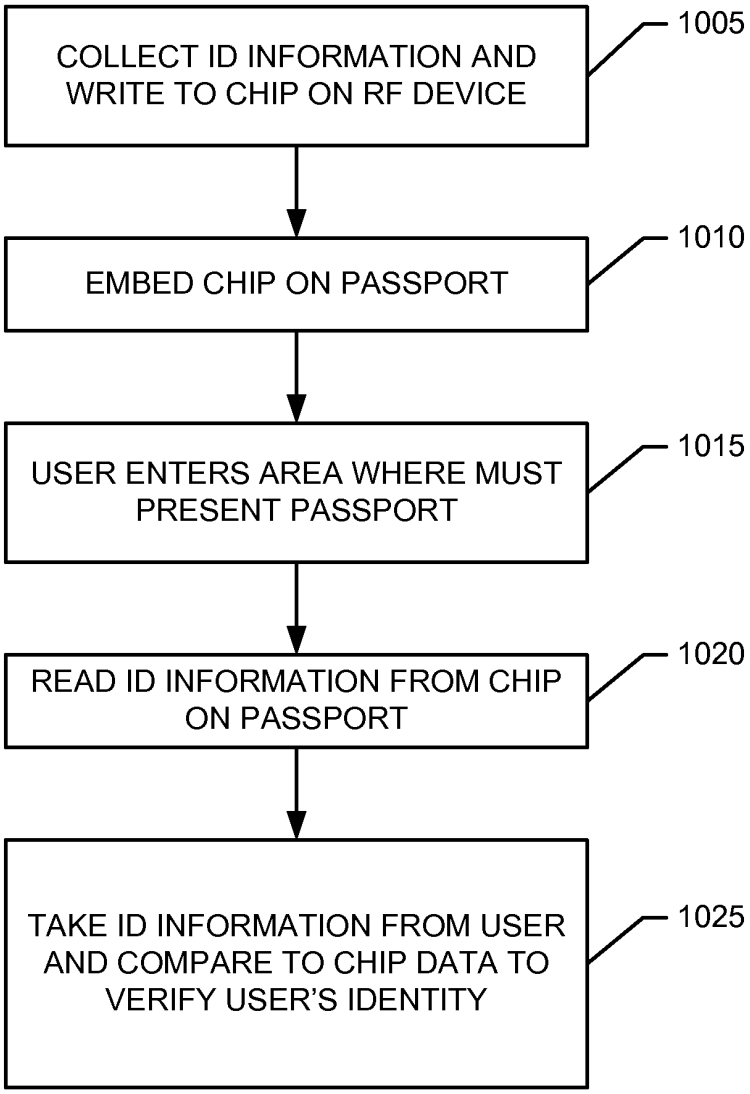

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

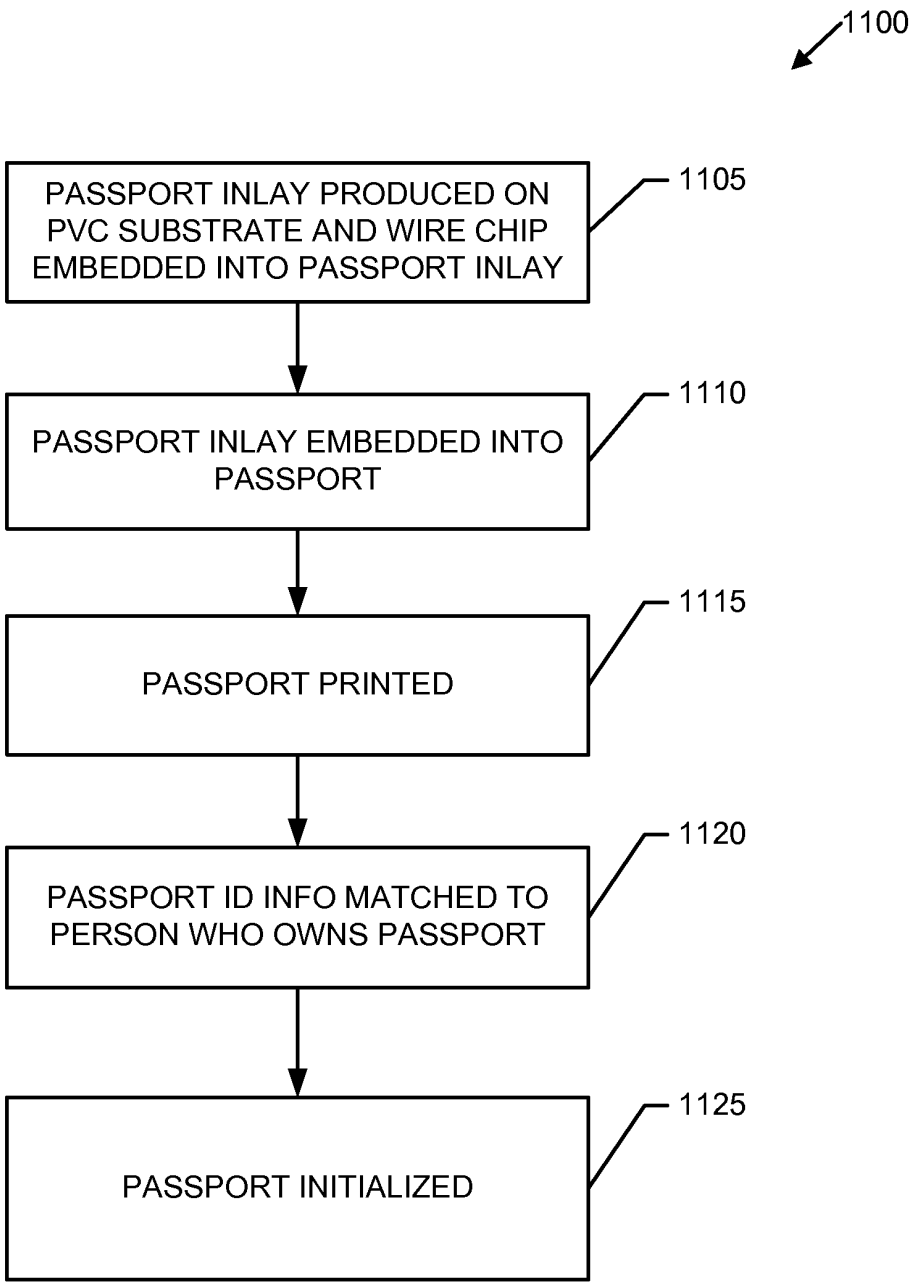

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

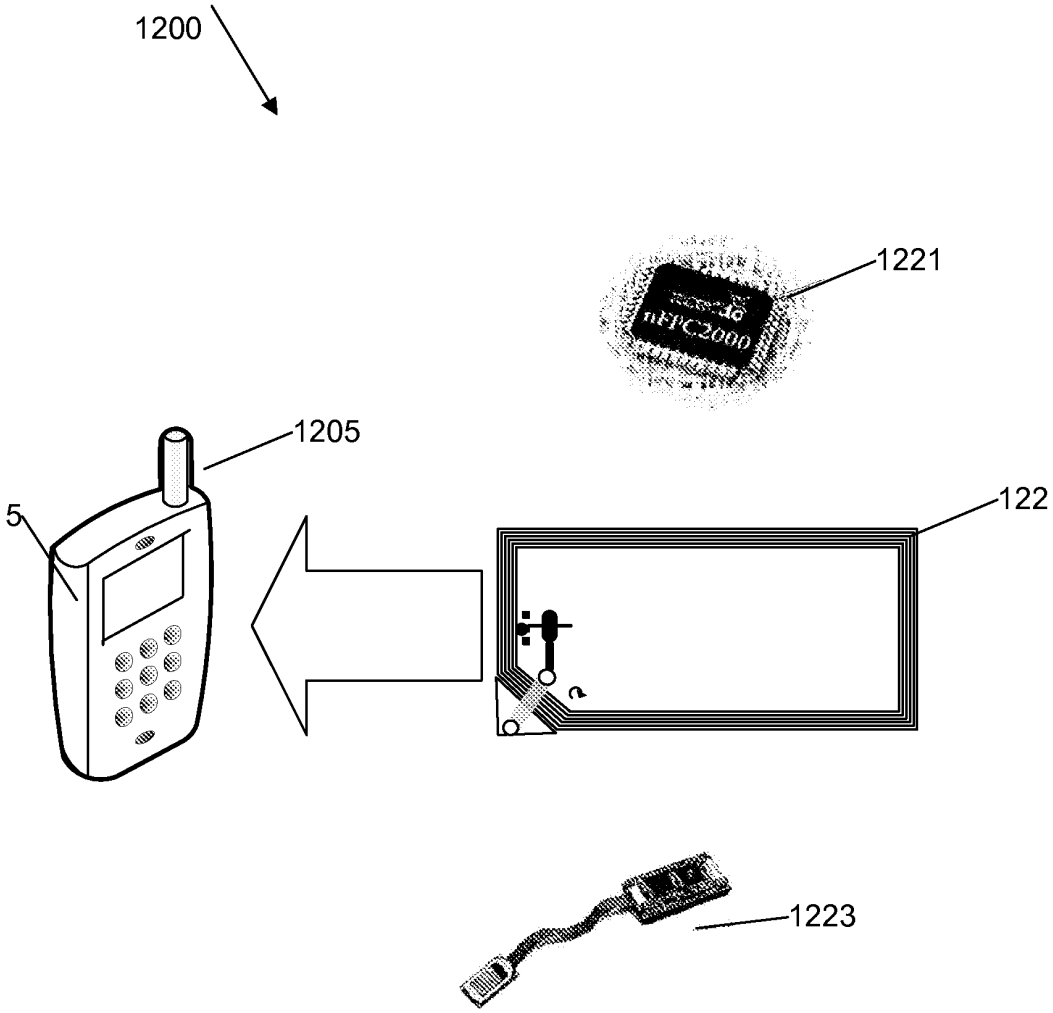


FIG. 12

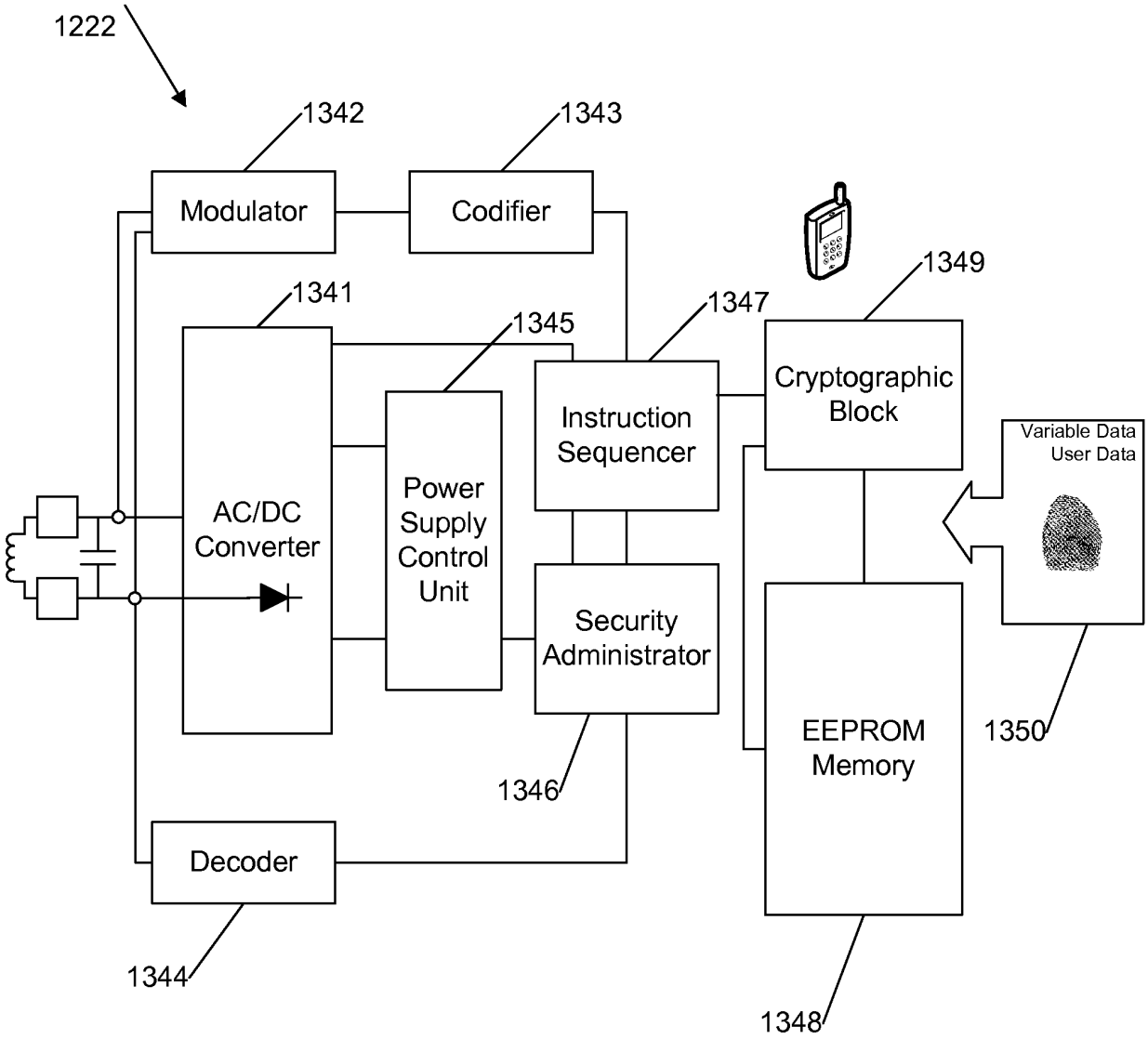

1222
1342
1343
Modulator
Codifier
1349
1341
1345
1347
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

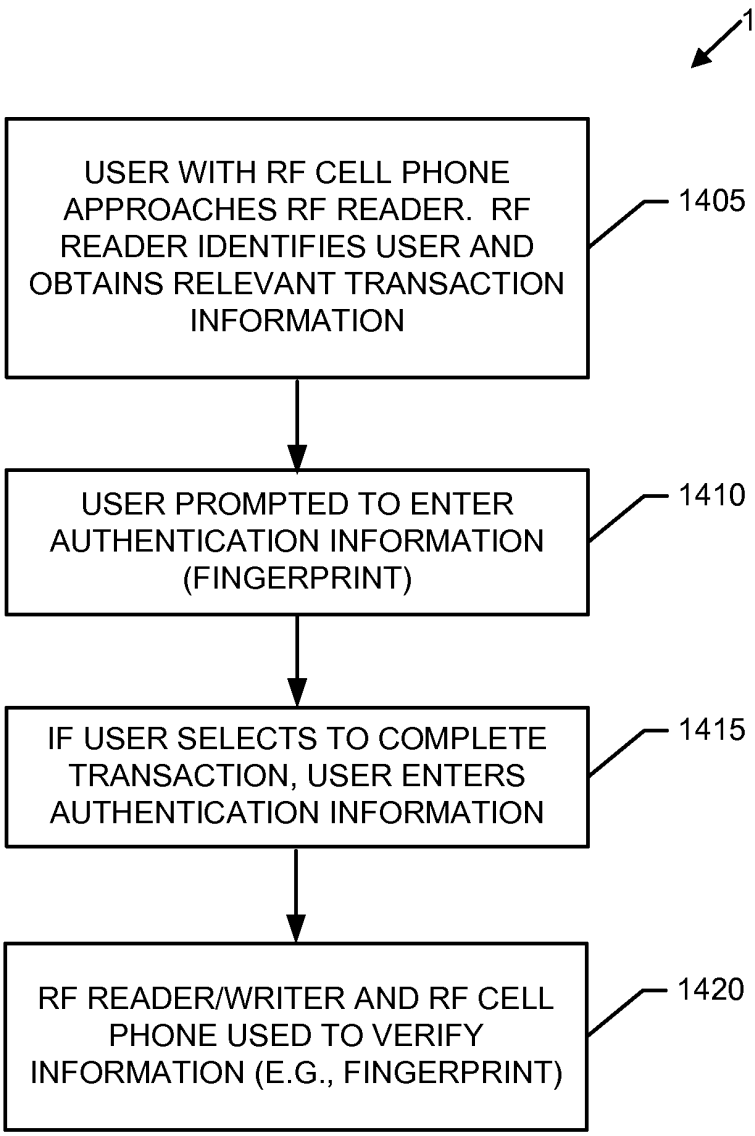

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND RF CELL PHONE USED TO VERIFY INFORMATION (E.G., FINGERPRINT)
1420

FIG. 14

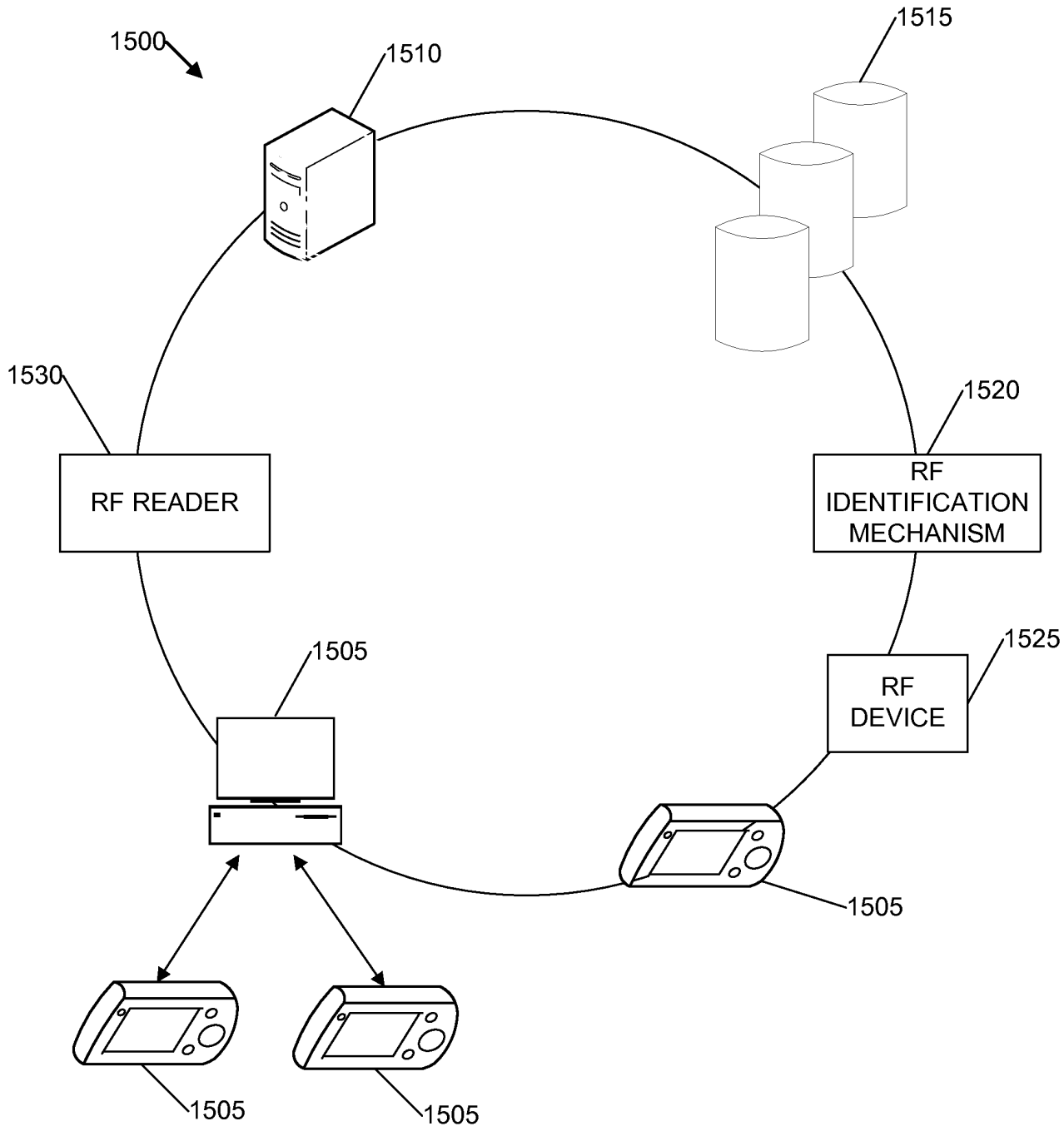

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

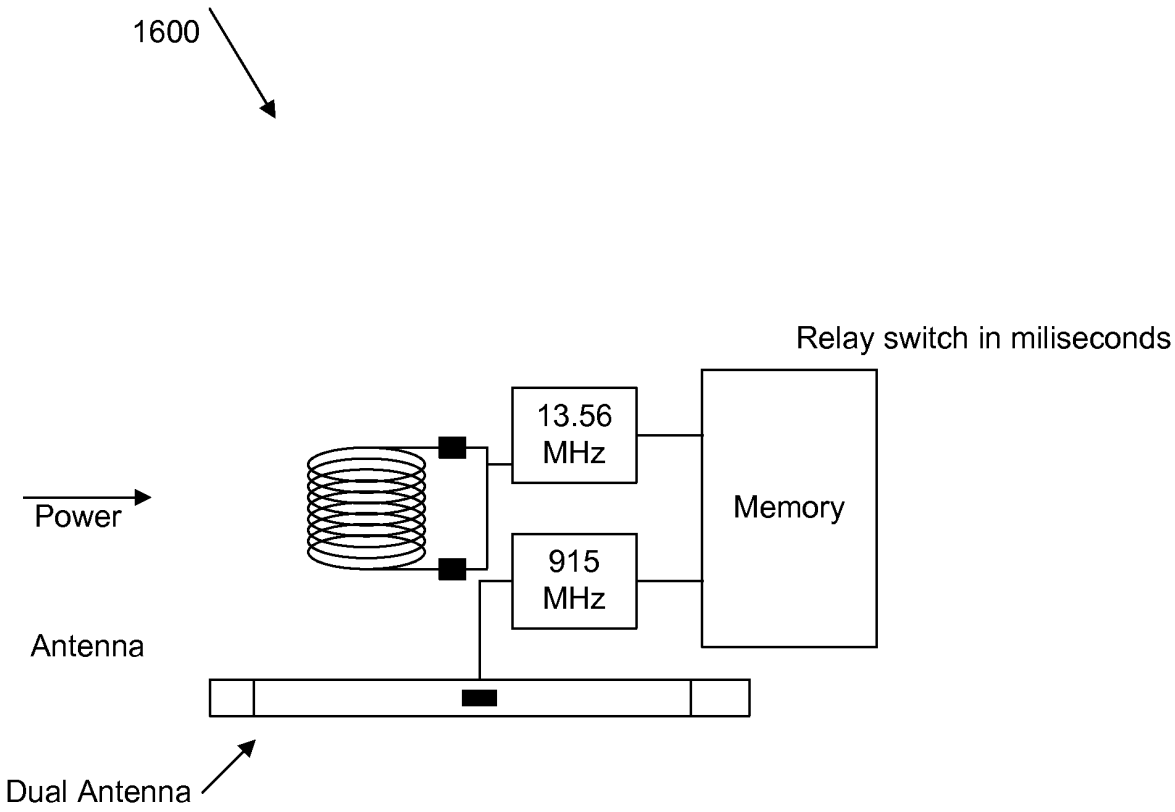

1600
Relay switch in miliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

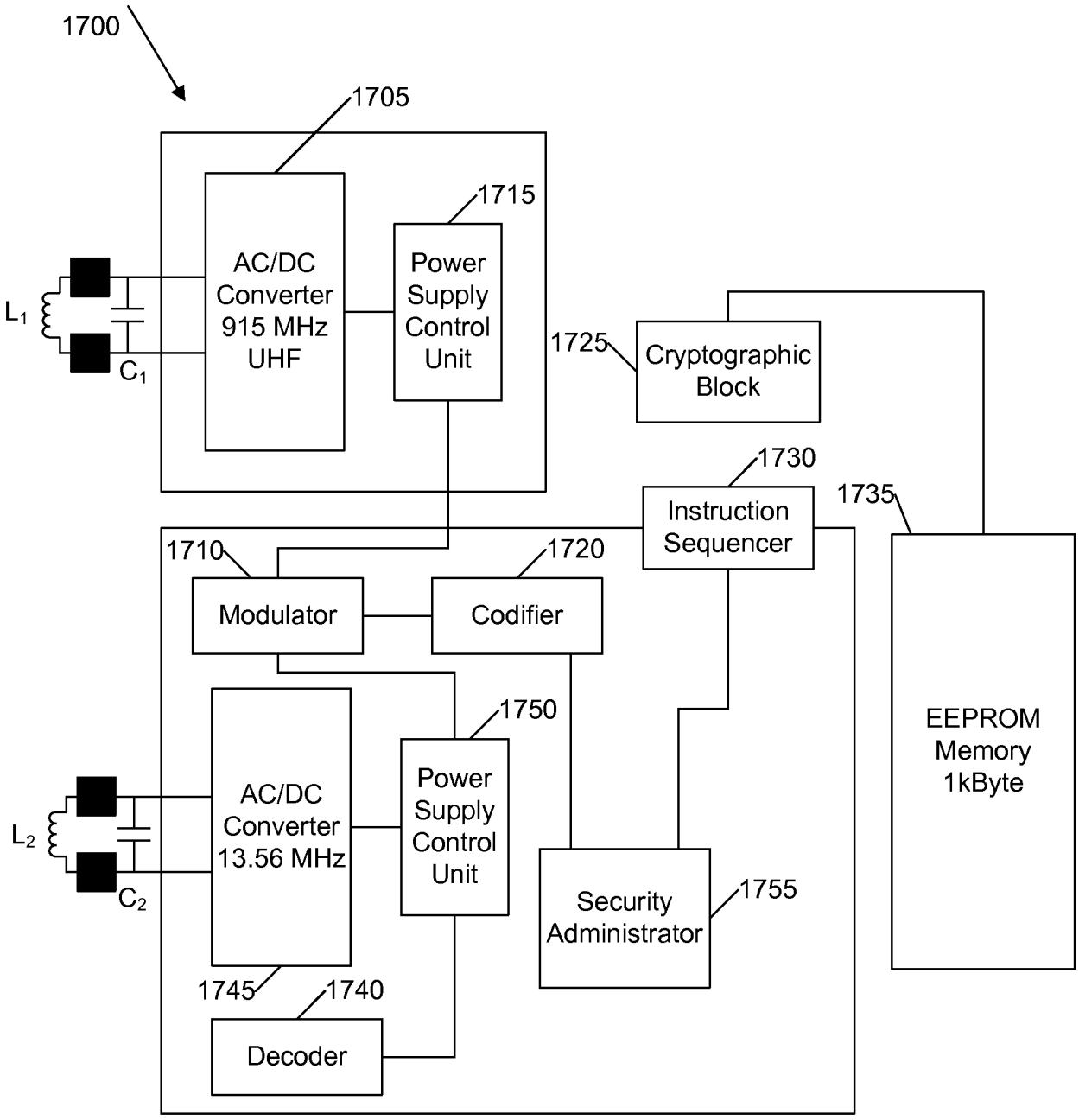

1700
1705
1715
AC/DC
Converter
915 MHz
UHF
Power
Supply
Control
Unit
L1
C1
1725
Cryptographic
Block
1730
1735
Instruction
Sequencer
1710
1720
Modulator
Codifier
1750
AC/DC
Converter
13.56 MHz
Power
Supply
Control
Unit
L2
C2
EEPROM
Memory
1kByte
Security
Administrator
1755
1745
1740
Decoder

FIG. 17

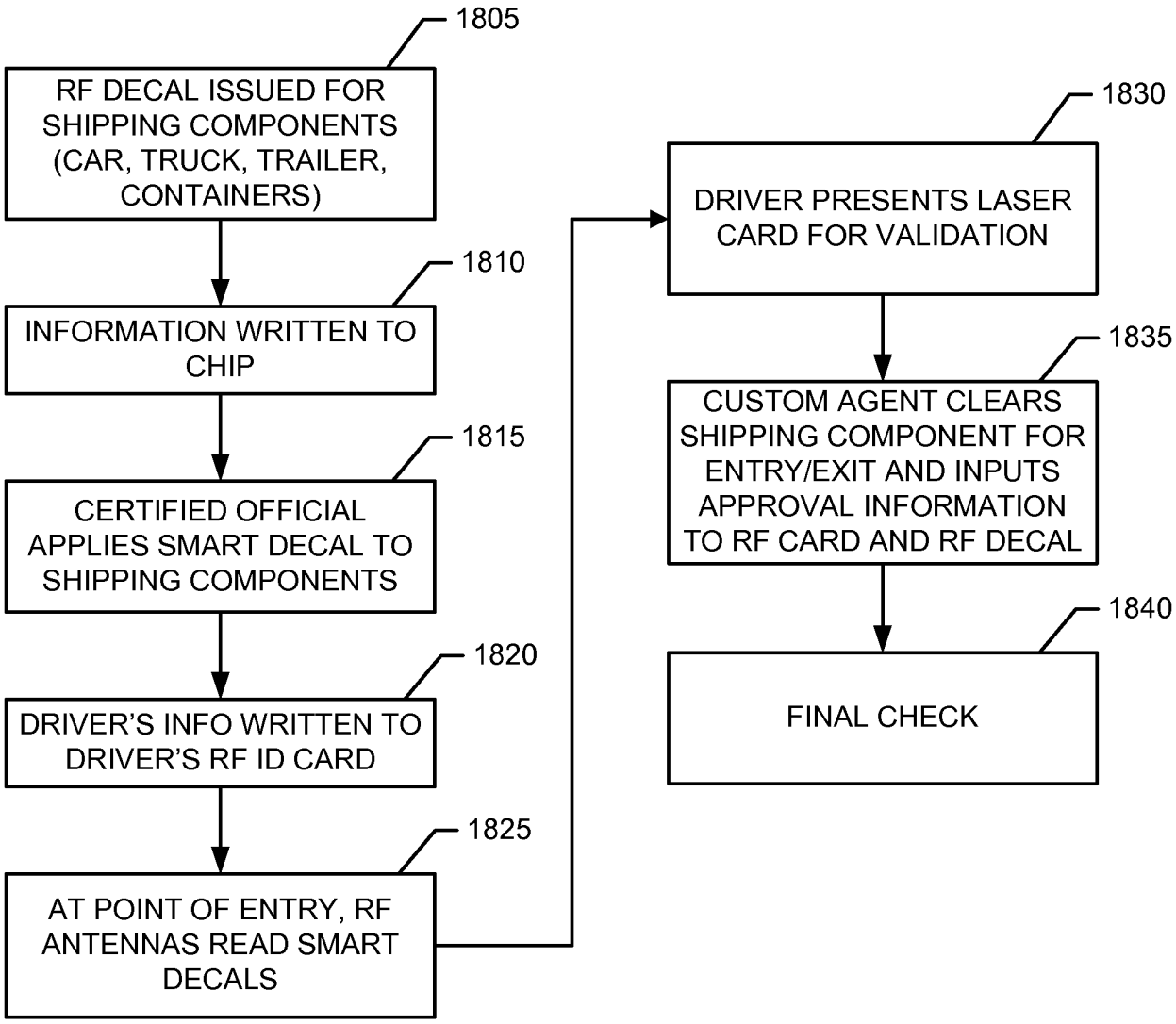

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS LASER CARD FOR VALIDATION
1835
CUSTOM AGENT CLEARS SHIPPING COMPONENT FOR ENTRY/EXIT AND INPUTS APPROVAL INFORMATION TO RF CARD AND RF DECAL
1840
FINAL CHECK

FIG. 18

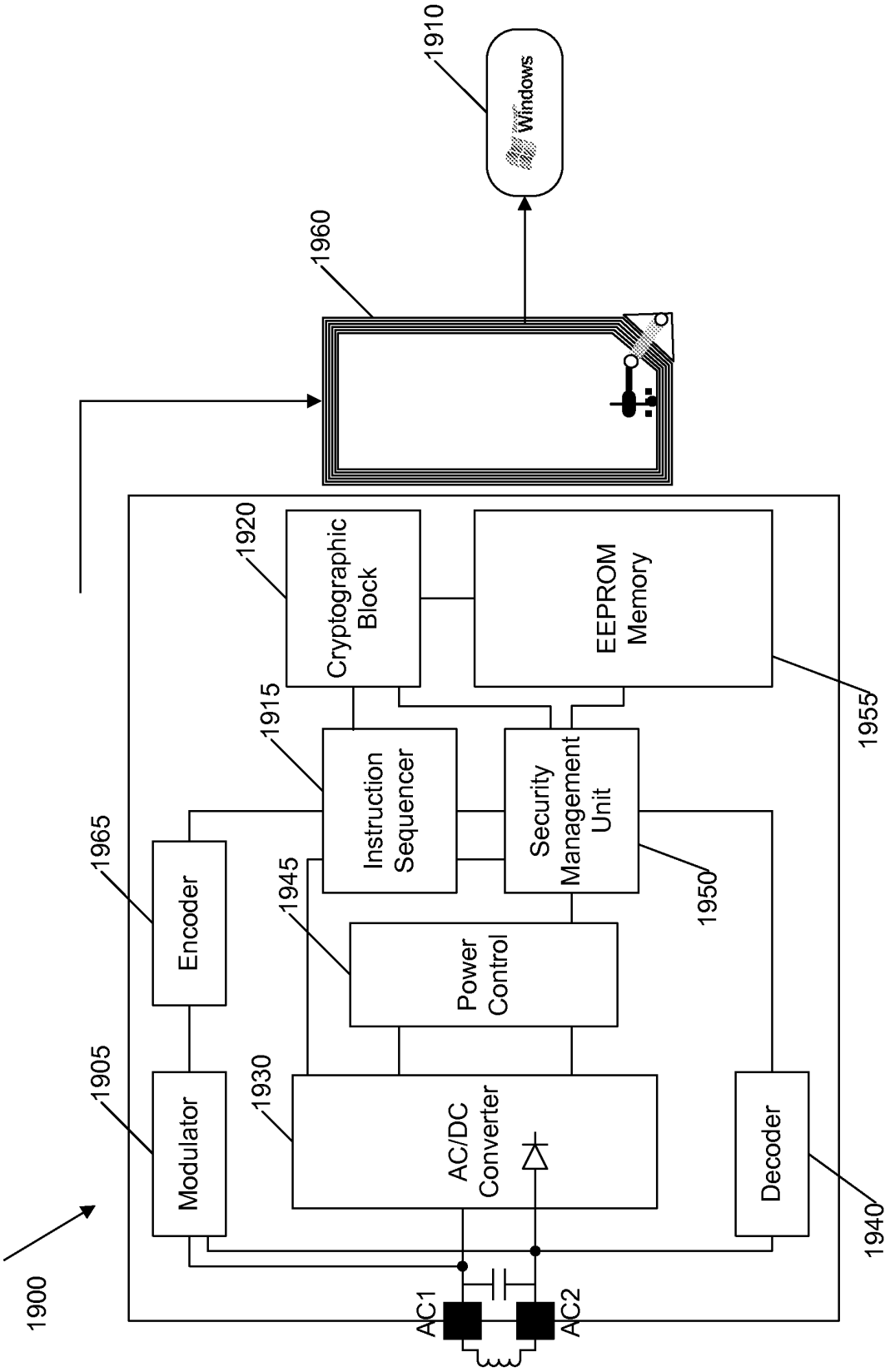


FIG. 19

2114747

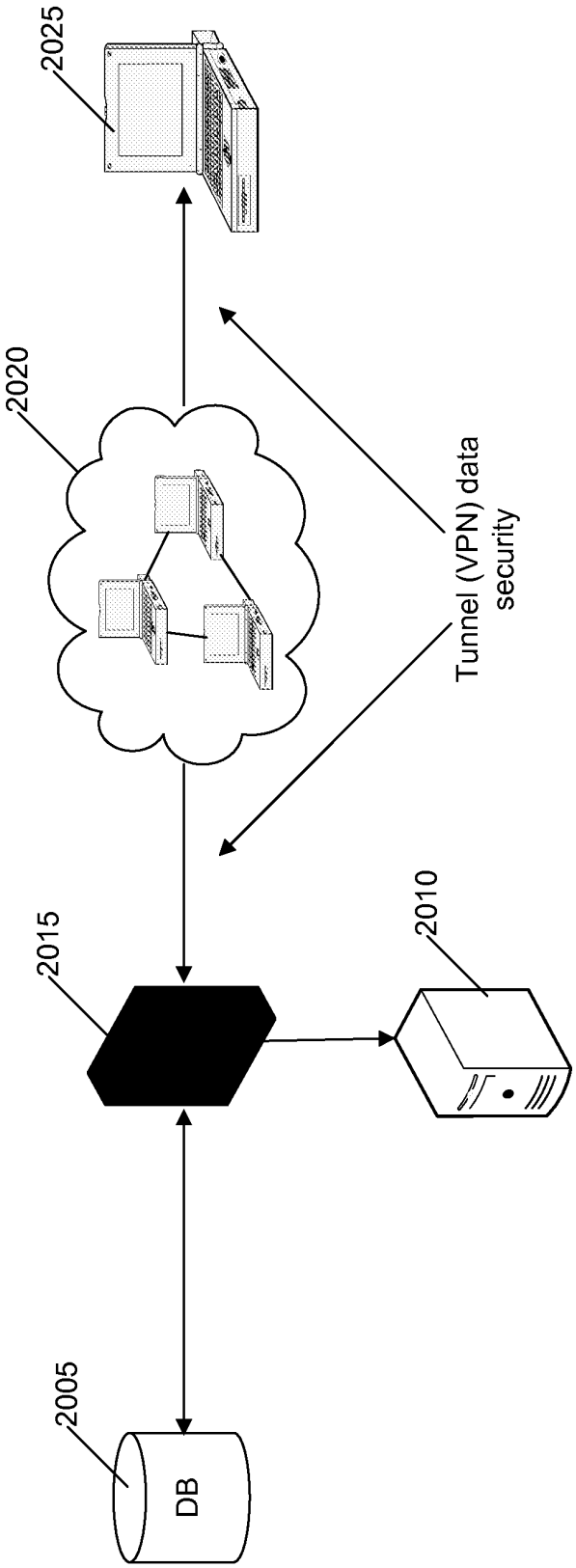


FIG. 20

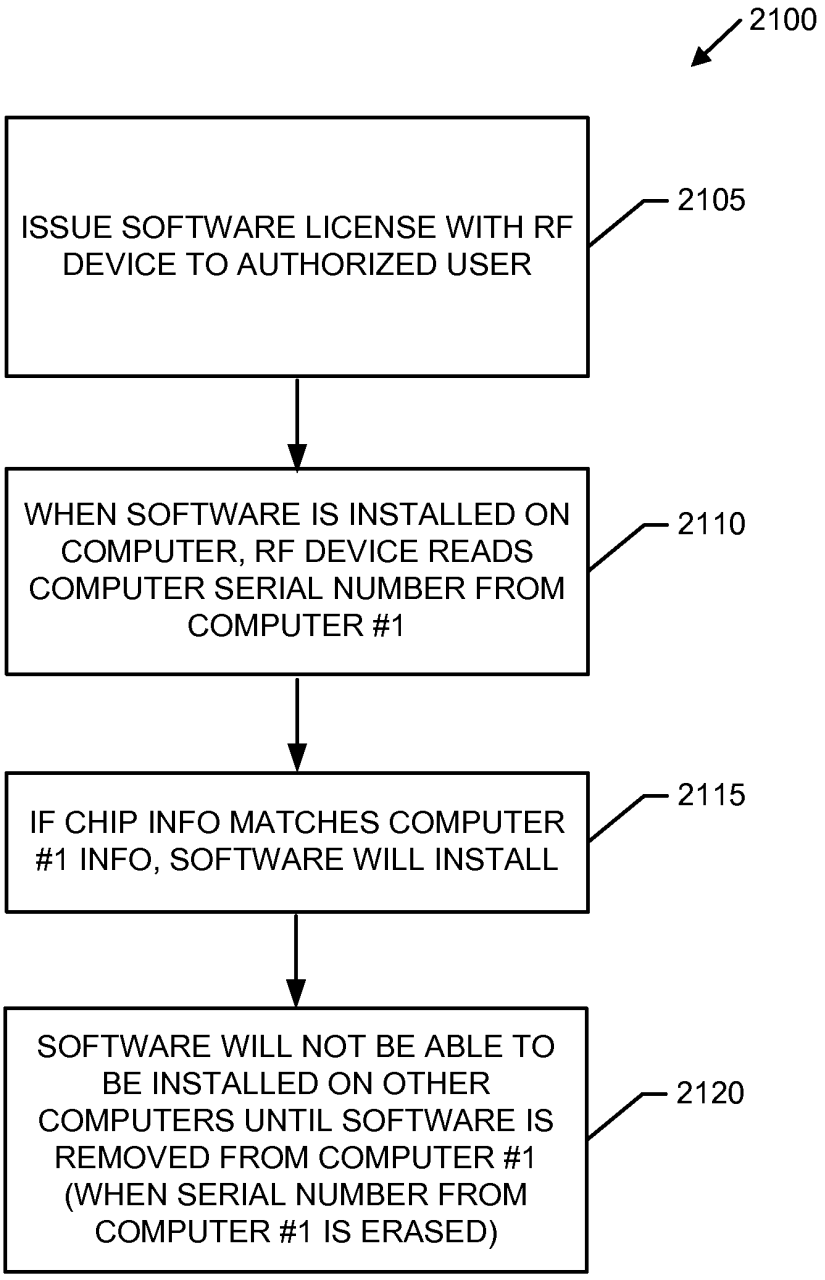

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL SOFTWARE IS REMOVED FROM COMPUTER #1 (WHEN SERIAL NUMBER FROM COMPUTER #1 IS ERASED)
2120

FIG. 21

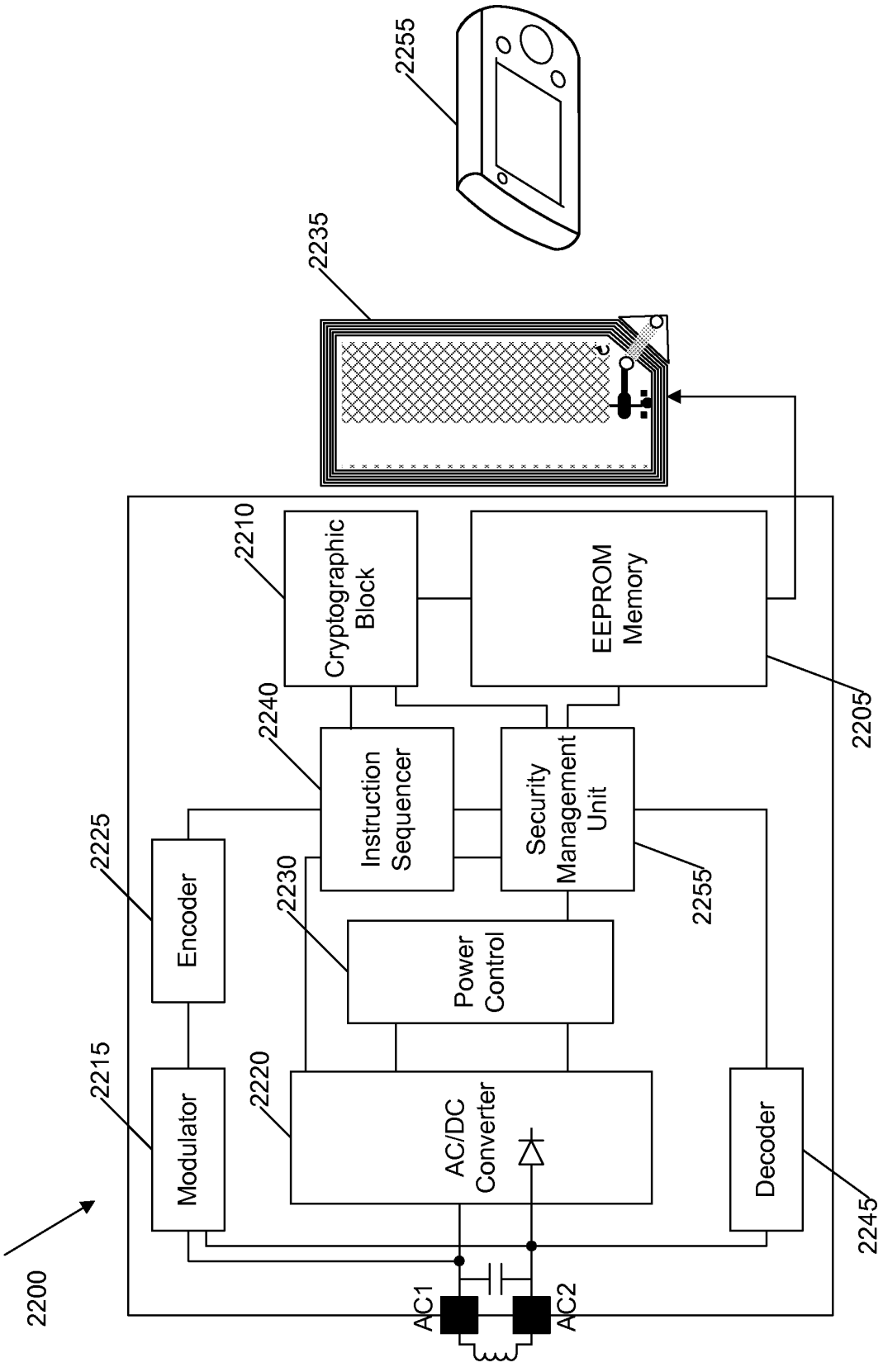

2255
2235
2210
Cryptographic Block
EEPROM Memory
2240
Instruction Sequencer
Security Management Unit
2205
2225
Encoder
2230
Power Control
2255
2215
Modulator
2220
AC/DC Converter
Decoder
2245
2200
AC1
AC2
2114747

FIG. 22

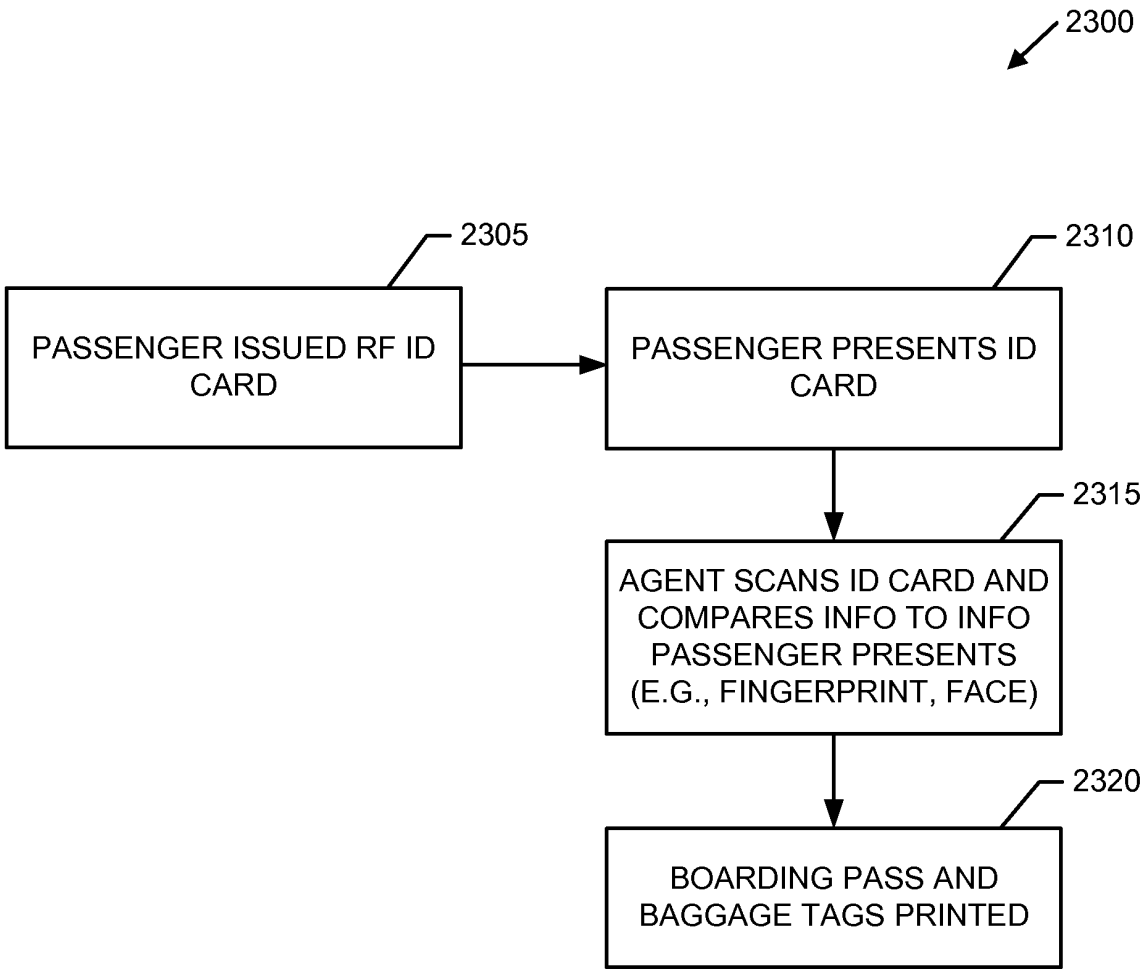

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SPECIFICATION

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention generally relates to a system and method for providing secure identification solutions, and specifically to a system and method for verifying and tracking identification information.

SUMMARY OF THE INVENTION

[0002] The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to:

- An RF Registration Item (e.g., License Plate) and Method of Use.
- An RF Identification Mechanism (e.g., Passport) and Method of Use.
- An RF Communications Device (e.g., Cellular Telephone) and Method of Use.
- A System and Method of Border Crossing Control.
- A System and Method for Limiting Software Downloads to Authorized Users.
- A System and Method for Airport Security.

[0003] The embodiments of the present invention are discussed below. Those experienced in the art will see that multiple features of certain embodiments described below can be incorporated into other embodiments both described and not described below.

[0004] The present invention is not limited to the above embodiments. Additional advantages and novel features of the invention will be set forth in part in the Description that follows, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

BRIEF DESCRIPTION OF THE FIGURES

[0005] Figures 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention.

[0006] Figures 5-8 illustrate the RF registered item and method of use, in an embodiment of the present invention.

[0007] Figures 9-11 illustrate the RF passport and method of use, in an embodiment of the present invention.

[0008] Figures 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention.

[0009] Figures 15-18 illustrate a system and method for border crossing control, m an embodiment of the present invention.

[0010] Figures 3A-3B and 19-21 illustrate a system and method for limiting software downloads to authorized users, in an embodiment of the present invention.

[0011] Figures 22-23 illustrate a description of the system and method for airport security, in an embodiment of the present invention.

DESCRIPTION OF THE INVENTION

I. GENERAL RF IDENTIFICATION SYSTEM AND METHOD OF USE

[0012] Figure 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120.

A. RF Device

[0013] Figure 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode.

[0014] Figure 5 illustrates a dual frequency RF device 110, according to one embodiment of the present invention. Those experienced in the art will see that a one frequency or multiple (more than two) frequency RF device can also be used. The RF device includes the following components: A modulator 215 is a device that receives baseband signals from an antenna. An AC/DC converter 220 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 225 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 245 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 250 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 230 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 255 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 210 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 205 stores data. Information can be read and written from or to this device.

[0015] A more detailed description of an RF device can be found in U.S. Patent Application S.N. 10/118,092 filed 09 April 2002; PCT Patent Application PCT/IB02/01439, filed 30 April 2002, which are herein incorporated by reference. Additional information on the RF device can be found in the accompanying documents.

B. RF Identification Mechanism

[0016] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are

possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA).

[0017] There are a variety of ways to make identification cards that are resistant to fraud and counterfeiting. In one embodiment, the present invention incorporates numerous security features, as explained below.

C. Features of Secure Identification Mechanisms

[0018] The present invention offers a variety of solutions for making secure and durable identification mechanisms resistant to fraud and counterfeiting. The following features help make the identification card more secure. These features are only examples, and those experienced in the art will see that the present invention is not limited to these features and that many other features can be incorporated.

[0019] In one embodiment of the present invention, at least one of the following features is incorporated: visible features, machine readable features, and proprietary substrate based features. Visible features require only the human eye to detect the security features. Machine readable features require special hardware (e.g., an ultraviolet light source, magnetic reader) to detect the security features. Proprietary substrate based features are security features incorporated within a plastic substrate.

[0020] In one embodiment of the present invention, at least one of the following characteristics are present relative to the identification mechanism: it is extremely difficult to duplicate; it is tamper proof, it is recognizable either visually or utilizing a machine readable device; it is durable enough to withstand harsh environments; it is produced by specialized, difficult to obtain production equipment; it can be machine readable; and cost savings are realized by volume production of the identification mechanism.

[0021] Security features curb petty, semiprofessional and professional counterfeiters by creating features that are highly difficult to reproduce. For example, the ready accessibility of dye sublimation card printers, color scanners, color printers, heat sources (e.g., hair dryers), and color photo copiers make it relatively easy to reproduce ordinary photo identification cards. In one embodiment, the present invention, therefore, utilizes images and texts that cannot be scanned or photocopied without noticeable distortion, or cannot be recreated without highly sophisticated and expensive equipment.

[0022] Security Features. In one embodiment, the present invention can incorporate at least one of the following security features:

- *Tamper Proof Material*. This material consists of metalized polyester treated with a chemical that will not allow an auto adhesive hologram to be transferred from one document to another one. It will self-destruct by any attempt at transfer.

- *Bidi-Tri-Dimensional at Three Levels*. This material must be created in an optical table by a qualified holographer and with a combination of design and dot-matrix effects created by precise digital means allow identification of the document's authenticity.

- *Hidden Images*. A hologram can contain a hidden image that cannot be detected with the naked eyes. The hidden image can be identified by shooting a laser at 45 degrees. The reflection shows a spectrum of a text shield or design. A special lens to protect the eye from laser damage can be used.

- *Dot-Matrix*. A dot-matrix 1,000 dots per inch (DPI) effect is created in a computer and comprises engraving dots with a laser in a specific angle which a minimum density of 1200 to 2000 DPI's. It allows printing of micro text contained within a hologram with great precision and creates very precise 2D and 3D effects.

- *Hot Stamping*. Hot stamping places a hologram on a document by thermal transfer. This hologram will interlace with a paper substrate and will not allow a hologram to be transferred from one document to another.

- *Moire Pattern*. The moire pattern is a design-based pattern which superimposes two patterns with non-identical spatial frequencies. The effect is visually detected after utilizing a normal photocopier to reproduce the original pattern. The reproduced pattern induces a "moire" or aliasing which immediately suggests the reproduced image is counterfeit. The original is produced utilizing digital image technology which differs from normal photocopy technology. This effectively "tricks" the photocopier and reveals the moire in the reproduced pattern.

- *Hot Stamp Metalized Hologram*. This feature is a visual/substrate-based feature which can also be machine readable. It uses a special metalized hologram (e.g., as found on various currencies) or a holographic hot stamp (e.g., that is non-machine readable). This feature comprises special stripes placed within the card laminations and visible to the eye. These holograms can be proprietary in order to limit the availability to counterfeiters. The metalized holograms can also be machine readable to verify authenticity. The security of this feature is high because to duplicate it, a counterfeiter must have access to both the card manufacturing equipment and the source of materials, which are both difficult to obtain.

- *Microprint: Offset Printed, Visual/Machine-Readable Text of Particular Size*. The text is indecipherable without the use of a reading lens, and is usually incorporated as a single line. This feature is used to print misspelled words to fool counterfeiters who often assume complete and correctly spelled microprint. The offset printed text is located under a translucent lamination to protect it from abrasion. This feature is difficult to produce with clarity and resolution using a photocopier, scanner, or dye sublimation printer.

- *Microprint: Visual/Machine-Readable Text of Particular Size*. This text is indecipherable without the use of a reading lens, and is usually incorporated to appear as a single line. This feature is used to print misspelled words to fool counterfeiters who often assume complete and correctly spelled microprint. This feature is difficult to produce with clarity and resolution using a photocopier, scanner, or dye sublimation printer.

- *Ultraviolet Fluorescence: Offset Printed, Visual/Machine-Readable Art or Text which Produces Light When Activated by an Ultraviolet Light Source*. This feature is normally undetectable to the naked eye and can be overlooked by the casual counterfeiter. This feature is difficult to produce with easily obtained equipment. Special fluorescent colors are available for added security.

- *Light Pipe*. This is a substrate based, machine readable feature requiring a light source to detect. This feature is produced using optical techniques which direct light to specific locations of the card (e.g., the edge). The effect is a brilliant light at a location different from where the light source is pointed, and usually in a specific color. Since this feature involves specific translucent materials and optical design of substrates, counterfeiters may never detect this feature. It is also almost impossible to recreate such a feature.

- *Laser Engraving*. This visual substrate-based feature can be either tactile or subsurface depending upon the types of plastics employed. The feature can be either graphic or alphanumeric. Using a laser, a pattern or alpha numeric text is ablated into the sub-layers of a plastic card. Depending on the parameters of the laser system and the materials of card substrate, a tactile or subsurface mark appears. This feature is particularly effective in the serialization of cards to reduce the risk of lost or stolen cards. The mark cannot be "scraped off without noticeable damage to the card surface. A tactile surface is helpful in quick recognition of authenticity. Laser systems of such complexity are expensive and difficult to obtain.

- *Metalized Stripe*. This stripe is a visual substrate-based feature which can also be machine readable. This feature uses a special metalized stripe (e.g., found commonly inside various currencies) or a holographic stripe (e.g., non-machine readable). These special stripes are placed within the card laminations and are visible to the naked eye. The special stripes can be proprietary in order to limit the availability to counterfeiters. The metalized stripes can be machine readable to verify authenticity. This level of security feature is high because counterfeiters need access to both card manufacturing equipment and the source of materials. These are both difficult to obtain.

- *Guilloche Pattern*. This feature is an intricate pattern of curvilinear fine lines which were originally created by "engine turning," commonly used in currency design. This visual feature is design-based and commonly produced using offset

printing onto plastic. It is normally contained under a translucent lamination which acts as protection from abrasion. The fine lines are difficult to reproduce with full clarity and resolution on a copier, dye sublimation card printer, or scanner/personal computer/inkjet system because the dye sublimation printer can print only onto the surface of the card.

- *Rainbow Guilloche*. This feature is similar to the guilloche pattern above and is used in conjunction with a color spectrum which gradually changes from color to color achieving a continuous effect across the surface of the card. The level of security is slightly greater since use of a sophisticated color copier is required to duplicate the pattern effectively.

- *Cameo Effect*. This feature is the result of cropping the background of an image with software to print only a silhouette of the person which makes it more difficult to replace than a square image. This effect is combined and interlaced with other security features, such as hidden infrared on the background of the picture, or interlacing a photo with guilloche patterns on the back.

- *Ghost Image*. This feature provides the ability to print a second photo of a person, which is degraded by software, and it is printed on a faded gray or color scale over the personal data of the person to protect this information from tampering or altering. This effect is also achieved by software.

[0023] **Types of Holograms**. Many different types of holograms with unique visual effects are utilized for commercial and security applications, as well as promotional products. In one embodiment, the present invention includes at least one of the following holograms:

- *Two Dimensional (2D) Hologram*. This hologram lies on one single layer, which projects vivacity of color. With this technique, we convert standard color line artwork or photography into an array of holographic colors.

- *Three Dimensional (3D) Hologram*. This hologram is created from a solid model or sculpture. The product's third dimension is captured. The design becomes a 3D

image after the depth of the image is captured through the use of a sculpture. A logo or product will be seen without the need of special glasses or lenses.

- *Two/Three Dimensional (2D/3D)*. This hologram combines a superficial layer with other dimensional layers, which can be a combination of both technologies, as mentioned previously. One image produces multi-color levels because of the positioning of the various layers. This system adds a third dimension to pictures.

- *Line Artwork & Photographs*. One embodiment of the present invention uses line artwork, photographs, or a combination of both, to create several layers of images separated by specific distances in order to give the illusion of depth. In general, two layers are enough, but if necessary, five different layers of images can be used.

- *Colorgrams*. Also known as true color holograms, colorgrams usually use someone's photo. It is made up of photographic quality art-work. These holograms are surprisingly capable of displaying true colors of the object, like true human skin tones or the original colors of a flag. If a counterfeiter cannot get the original photo, they cannot duplicate the label. It is a good way to prevent counterfeiting. The colorgram system is similar to the 2D/3D system. Full-color photographs are reproduced in their true, original colors at a specific angle, usually at a 45 degree viewing angle. The system can combine photographs with line artwork at different layer levels.

- *Stereograms*. Stereograms involve the latest in advanced technology. They are the result of a complex system that gathers full images, volume, movement, color and total animation. Total animation gives the sensation of the movement of a live recording.

- *HolomatrixTM from 50 DPI to 2000 DPI*. This feature comprises microtext, optical variable effects, and computer-generated optical devices. Graphic images for this type of hologram are created with microdots. Each dot is an individual embossment made with a laser beam. This feature creates holograms through the

use of sophisticated computer technology. The laser beam individually embosses each dot, creating a luminous image with a fascinating presentation of colorful optical effects. This technique prints small dots and is similar to a laser printer or inkjet system. These dots are holographic gratings that act like small prisms that sparkle intensely. With this system, optical patterns can be built of images in such a way that the images can be viewed at a 360 degree angle, and have multiple images in the same hologram. Because of the difficulty of reproducing these images, this feature is excellent for security applications.

- *Diffractive Optical Variable Image Devices*. All the products classified as DOVIDs (Diffractive Optical Variable Image Devices) present an image which changes colors when tilted in various angles. This essential characteristic makes the Images impossible to copy or imitate by traditional printing and graphics software.

- *Optical Variable Devices*. An optical variable device (OVD) is a way of printing an image in such a way that certain characteristics vary when viewed or illuminated from different angles.

- *Combined Holograms*. These holograms combine two or more of the above mentioned types of holograms. Combining Holomatrix™ with any of the above types makes the hologram more complex and ideal for security applications.

[0024] Optional Tests. In one embodiment of the present invention, the identification mechanism is tested in multiple ways. Laboratory tests are used to demonstrate durability, tamper proof, temperature and humidity stability, abrasion resistance, adhesiveness and light stability to ensure durability of the identification mechanism and to ensure that the dyes will not fade or degrade before at least 5 years of extensive use. In addition, dual lamination can be performed.

[0025] One embodiment of the present invention can include at least one of the following tests.

- *Static Bending Test*. In this test, a composite card is tested to exceed 100,000 bending cycles without breaking or losing its integrity.

- *Heat Test*. In this test, a composite card is exposed for an extended period of time to intense sunlight, boiling water, and a temperature of up to 220 degrees Fahrenheit without twisting or bending.

- *Rigidity Test*. In this test, multiple layers are applied to a composite card to give it rigidity so that when it is laminated it will not lose its flat shape, guaranteeing that the bar code is readable.

- *Durability Test*. In this test, a card is placed in a steam pressure chamber at 160 degrees Fahrenheit for four days to test that the card will not warp or break, and that the over lamination will not come off.

- *Abrasion Test*. In this test, a card is placed in an agitator containing a water and sand solution and subjected to 30 minutes of agitation.

[0026] **Required Security Levels**. Multiple security levels exist and are explained below.

[0027] First Level Security Features. First-level security features are clearly visible so that any attempts to modify the text data, photo image, or other personalized information is evident at a simple glance.

[0028] In one embodiment, the first-level security features include a complex hologram with multiple security features, combining a complex hologram structure with micro printing. The printer and the hologram are transferred through a holographic registration and a fiber optic sensor to assure very high accuracy. The holographic pattern is always transferred in the same position.

[0029] In one embodiment of the present invention, the hologram includes at least one of the following general features:

- A highly integrated technology and expensive machinery is required for mass production. Only manufacturers with sophisticated know-how can maintain its quality.

- The hologram makes the object visibly distinguished from other printing materials or those color copied.

- Some types of hologram (e.g., Kaleidogram, Finegram) ensure more satisfying security features than of the flat types, since the most advanced equipment is necessary in the process of production.

[0030] In one embodiment of the present invention, reproduction features include:

- A Transparent Kaleidogram with protective OP layer that is heat transferred on to the card book. It covers the entire printed area.

- Attempts to remove the hologram layer will damage the composition of the hologram. Thus it cannot be reused, or tampered.

- Combined with micro-letter printing, the reproduction by color copy or photomechanical process is not feasible, as the 0.26 mm size characters is ruined when reproduced. Additional first-level security features can be integrated with the RF identification mechanism (e.g., card) in the future. An example of such security features would be icons, symbols, or guilloches that could be printed in special solvent sensitive inks. These features can be printed directly onto the intermediate transfer layer. These security features could be employed at some time in the future if a solvent tampering technique is identified.

[0031] Overall, the proposed first-level security features provide the document with excellent protection against altering and falsification, as well as acts of counterfeiting. The features are readily visible and any attempts to modify the underlying information is evident at a glance.

[0032] Second Level Security Features. Second-level security features can also be included. These second-level security features are invisible to the eye under normal viewing conditions, and are evident only when using a proper detection device. In one embodiment of the present invention, at least one of the following features is included:

- *Invisible Ultraviolet-Fluorescent Features*. The visible portion of the energy spectrum extends from deep blue at, for example, 400 nm to deep red at, for

example, 700 nm. Long wavelength ultraviolet energy in the region of the spectrum for example, between 350 nm and 400 run, such as 380 nm, is used to excite an embedded ultraviolet-fluorescent material. These high-energy ultraviolet photons are absorbed by the fluorescent material that happens to be invisible or transparent in the 400 rim. to 700 nm region of the spectrum. The ultraviolet photons pump the absorbing material to excited energy states. The material in the excited states quickly relaxes back and releases the absorbed energy again in the form of photons. Because some of the energy is lost in this transition, the emitted photons have less energy than the absorbed photons. The visible portion of the energy spectrum is positioned at the lower energy photon levels. Consequently, the process results in visible light being emitted from the material when it is illuminated by ultraviolet light. In a darkened room, the eye detects the glow being emitted by the ultraviolet-fluorescent material but not the ultraviolet light that is used to excite the material.

- *Two-Dimensional Bar Code*. The card solution can include a PDF-417 format barcode (two-dimensional barcode) that is printed onto the card. The PDF -41 7 barcode can hold several types of data (e.g., fingerprint minutiae, personal information).

[0033] *RF Device*. An RF device can complement all the previously mentioned security features, as it has a unique identifier (e.g., a unique 64 bit serial number), and the information contained on it is protected by sundry cryptographic methods. The capacity of the device will allow a great deal of information about the holder to be stored on the device (e.g., fingerprint minutiae or other biometric template, the holder's biographical information, statistical information). Those experienced in the art will see that an RF device allows data to be written to and read from the device via an antenna without the holder having to present the document for verification through traditional methods such as visual inspection, or other method of machine reading.

[0034] *Third Level Security Features*. Two optional security features can be changed every eighteen months: special IR-activated security taggant material and proprietary security taggant material.

[0035] *Special Infrared-Activated Security Taggant Material.* A special ceramic compound (e.g., such as a product named Taggant, provided by Secure Products) is mixed with a clear ink media in very small concentrations. (The ceramic compound is referred to as Taggant, but those experienced in the art will recognize that other ceramic compounds or equivalent product can be used.) This mixture is printed on the intermediate transfer material surface. After being ground to small particles that are approximately 2 - 3 pm in diameter, the special ceramic compound appears to be a very fine white-colored powder. The combination of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye.

[0036] A low-power, eye-safe near-infrared laser can be used to activate the special IRactivated taggant material. The input wavelength of the laser must be tuned within a 3-5 nm bandwidth in order to activate the material. The input energy is pumped into the material with the lower energy photons of the laser. The combination of the long lifetimes for the excited energy states and the high concentration of photons from the near infrared laser result in a second transition upward in energy level. In other words, two photons are absorbed by the material to increase the available excitation energy. These high excitation energy states relax releasing photons in the visible portion of the spectrum as well as the near-infrared portion.

[0037] This process of effectively adding two lower energy photons together to release a higher energy photon is called "up-conversion." The special IR-activated security taggant material has three separate emissions or security features. When an appropriate infrared laser, which is invisible to the eye, is focused on the special taggant material, three features are emitted simultaneously. These three features are a visible green spot at the point of focus, a visible blue spot at the point of focus, and an invisible infrared point at a higher energy level in the near infrared portion of the spectrum. When viewed by the eye, the green and blue spots blend together to create a vivid turquoise color. However, all three features can be detected automatically and separately with the proper equipment.

[0038] *Proprietary Security Taggant Material.* A proprietary security taggant material can also be included in the card design. A special ceramic taggant material (e.g., such as the one produced by Secure Products) exhibits multiple security features and is in part based on the "up conversion" concept. The white powder is ground into particles that are 2 - 3 nm in diameter and is mixed into a clear ink media in very small concentrations. Again, as before, the combination

of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye. However, this special material can be activated by several wavelengths and each activation wavelength results in a different response.

[0039] One characteristic and security feature is activated by a special low-power, eye-safe near-infrared laser. The activation bandwidth is approximately 3 nm and is located on the longer wavelength side of the activation energy required for the second-level feature. Laser devices are far less common in this area of the spectrum. When the special taggant is excited by a laser specially tuned to this excitation frequency and bandwidth, two separate emissions are observed. One emission is in the visible portion of the spectrum and can be observed as a green spot at the point of incidence. The second emission is in the near-infrared portion of the spectrum near the excitation wavelength of the first optional security feature.

[0040] A second characteristic and security feature is observed by using a second low power, eye-safe near-infrared laser at about the same excitation energy as the similar second-level feature. At this excitation wavelength, a green spot can be observed at the point of incidence due to the "up-conversion" process.

[0041] Finally, a third characteristic and security feature can be observed by applying energy in a wider bandwidth in the upper portions of the visible energy spectrum. This wavelength of energy is absorbed and re-emitted as longer wavelength infrared energy. In one embodiment, the initial implementation activities will focus on a verification process that utilizes a single excitation wavelength and a single observation wavelength. The implementation of the other embedded security characteristics can be phased into the program as new features are required to maintain the overall security of the card documents. Since these untapped security features and benefits will have existed in the documents from the initial issuance, the implementation of the new features will minimize the impact to the overall system.

[0042] In addition, new security features can be integrated into the present invention should the need arise.

D. Method of Using the General RF Identification System

[0043] Figure 4 illustrates the methods of using the RF identification system 400, according to one embodiment of the present invention.

[0044] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity.

II. RF REGISTERED ITEM AND METHOD OF USE

[0045] One embodiment of the present invention allows authorities to track information regarding a registered item (e.g., a vehicle), identify the item, and determine whether a driver of the item has the right to operate the vehicle. The present invention is described using the illustration of a license plate, but those experienced in the art will recognize that multiple other embodiments are possible, including, but not limited to: a sticker (e.g., a self-adhesive decal that can be placed on an automobile window, windshield or license plate), an RF embedded license plate (e.g., if the license plate is to be manufactured with some non-conductive material, the RF device can be embedded directly into the license plate), an encapsulated RF device (e.g., in the housing of a rear-view mirror, headlights or taillights, the vehicle's front or rear bumpers, or in any non conductive component of the vehicle; the device can be encapsulated in such a way that it will resist normal use and exposure to the elements, or embedded directly into the materials comprising the aforementioned placement media).

[0046] The present invention can be used, for example, for vehicle identification, border crossing solutions, traffic violations, insurance programs, pollution control, vehicle access control, traffic logistics planning and engineering, toll booths, and other vehicle control applications. The present invention takes centrally stored information and makes it accessible to the field (e.g., to police or other authorities). It also extends and expands the verification of individual and item (e.g., vehicle) information.

A. RF Registered Item

[0047] Figure 5 illustrates an RF registered item 500, according to one embodiment of the present invention. The registered item 500 includes the following components: A modulator 515 is a device that receives baseband signals from an antenna. An AC/DC converter 520 is a device

that receives an alternating current (AC) and converts it to direct current (DC). An encoder 525 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 545 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 550 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 530 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 555 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 510 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 505 stores data. Information can be read and written from or to this device.

B. Method of Using RF Registered Item

[0048] Figure 6 illustrates the method of using RF registered item 600, according to one embodiment of the present invention. In 605, individual identification information (e.g., fingerprint, picture) and/or vehicle identification information (e.g., registered vehicle, license number) are collected and written to an RF device (i.e., a chip with an RF antenna). In 610, the RF device is embedded onto an identification mechanism, a license plate. In 615, an authority wishing to check a vehicle uses an RF reader/writer to read the chip data. In 620, the authority takes and compares the individual identification information (e.g., user's fingerprint, check user's face) and/or vehicle identification information (e.g., check make and model of vehicle, check vehicle license number) and to the chip data to verify an individual's identity and whether the individual has the authority to possess and operate the vehicle.

[0049] In one embodiment, a selective metalizing procedure is used to selectively metalize the areas which will not carry the RF device. This can be done by using a mask, as illustrated in Figure 7.

C. Method of Making RF Registered Item

[0050] In one embodiment, the identification mechanism (e.g., license plate) comprises a material that allows visual validation of the registration, even at night. The material can be a retro-reflective material, holographic foil, or another substrate with a high metal content.

[0051] Figure 8 illustrates method of making RF registered item 800, according to one embodiment of the present invention. In 805, antennas are produced on a demetalized or

selective metalizing process. In 810, after demetalizing, resistance is decreased and conductivity is increased by applying inks containing silver or copper (e.g., conductive inks). In 815, an adhesive layer is applied to the antenna in a Web environment or with automatic label capabilities.

[0052] In one embodiment of the present invention, at least one of the following is tracked:

- *Vehicle Identification Number (VIN)*. The VIN is the vehicle's international registration number and is the "fingerprint" of the car. Vehicle identification is performed by visually reading the car's VIN, and using the software to validate the VIN. This software allows a user to determine if the vehicle has been modified, altered, and/or stolen.

- *Owner Identification*. Owner identification is made using photographic information (e.g., a photograph) and/or biometric information (e.g., a fingerprint, iris pattern) stored in the RF device.

- *Tracking Information*. The RF device is used to read the VIN number and the owner's information. This can be used to identify a vehicle or individual reliably without having to connect to a central database.

- *Central Data Base*. The central data base validates the identity information for increased security (e.g., tracking who and where the device was produced and who it belongs to).

D. Optional Security Features

[0053] In one embodiment of the present invention, at least one of the following security features is included:

- *Secure Device*. In one embodiment, the device has: numerous (e.g., five) visual inspection security features visible only to the naked eye; numerous (e.g., three) nonvisual forensic security features that require a special device for detection; and at least one security feature requiring a special detection device that is proprietary (i.e., it was manufactured specifically for a particular client).

- *Secure Identification*. This feature requires information contained in the device to be unalterable without a determination of who wishes to alter the information and for what purpose. Highly secure chips with a hardware programmable cryptographic block with credit and debit exchange keys is used in one embodiment of the present invention. In addition, the individual information of the vehicle (e.g., the VIN) and the personal information (e.g., biometrics) contained in the device must be protected. • Secure Transaction. This feature protects the device from the equipment that reads and writes from the device. This equipment must be initialized using the same encryption keys as the RF device.

- *Secure Data Base*. This feature protects information in the central data base and the transaction log indicating where and for whom the device was produced. Central data base security is possible using encryption. This technology allows centrally-stored information to be taken to the field (e.g., to track the inspections for stolen vehicles). It also extends and expands the verification of both individual and vehicle identity.

III. RF IDENTIFICATION MECHANISM AND METHOD OF USE

[0054] The present invention includes an RF identification mechanism, such as a passport, and a method of using the same. The present invention will be described in the context of a passport. However, those experienced in the art will recognize that the RF identification mechanism is not limited to a passport, and multiple other embodiments are available, including, but not limited to: a license, credit card, cell phone, etc.

A. RF Identification Mechanism

[0055] Figure 9 illustrates an RF registered item 900, according to one embodiment of the present invention. The registered item 900 includes the following components, as described earlier: a modulator 915, an AC/DC converter 920, an encoder 925, a power control 930, an instruction sequencer 940, a cryptographic block 910, a decoder 945, a security management unit 955, a memory 905, and an antenna 935.

B. Method of Using an RF Identification Mechanism

[0056] Figure 10 illustrates a method of using the RF passport, according to one embodiment of the present invention.

[0057] In 1005, identification information (e.g., a biometric template, photography, social security number, personal identification number) is collected and written to the chip on the RF device. In 1010, the RF device is embedded on a passport. In 1015, the user enters an area where a passport must be presented and an RF reader/writer reads the identification information from the RF device on the passport. In 1020, an authority collects second identification information from the user (e.g., takes the user's fingerprint, looks at the user's face) and the information is compared to the RF device data to verify the user's identity.

C. Method of Making an RF Identification Mechanism

[0058] Figure 11 illustrates how an RF passport is made, according to one embodiment of the present invention. In 1105, the passport inlay is produced on a PVC substrate. A copper wire and chip are embedded into the passport inlay. In Ill 0, the passport inlay is embedded into the passport document. In 1115, the passport is printed using a holographic retransfer film and dye sublimation inverse printing. In 1120, the RF passport identification information is matched to the person who owns the passport. In 1125, the passport is initialized, and personal information and/or biometrics are encoded on the passport to the RF device. This is done after the passport is personalized for security reasons. The RF passports are of no utility if they are stolen, as they need to be initialized with proper encryption keys and personalized.

IV. RF COMMUNICATION DEVICE AND METHOD OF USE

[0059] One embodiment of the RF communication device creates a communication through a network to a point of sale ("POS"). This is performed, for example, by a wireless RF device that stores a person's identification information, and can thus become a person's identification "document." This is discussed in the context of an RF cellular telephone, but those experienced in the art will recognize that any communication device, including but not limited to a personal digital assistant or a pager, can be used.

[0060] As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone. The user is then asked to enter authentication information (e.g., a fingerprint). If the user wishes to complete a transaction, the user enters the authentication information. An

exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information.

[0061] The present invention, referred to in one embodiment as an RF cellular telephone, creates a communication through a network of cells to a point of sale (POS). This is performed by combining Global System for Mobile Communication (GSM) technology with a wireless RF device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). GSM technology includes a compact chip located on the back of the telephone. The compact chip has an operating system. The GSM telephones identify the telephones to a network carrier to avoid, for example, telephone cloning.

[0062] The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card or other card (e.g., mileage cards). Multiple types of information can be carried and stored on the RF cellular telephone. The following uses are examples of how the RF cellular telephone can be used: an RF cellular telephone can be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities; an RF cellular telephone can be a personal identification or a Portable Data File (PDF); an RF cellular telephone can be integrated with a Global Positioning System (GPS) receiver; an RF cellular telephone can be integrated with hand held devices to provide Internet access, and access to business and personal information (e.g., email); and an RF cellular telephone could be a boarding pass (e.g., e-ticket) and/or could track a user going through security with authentication by fingerprint at a gate or other local area. Those experienced in the art will recognize that there are multiple other examples and uses of the RF cellular telephone.

[0063] One embodiment of the present invention provides at least one of the following benefits: assists in avoiding current credit card fraud, through donation, substitution of identity, or counterfeit documents; reduces or eliminates the need to carry credit cards, documents (e.g., a boarding pass) or other information; reduces or eliminates the need for an entity to issue or update credit cards or identification documents (e.g., tickets), with associated fees (e.g., mailing costs); and reduces or eliminates the need to stand in line or wait for services.

[0064] The present invention is discussed in the context of using a fingerprint for identification, as this is a widely recognized identification tool. However, those skilled in the art will recognize that any type of identification information (e.g., Personal Identification Number (PIN)) or any other biometric identifier (e.g., a voice print, iris recognition, facial recognition) could be used.

A. RF Communications Device System

[0065] Figure 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

[0066] The POS 1210 can include an RF reader/writer 31 and a fingerprint digital scanning device 1232. One-to-one verification ensures that the information on the RF cellular telephone matches the holder of the RF cellular telephone.

[0067] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact.

[0068] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in Figure 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from an antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a

device that decodes information from the encoder output so it may be used by another device or display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 134 7 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device.

[0069] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel mileage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security.

B. Method of Using an RF Communications System

[0070] Figure 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone.

[0071] According to Figure 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF

reader/writer connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information).

[0072] In 141 0, the customer purchases a service or product and is prompted to enter authentication information (e.g., a fingerprint). In 1415, if the user wishes to complete the transaction, the user enters authentication information (e.g., imprints a fingerprint into a fingerprint scanner) and it is loaded to the RF device.

[0073] In 1420, the RF reader/writer and RF cellular telephone are used to verify the authentication information (e.g., the fingerprint scanner works with the RF reader/writer and the RF cellular telephone and/or other devices to ensure the customer's fingerprint matches the fingerprint stored on the RF cellular telephone) and this information is presented to a point of sale or access control device to retrieve purchase information.

[0074] Although the present invention has been described in the context of a POS, those skilled in the art will recognize that a user could use the RF cellular telephone without a POS. For example, a user could call a telephone number to buy a ticket to access a stadium, using identity verification and other transmitted information. As another example, a user could load a boarding pass or ticket to an event on an RF cellular telephone, and the boarding pass or ticket would be confirmed at an access control device around the perimeter of an airport lounge or stadium.

[0075] Additional information related to the present invention can be found in U.S. Patent Application 10/118,092, filed April 2, 2002, and PCT Patent Application IB0201439, filed April30, 2002, which are herein incorporated by reference.

V. SYSTEM AND METHOD FOR BORDER CROSSING CONTROL

[0076] One embodiment of the present invention provides a border crossing control mechanism using RF technology. This technology helps provide a flexible, efficient, and effective border crossing security system to meet the needs of rapidly changing security conditions. The present invention provides heightened security while at the same time efficiently and quickly moving vehicles and people across borders and through customs. In this embodiment, an identification mechanism (e.g., a laser card) is integrated with a vehicle decal that registers and matches any shipping components (e.g., drivers, vehicles, containers). The shipping components will be pre-registered in the decal at a point of origin. A fingerprint

biometric of the driver is written into the identification card and the decal at the factory. An RF antenna embedded into the decals allows tracking of, for example, the driver, cab and trailer, and validation of these components at strategic checkpoints. It also provides for designated routing through the port for inspection and clearance prior to departing the port.

[0077] The present invention can be used in a closed system or open system. In a closed system, all information resides on the RF laser card and RF decals. In an open system, information is passed from the point of original to country A's custom's inspectors, and from country A's customs inspectors to Country B's customs inspectors using a network (e.g., the Internet). This makes integration and implementation easier.

A. Border Crossing Control System

[0078] Figure 15 illustrates border crossing control system 1500, according to one embodiment of the present invention.

[0079] The system 1500 includes at least one client 1505, application server 1510, database 1515, RF identification mechanism 1520, RF device 1525, RF reader/writer 1530, connected by a network 1520.

[0080] **Client**. According to one embodiment of the present invention, clients are any computers (e.g., PC, PDA, cellular phone) connected to a network (e.g., LAN [Local Area Network], WAN [Wide Area Network], VPN tunnel [Virtual Private Network Tunnel], Internet).

[0081] **Application Server**. According to one embodiment of the present invention, an application server is used (e.g., an Oracle9iAS integrated into a J2EE application server). The application server can support web application software, wireless, web page caching, business intelligence features, and offer complete integration in a single product. The application server can also offer scalability, reliability, and security features. It can also include advanced clustering features to keep critical applications up and running 24x7; offers zero downtime and planned downtime through a fast start fault recovery architecture; and recover from incidents quickly and gracefully.

[0082] In the example embodiment of an Oracle9i application server, the high availability infrastructure includes Oracle9iAS Web Cache clusters, Oracle HTTP Server (Apache), and Oracle9iAS Containers for J2EE. In addition, database applications hosted on Oracle9i

Application Server can take advantage of Oracle9i Real Application Clusters (RAC) to make them more available. Oracle9i Application Server is the middle-tier deployment platform for all applications developed using Oracle9i Developer Suite. All applications can be deployed on the same middle-tier. Oracle9i Developer Suite is a complete and standards-based set of development tools. The suite includes Oracle9iAS Developer, Oracle's flagship J2EE and XML development environment that supports the full development life cycle of J2EE applications and Web services. It also includes Oracle9i Forms Developer for easily and quickly construct sophisticated database forms and business logic delivered through any Internet browser as a high performance, rich Java client.

[0083] **Database**. In one embodiment, the present invention uses a database with real application clusters (RAC) that can transparently scale and protect packaged applications with no changes necessary for the application (e.g., Oracle9i). RAC can scale all applications and also provides superior data protection with hot failover in less than 30 seconds.

[0084] According to one embodiment, the database provides a unique combination of scalability and availability in the same clustered database solution. With RAC, efficient scaling can be accomplished by simply adding servers to the overall cluster as the demand grows. Since RAC databases can grow flexibly, applications are protected from having to purchase excess computing power at a premium price. A RAC database can have costs significantly lower than the same solution implemented on an SMP (Symmetric Multi Processing) machine.

[0085] The database may include security and manageability features. The security features include: a Virtual Private Database (VPD); fine-grained auditing; data encryption.

[0086] The VPD technology provides programmatic row-level security and is enabled by associating tables or views with centrally defined access control policies. VPD addresses the application bypass problem and ensures that the same access control policy is enforced whether a user gains access to data through an application, ad hoc tool or SQL *Plus. As a result, multiple communities of users can securely share data within the same database.

[0087] Fine-grained auditing allows businesses to audit database activity by statement, system privilege, object or user. Its enhanced fine-grained auditing functionality enables organizations to centrally define specific audit policies that alert administrators to data access

misuse. Audit records, stored within the database, capture the user statement's exact SQL text and can be easily viewed through ad hoc queries.

[0088] Data encryption is the ability to natively encrypt data in the database, enabling applications to guard sensitive data. Server-based encryption supports industry-standard Data Encryption Standard (DES) and Triple-DES (3DES), in both two and three key modes for any organizations who require the strongest level of encryption. Encryption can also support the MD5 secure cryptographic hash to ensure data integrity and a Federal Information Processing Standard (PIPS) 140-certified random number generator for generating secure encryption keys.

[0089] The manageability features include intelligent self-managing and tuning. The database can enhance database manageability by automating routine tasks, reducing complexity of administration and making the database more self-tuning and self-managing. Features can be added to streamline space, memory, and resource management as well as other day-to-day database administrative tasks.

[0090] **RF Identification Mechanism, RF Device, and RF Reader/Writer**. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing a Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer.

[0091] **Multiple Chip Background Information**. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequencies can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See Figure 16.)

[0092] In one embodiment of the present invention, instead of, or in addition to incorporating the chip on the RF identification mechanism (e.g., RF smart laser card or RF decal), a chip can be embedded on a car windshield for smart windshield applications for vehicle registration, manufacturing, distribution of traffic violations, or any operation that requires contact with certain authorities. In this embodiment, the RF antenna can be used as radio antennas embedded on glass with copper wire during the manufacturing process, and connected to a module or embedded in the glass itself.

[0093] The resonant frequency of the antenna circuit in the RF device can be given by solving this equation:

$$f = \frac{1}{2\pi\sqrt{LC}}$$

f = frequency (Hz)
L = inductance (H)
C = capaticance (F)

[0094] The frequencies at the poles are parallel resonant frequencies, and depending on the technology can be:

$f_1 = 13.56\ MH_z$
$f_2 = 915\ MH_z$

$$L = \frac{N^2 \mu_\circ A}{1}$$

N = number of windings around inductor
$\mu_\circ$ = permeability of freespace (Hm^{-1})
A = cross-sectional area of inductor (m^2)
L = length of inductor (m)

[0095] The inductance " L " depends on the number of turns of the coil, of the area perpendicular to the coil and of the permeability of free spaces and length of the coil. Therefore:

$$l = \frac{N^2 \mu_o A}{l} \Rightarrow$$

$$\frac{N^2 \mu_o A}{l} \quad \frac{l}{f^2 4\pi^2 C} \Rightarrow$$

$$l = f^2 4\pi^2 N^2 \mu_o A$$

[0096] For substitution, the following values are used:

$L_1 = 2.931X\ 10^8\ H$

$L_2 = 6.437X\ 10^{10}\ H$

[0097] The data signal between the antenna and the tag is modulated by amplitude and coded by a Manchester encoding. Thus, manchester data= NRZ data 1\ (NRZ clock).

Multiple RF Chip Overview

[0098] Figure 17 illustrates an overview of the chip, according to one embodiment of the present invention. As described in detail above, the chip includes: an AC/DC converter (915 MHz) 1705 and accompanying power supply control unit 1715; a modular 1710; a codifier 1720; an AC/DC converter (13.56 MHz) 1745 and accompanying power supply control unit 1750; a decoder 1740; a security administrator 1755; an instruction sequencer 1730; a cryptographic block 1725, and memory 1735.

B. Method of Using a RF Border Crossing Control System

[0099] Figure 18 illustrates method for using an RF border crossing control system 1800, according to one embodiment of the present invention. In 1805, an RF decal is issued at the point of origin for each shipping component (e.g., tractor/cab; trailer/bed; containers). In 1810, data is written to the embedded chip using a computer (e.g., a PC) located at the point of origin. Electronic forms can be used to ensure consistency, accuracy and completeness in the information gathering and decal Issuance process. Information includes: specific details for identification and verification of the tractor, trailer, and containers; specific information on the driver including photo and biometric information (e.g., fingerprint); time stamp of when the driver, tractor, trailer, and containers leave the point of origin.

[00100] In 1815, a certified official (e.g., company official, customs agent) applies the RF decal to the shipping components (e.g., cab, trailer, containers) at the point of origin or other appropriate place. In 1820, the driver's personal data and shipment information are written to the driver's RF identification mechanism (e.g., laser card) at the point of origin or other appropriate place.

[00101] In 1825, at the point of entry or other appropriate place, RF antennas automatically read the RF decals as the vehicle approaches the custom's station and displays the data. A display screen on a computer (e.g., PC, PDA) in the customs area displays a reading of each RF decal as they pass within X number of feet of the antennas. The computer validates each RF decal by providing identification information (e.g., driver's photo, fingerprint, other data input at point of origin.) In 1830, the driver presents his RF laser card to a custom's officials at the point of entry (or other appropriate place) for validation and shipment verification. In 1835, the customs agent clears the shipping components for entry/exit and inputs this approval information to the RF card

and RF decal. If the vehicle requires additional customs inspections, the customs agent will assign the next inspection station information to the driver's RF card and RF decals.

[00102] In 1840, as an additional option, at the conclusion of the customs inspection process, and after all approval data is written to the RF decals, a final check is conducted at the port exit or other appropriate place. As the vehicle approaches the exit point, the RF decals are read for the final check to ensure all have matching data. This will be proof that the vehicle passed through all required checkpoints, inspections, and processing. As with the point of entry, each RF decal is read in sequence and the information is displayed to the custom agent's display screen. If any RF decal information does not match, the display will indicate a stop and the vehicle will be stopped for additional inspection or validation.

VI. SYSTEM AND METHOD FOR LIMITING SOFTWARE DOWNLOADS

[00103] One embodiment of the present invention relates to a de-metalizing edging process, and various resultant combinations of embedded processor chip, antenna, metallic hologram, integrated circuit, and substrate form factors to produce an end product (e.g., smart card or smart label). This enables RF communication within a networked system configured for various identification and verification applications. These security RF smart labels can be adapted to the identification and data capture requirements associated with unique software media or packaging of any software publisher, ISV or manufacturer.

A. System for Limiting Software Downloads

[00104] Figure 19 illustrates system for limiting software downloads, according to one embodiment of the present invention. The system includes a RF read/write device, an RF smart label with a chip and RF antenna, and the software.

[00105] The software media (e.g., a CD) and/or package carries an RF smart label, containing an RF antenna providing a link to a chip 1900. The chip has encryption and read/write capabilities. Access is controlled through a certificate of authenticity 1910. Working in combination with an RF reader/writer, the present invention will capture any available unique digital central processing unit (CPU) or processor number and read/write to an original certificate of authenticity. The system locks the certificate to the CPU or processor, and will not allow this unique software to be installed on any machine other than the one on which it was initially authorized to be loaded. This highly secure encrypted solution can also be used to

control access to customer support, debugs, updates and other services via the network (e.g., Internet) for authentic paid software licenses only. As described above, the chip includes a modulator 1905, encoder 1965, decoder 1940, instruction sequencer 1915, cryptographic block 1920, converter 1920, power control 1945, security management 1950, memory 1955, and antenna 1960.

[00106] **VPN Tunnel Mode**. The present invention can be incorporated into a network, such as a Virtual Private Network (VPN). A VPN is a private data network that makes use of the public telecommunication network or Internet infrastructure, maintaining privacy through the use of security and authentication procedures. A VPN is the emulation of a virtual private Wide Area Network (WAN) facility using Internet Protocol (IP) facilities. The VPN may use many aspects of networking, such as IP addressing, advertising reach ability, Quality of Service (QoS), data security and access control.

[00107] Figure 20 illustrates a VPN tunnel mode solution, according to one embodiment of the present invention. A database 2005 is connected to a security gateway 2015, which is connected to an application server 2010, connected to the client 2025 through a network 2020. Tunnel mode is used when one or more IP clients need to communicate to a main computer or server computer. The tunnel mode utilizes data encryption and key management. The VPN end points monitor the operation of the VPN tunnels (VPN clients) to ensure the connectivity has not been lost, and take appropriate action if there has been a failure. This is very important because all applications are dependent.

[00108] The present invention utilizes features that provide high-quality, interoperable cryptographic base security for access central information. For example, two traffic protocols are used: an Authentication Header (AH) that provides data integrity; and an Encapsulation Security Payload (ESP) that provides confidentiality (e.g., encryption of data), data integrity, and thought use of cryptographic-key management procedures. ESP is known as an Internet Key Exchange (IKE) protocol. This protocol negotiates the security association between two end points and exchanges keys between them.

[00109] There exist two operation modes for both AH and ESP: transport mode and tunnel mode. Transport mode is used to authenticate information transmitted between nodes or machines (e.g., computers, servers) on a WAN/LAN network. Tunnel mode is used for

communication between two or more end points that pass through a public network (e.g., the Internet). Tunnel mode is used to provide more security for information accessed by remote users or applications.

[00110] Figure 3A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in Figure 38.

B. Method of Limiting Software Downloads

[00111] Figure 21 illustrates method for limiting software downloads to authorized users 2100, according to one embodiment of the present invention. In 2105, a software license is issued with an RF device (including a chip with an RF antenna) to an authorized user for one computer. In 2110, when the user installs the software on a computer (e.g., computer #1), the RF device reads the computer's serial number from computer #1. In 2115, if the chip information on the RF device matches the information on computer #1, the software is installed. In 2120, as the software license in this case is for only one computer, the software will not be able to be installed on other computers until the software is removed from computer #1, when the serial number from computer #1 is erased. In an alternate embodiment, where a license is granted for X number of users, only X number of computer serial numbers will be able to be checked by the RF device, and thus only X users can download the software.

[00112] In additional embodiments, use of other unique identifying characteristics associated with other computer components (e.g., mouse, motherboard or central processing unit cabinet), can be utilized. In a further embodiment, the present invention is used for multi-license and corporate environments. In these cases, where an authorized corporate licensing entity with a registered billing address has access to software through a network (e.g., the Internet), the RF device limits the download of software to the number of users or units authorized under the license agreement. The present invention can control downloads to any computer, including central servers or individual PCs. This simple, yet highly secure kit locks the number of each CPU or processor for the central server and the PCs to the authorized number of users for each version of software, thus providing a seamless, secure upgrade capability. In an additional embodiment, the present invention provides an adapted PDA to provide additional support for software distribution and inventory control, as well as instant legal software authentication for law enforcement and industry piracy control.

VII. SYSTEM AND METHOD FOR AIRPORT SECURITY

[00113] The present invention is a scalable, end-to-end RF identification system for airport and air transport security and addresses, for example, the following issues: establishes the actual identity of a passenger; runs a hot file fingerprint search against the INS, CIA, INTERPOL, FBI databases; links passenger to boarding pass and checked/handheld baggage; cross-verifies passenger identification at strategic points within the airport environment; cross-verifies stowed baggage with boarded passengers; track individuals within the airport; highly secure, cost effective, and non-intrusive; enables speedy and accurate passenger processing. In a security system that ultimately extends to existing airline and government computer systems and databases, the present invention is the "final link" that allows designated security personnel to track and validate on the spot the status of persons or items throughout the airport environment.

[00114] While the invention is described in the context of airport security, those experienced in the art will see that any facility (e.g., train station, ship, company campus, university campus) with a need for security can use the present invention, and the present invention is not limited to use in an airport facility.

A. Airport Security System

[00115] Figure 22 illustrates a chip of an airport security system, according to one embodiment of the present invention. The present invention includes: an RF reader/writer; and an RF identification mechanism (e.g., RF boarding pass, RF luggage tags, RF identification cards) including an RF device. Alternatively, AFIS verification scanners, security and control software, and distributed databases can be included.

[00116] The RF reader/writer can comprise computer system components (e.g., remote readers/writers, verification scanners, client/server or thin client systems and networks, and application software and databases).

[00117] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz.

[00118] The chip contains unique identifying data for persons or items subject to scrutiny, and can be read by nearby security or other control personnel with handheld or stationary RF reader/writer or RF reader/writer devices for real time validation. Furthermore, the RF device is manufactured with light diffraction and other high security print features that eliminate document

forgery and enable instant visual verification of authenticity. The RF device also includes an integrated AFIS digital fingerprint capability. The present invention can also use other unique identifying characteristics associated with additional elements of the air transport industry, including cargo, flight services, maintenance, and aircraft parts.

[00119] As described above, the chip has a memory 2205 (e.g., 2k), an option hardware wired cryptographic block 2210 (with 4 exchange encrypted keys with up to 256 bits), a modulator 2215, a converter 2220, an encoder 2225, a power control2230, an instruction sequencer 2260, a decoder 2245, a security management unit 2255, a memory 2205.

B. Method of Airport Security

[00120] Figure 23 illustrates a method of airport security, according to one embodiment of the present invention. In 2305, to facilitate air travel security, passengers are issued an official RF air travel identification card (e.g., with a photo and fingerprint scan) by a federal authority or the airlines following an agreeable level of background check. This process could be as simple as checking names verified by some acceptable identification (e.g., drivers' license, passport) against a networked hot list. The identification data is read and locked to the RF air travel identification card. During processing and prior to issuance, applicants' biometrics are processed and compared with a "one-to-many" hot list. With a successful security check, the applicant is issued a highly secure identification document with unique visual, biometric, and descriptive data that can be quickly verified throughout the airport and across the air travel system. A similar process would be applied to airport, airline, and service personnel. Those experienced in the art will note that a general RF identification card or mechanism (e.g., PDA) can be used instead of specific air travel RF identification card.

[00121] In 2310, a passenger presents the RF air travel identification card or other RF identification mechanism to the airline authority when traveling. In 2315, the agent scans the RF air travel identification card. In 2320, the RF boarding pass and RF baggage tags are printed for the passenger. The boarding card now contains all data and tracking mechanisms required for secure passenger access to the gate and the matching aircraft, as well as boarding verification. In an alternative embodiment, instead of issuing an RF boarding pass, the RF air travel identification card can also contain e-ticket information. In parallel to the issuance of the boarding pass, identity information is captured by the system and digitally copied, together with

the relevant travel route and destination data onto the RF baggage tags. The RF baggage tags are printed through systems and printers enhanced with an RF identification write device. The RF baggage tag now contains all data and tracking mechanisms required to link passenger, bag, and flight, thus enabling verifiable passenger/baggage/flight cross-referencing to the matching aircraft.

CONCLUSION

[00122] Additional advantages and novel features of the invention will be set forth in part in the Attachments that follow, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

What is claimed

1. A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database.

5. The mobile device of claim 4, wherein the POS device includes an RF reader.

6. The mobile device of claim 4, wherein the central database is configured to validate the key and the payment information.

7. The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. The system of claim 10, wherein the payment information is associated with a primary account number.

13. The system of claim 10, wherein the POS device includes an RF reader.

14. The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

.

ABSTRACT

The present invention provides a method and system for verifying and tracking transactional information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Li Zhang/cindy guido
Attorney Docket Number:	116546-661CT2

Filed as Large Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Request for Prioritized Examination	1817	1	4000	4000
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**5740**

Electronic Acknowledgement Receipt

EFS ID:	21785734
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Li Zhang/cindy guido
Filer Authorized By:	Li Zhang
Attorney Docket Number:	116546-661CT2
Receipt Date:	16-MAR-2015
Filing Date:	
Time Stamp:	21:17:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$5740
RAM confirmation Number	6829
Deposit Account	502075
Authorized User	ZHANG, LILY

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	116546_661CT2_ADS_Track_One.PDF	1562012 952f8d2e9c2caa1246efb153fbe8d361683a3162	no	8
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	116546_661CT2_IDS.PDF	614525 83324dbf630f93523eccae43554f27de01903b91	no	11
Warnings:					
Information:					
A U.S. Patent Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
3	Foreign Reference	WO2004006165.pdf	8287414 ccf962b357649501ea161f180ab49d88d34d635d	no	94
Warnings:					
Information:					
4	Foreign Reference	JP2002042076A.pdf	6062031 aef9cae27c68146ab1bd10929b9bb097cc6dd2bf	no	9
Warnings:					
Information:					
5	Foreign Reference	DE19608757A1.pdf	6243657 3e48af78b06995e4c9478d53a48ebeda79b7d8b0	no	6
Warnings:					
Information:					
6	Foreign Reference	DE10042805A1.pdf	12644805 15185b18f8ef4d7216e6a390bdac05b6f68049fa	no	12
Warnings:					
Information:					
7	Foreign Reference	WO9843104.pdf	4029432 14b5aae0082493ceeafdf3e529347bcd5208fb21	no	38
Warnings:					

Information:					
8	Foreign Reference	EP0993999A2.pdf	12611327 2c543c3aef63239bacf9e9cbb1ad0f814ac84cbb	no	10
Warnings:					
Information:					
9	Foreign Reference	EP0977145A2.pdf	5553821 b603626f49c6b57760f8e642c9acc5ae2730aa71	no	43
Warnings:					
Information:					
10	Non Patent Literature	Atmel.pdf	3746076 bfe124125d345ba7ab49937ff63aa0c06442ea80	no	12
Warnings:					
Information:					
11	Foreign Reference	ESR_101820330.pdf	317655 4cf3a9bd1f8846735118ed0bb4249bee9724f240	no	7
Warnings:					
Information:					
12	Non Patent Literature	Fancher.pdf	1969166 f6b7bd9680c8440ca470d201b40603bf72ca4d5c	no	7
Warnings:					
Information:					
13	Non Patent Literature	Rakers.pdf	654929 82eeacb26ccd13a1c3d9e4734085e71a50f25e32	no	7
Warnings:					
Information:					
14	Foreign Reference	JPOA_2004519130.pdf	263172 b9a532720615c437f12b4d24befa6d6e59b37b93	no	3
Warnings:					
Information:					
15	Non Patent Literature	Anonymous_Security.pdf	173413 d75cb61523a2b6c9a1bb2509a01e0f46e5e7d20d	no	1
Warnings:					
Information:					
16	TrackOne Request	116546_661CT2_Track_One_Form.PDF	113964 f246ea20949344279c043917dfcba7bd17327966	no	2
Warnings:					

Information:					
17	Drawings-only black and white line drawings	116546_661CT2_Figures.PDF	327595 443d55d1f1a6c41552e03fe0886952 2aa8670ef1	no	24
Warnings:					
Information:					
18		116546_661CT2_Specification.PDF	261785 3132c644d37fe0ac5deb8f8abd0b34f6b4826a10	yes	39

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	35
	Claims	36	38
	Abstract	39	39

Warnings:					
Information:					
19	Fee Worksheet (SB06)	fee-info.pdf	38552 02d26b1ae66915f1794c7567b30155021a8b25af	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	65475331		

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

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

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

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

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Francisco		Martinez de Velasco Cortina	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	La Jolla	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	12760 Danielson Ct.		
Address 2	Suite A		
City	Poway	State/Province	CA
Postal Code	92064	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Manfred		Rietzler	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Marktoberdorf	Country of Residence i	DE

Mailing Address of Inventor:

Address 1	Am Alsterberg 11		
Address 2			
City	Marktoberdorf	State/Province	
Postal Code	87616	Country i	DE

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ **An Address is being provided for the correspondence Information of this application.**			
Customer Number	27189		
Email Address	docketing@procopio.com	Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS		
Attorney Docket Number	116546-661CT2	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	24	**Suggested Figure for Publication (if any)**	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	27189		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14585057	2014-12-29

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14585057	Continuation of	14028469	2013-09-16	8933807	2015-01-13

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14028469	Continuation of	13350665	2012-01-13	8587436	2013-11-19

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13350665	Continuation of	13175768	2011-07-01	8237568	2012-08-07

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13175768	Continuation of	12688666	2010-01-15	8004410	2011-08-23

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12688666	Continuation of	11279912	2006-04-17	7671746	2010-03-02

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11279912	Continuation of	10615026	2003-07-09	7081819	2006-07-25

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10615026	Claims benefit of provisional	60394241	2002-07-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i]the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	Neology, Inc.

Mailing Address Information:

Address 1	12760 Danielson Ct., Suite A		
Address 2			
City	Poway	**State/Province**	CA
Country [i]	US	Postal Code	92064
Phone Number		Fax Number	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/li zhang/			Date (YYYY-MM-DD)	2015-03-16
First Name	Li	Last Name	Zhang	Registration Number	70902

Additional Signature may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-661CT2
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SCORE Placeholder Sheet for IFW Content

Application Number: 14659502 Document Date: 03/16/2015

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 03/26/2015

MTEKLEMI SALE #00000014 Mailroom Dt: 03/16/2015 502075 14659502
01 FC : 1051 140.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/659,502

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	16 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

APPLICATION AS AMENDED - PART II

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

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/659,502	03/16/2015	2683	1740	116546-661CT2	16	2

CONFIRMATION NO. 3012

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

FILING RECEIPT

OC000000074248176

Date Mailed: 03/30/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Francisco Martinez de Velasco Cortina, La Jolla, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

Applicant(s)

Neology, Inc., Poway, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/585,057 12/29/2014
which is a CON of 14/028,469 09/16/2013 PAT 8933807
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 03/25/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/659,502**

Projected Publication Date: 07/09/2015

Non-Publication Request: No

Early Publication Request: No
Title

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Preliminary Class

340

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2

CONFIRMATION NO. 3012

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

NOTICE

OC00000074248177

Date Mailed: 03/30/2015

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

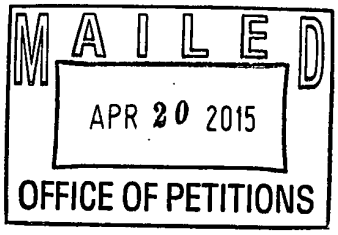
The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Francisco Martinez de Velasco Cortina
  Manfred Rietzler

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO CA 92101



Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.:14/659,502

1. THE REQUEST FILED March 16, 2015 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Kimberly Inabinet at 571-272-4618.

/ Kimberly Inabinet/ Paralegal Specialist, Office of Petitions

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2	3012

27189 7590 06/22/2015

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/22/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 14/659,502	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *March 16, 2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *March 16, 2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *March 16, 2015*.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) ☒ Other: *Smart Card Technology Past Present and Future. Understanding the requirements of ISO IEC 14443, RFID Handbook Active Load Modulations*.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-16 have been examined in this application. This communication is the first action on the merits (FOAM). An Information Disclosure Statement (IDS), submitted 03/04/2015, has been considered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4-5, 10, and 13 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

5. Per claims 4-5, 10, and 13, the claims are directed to a point of sale (POS) terminal. Claims 1 and 10 are directed to "A mobile device," see lines 2 on page 36 and line 10 on page 37. The claim limitations directed to other matters than a "mobile device" render the claims indefinite.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

JUDICIAL EXCEPTIONS TO SECTION 101

8. The Supreme Court held that the patent claims in Alice Corporation Pry. Ltd. v. CLS Bank International, el al. ("Alice Corp. ") are not patent-eligible under 35 U.S.C. § 101. 10. The Supreme Court made clear in Alice Corp. that it applies the framework set forth in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. _ (2012) (Mayo), to analyze all claims directed to laws of nature, natural phenomena, and abstract ideas for subject matter eligibility under 35 U.S.C. § 101. This framework is currently being used by the USPTO to examine claims involving laws of nature, but had not been used for claims involving abstract ideas. Therefore, the following instructions differ from prior USPTO guidance in two ways:

9. Alice Corp. establishes that the same analysis should be used for all types of judicial exceptions, whereas prior USPTO guidance applied a different analysis to claims with abstract ideas (Bilski guidance in MPEP 2106(11) (B)) than to claims with laws of nature (Mayo guidance in MPEP 2106.01).

10. Alice Corp. also establishes that the same analysis should be used for all categories of claims (e.g., product and process claims), whereas prior guidance applied a different analysis to product claims involving abstract ideas (relying on tangibility in MPEP 2106(II) (A)) than to process claims (Bilski guidance).

ALICE V. CLS BANK: TWO-PART ANALYSIS

11. Following Alice Corp, all claims (product and process) having an abstract idea must be analyzed using the following two-part analysis set forth in Mayo. For additional guidance, see "2014 Interim Guidance on Patent Subject Matter Eligibility" December 16, 2014.

12. Limitations referenced in Alice Corp. that may be enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

a. Improvements to another technology or technical fields;

b. Improvements to the functioning of the computer itself;

c. Applying the judicial exception with, or by use of, a particular machine; effecting a transformation or reduction of a particular article to a different state or thing; adding a specific limitation other than what is well-understood, routine and conventional in the field, or adding unconventional steps that confine the claim to a particular useful application.

13. Limitations referenced in Alice Corp. that are not enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

d. Adding the words "apply it" (or an equivalent) with an abstract idea, or mere instructions to implement an abstract idea on a computer;

e. Requiting no more than a genetic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. See also, MPEP 2106(1).

14. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

15. Claim(s) 1-16 are directed to an abstract idea of essentially conducting a payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice.

16. The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than significantly more than the abstract idea itself. The claims do not include limitations that meet the criteria required to determine the claims as a whole amounting to significantly more than the judicial exception itself (**see paragraph 12, a-c**). This is evident by the description, see paragraph 0067, stating "the RF cellular telephone 1205 can include the following: a fingerprint identifier… chip… and an RF device… to store identification information…"

17. The method steps amount to mere instructions to implement the idea on a generic computer or mobile device structure that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry, do not add meaningful limitations to the method as they would be routinely used by those of ordinary skill in the art in order to apply the correlation and yield predictable results. The functions performed by the "mobile device" and "module(s)" appear to be conventional and routine carried out by a general purpose computer or general mobile device. Moreover, the claims do not appear to improve the functioning of the "mobile device" and "module(s)" or

effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. One of ordinary skill in the art is able to readily understand the invention and carry out the recited limitations in order to apply the correlation using a generic computer or computers with instructions.

Claim Rejections - 35 USC § 103

18. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-6, 8-13, 15-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. (herein after referred to as simply Walker), in view of U.S. Patent 6,848,048 to Holmes (herein after referred to as simply Holmes), in further view of U.S. Patent 5,590,197 to Chen et al. (herein after referred to as simply Chen).

20. Per claim 1, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

c. Memory (memory) configured to store biometric authentication information (biometric information) and payment information (account number) [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

d. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory (processor); and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6].

f. a secure module configured to (processor) [Walker, Abstract]:

g. generate a key (generates a single use credit card number) when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory [Col. 5, Ln. 49- , Col. 6, Ln. 1-38 and Figures 1-9];

h. Walker, in view of Holmes do not explicitly teach encrypt the key and the payment information stored in memory [Walker, Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Chen does (encrypting the ticket using a public key) [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the generated key including the payment information in motivation of increasing security measures.

i. Walker does not explicitly teach provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches [...] via the short range RF circuitry [...] (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

Chen teaches provide, [...] the encrypted key and payment information for use in a transaction [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to provide a communication link that is a short range RF circuitry in motivation of increasing security measures.

Also, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Chen to provide over the communication link the encrypted key and payment information for use in a transaction in motivation of increasing security measures.

Examiner notes that the following limitation is an intended use limitation, "for use in a transaction."

21. Per claims 2 and 11, Walker teaches wherein the biometric module is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-9].

22. Per claims 3 and 12, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

23. Per claim 4, Walker teaches [...] a point of sale (POS) device [...] (merchant terminal, a terminal is a device) [...] [Col. 6, Ln. 39-53, Col. 8, Ln. 33-39].

Walker does not explicitly teach wherein the secure module is configured to provide the encrypted key and payment information [...], and wherein the POS device (merchant) is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database (account servicer); however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to transmit the encrypted key to a point of sale terminal, have the terminal receive the encrypted data and transmit this data to a central database (account servicer) in motivation of increasing security measures.

The above limitation is an intended use limitation.

24. Per claims 5 and 13, Walker does not explicitly teaches wherein the POS device includes an RF reader; however, Holmes does [Col. 1, Ln. 60-63, Col. 2, Ln. 34-61, Col. 4-5, Ln. 62-, 1-21 and Figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to insure that the POS includes an RF reader, in motivation of facilitating communication measures while enhancing security measures.

25. Per claim 6, Walker teaches wherein the central database (credit card issuer) is configured to validate the key and the payment information [Abstract, Col. 8, Ln. 33-67 and Figures 1-9].

26. Per claims 8 and 15, Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the secure module (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

27. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes in order to utilize radio frequency identification as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

28. Per claim 10, Walker teaches

a. A system, comprising [Abstract]:

b. a mobile device, comprising [Abstract]:

c. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

d. memory configured to store biometric authentication information and payment information, [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

e. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

f. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6]

g. a secure module configured to (processor) [Walker, Abstract]:

h. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; [Col. 6, Ln. 14-38 and Figures 1-3];

i. Walker, in view of Holmes do not explicitly teach encrypt the key and the payment information stored in memory [Walker, Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Chen does (encrypting the ticket using a public key) [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the generated key including the payment information in motivation of increasing security measures.

j. Walker does not explicitly teach provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches [...] via the short range RF circuitry [...] (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

Chen teaches provide [...] the encrypted key and payment information for use in a transaction [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to provide a communication link that is a short range RF circuitry in motivation of increasing security measures.

Also, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Chen to provide over the communication link the encrypted key and payment information for use in a transaction in motivation of increasing security measures.

Examiner notes that the following limitation is an intended use limitation, "for use in a transaction."

k. Walker teach a point of sale (POS) device (terminal / merchant terminal) configured to [Col. 6, Ln. 39-53, Col. 8, Ln. 33-39]:

l. Walker does not explicitly teach receive, from the secure module, the encrypted key and payment information; however Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teaching of Chen to include the receiving from the secure module, the encrypted key and payment information in motivation of processing the transaction while increasing security measures.

m. Walker does not explicitly teach transmit, to a central database (account servicer), the encrypted key and payment information; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1]; and

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to transmit the encrypted key to a central database (account servicer) in motivation of increasing security measures.

n. Walker does not explicitly teach a central database configured to validate the key and the payment information; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to have the central database (account servicer) validate the key and payment information in motivation of increasing security measures.

29. Claims 7 and 14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes and Chen as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

30. Per claims 7 and 14, Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes and Chen to include the teachings of Voltmer to store the data in partitions or separately in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

31. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

32. Claims 1-16 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14639034 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

33. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/639034 recite:

a. A mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is successfully authenticated;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

Claim 10:

a. A system, comprising:

b. a mobile device, comprising:

c. short range radio frequency (RF) circuitry;

d. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

e. a biometric module configured to read biometric information;

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

g. a secure module configured to:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

j. a point of sale (POS) device configured to:

k. receive, from the secure module, the encrypted key and payment information; and

l. transmit, to a central database, the encrypted key and payment information; and

m. a central database configured to validate the key and the payment information.

34. Claims 1 and 10 of co-pending application 14/639034 differ since they further recite additional claim limitations including associating the biometric authentication information with the payment information, authentication based biometric module associated with the payment information and stored biometric data. However, it would have been obvious to a person of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/639034 by removing the limitations directed to the memory and authentication resulting generally in the claims of the instant application since the claims of the instant application and the claim recited in co-pending application 14/639034 actually perform a similar function. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements

perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

35. Also, claims 1 and 10 of co-pending application 14/639034 differ since they fails to recite generating a key by determining that the biometric authentication information stored in memory corresponds to the biometric information read. Walker discloses generating a key once comparing the scanned biometric data to the stored biometric data matches (generating a single use credit card number once user scans biometrics, card compares to data in memory and generates single use credit card number) [Col. 5, Ln. 49-, Col. 6, Ln. 1-38 and Figures 1-9]. It would have been obvious to one of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/639034 and include the function of comparing the stored biometric data to the scanned data to generate a key as taught by Walker in motivation of preventing unauthorized use of the device by those that are not permitted (increase security measures).

36. Claims 1-16 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 2-17 of copending Application No. 14/321781 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

37. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 2 and 11 of co-pending application 14/321781 recite:

a. A mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is successfully authenticated;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction

Claim 11:

a. A system, comprising:

b. a mobile device, comprising:

c. short range radio frequency (RF) circuitry;

d. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

e. a biometric module configured to read biometric information;

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

g. a secure module configured to:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

j. a point of sale (POS) device configured to:

k. receive, from the secure module, the encrypted key and payment information; and

l. transmit, to a central database, the encrypted key and payment information; and

m. a central database configured to validate the key and the payment information

38. Claims 2 and 11 of co-pending application 14/321781 differ since they further recite additional claim limitations including associating the biometric authentication information with the payment information, authentication based biometric module associated with the payment information and stored biometric data. However, it would have been obvious to a person of ordinary skill in the art to modify claims 2 and 11 of co-pending application 14/321781 by removing the limitations directed to the memory and authentication resulting generally in the claims of the instant application since the claims of the instant application and the claim recited in co-pending application 14/321781 actually perform a similar function. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements

perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

39. Also, claims 1 and 10 of co-pending application 14/321781 differ since they fails to recite generating a key by determining that the biometric authentication information stored in memory corresponds to the biometric information read. Walker discloses generating a key once comparing the scanned biometric data to the stored biometric data matches (generating a single use credit card number once user scans biometrics, card compares to data in memory and generates single use credit card number) [Col. 5, Ln. 49-, Col. 6, Ln. 1-38 and Figures 1-9]. It would have been obvious to one of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/321781 and include the function of comparing the stored biometric data to the scanned data to generate a key as taught by Walker in motivation of preventing unauthorized use of the device by those that are not permitted (increase security measures).

Conclusion

40. The prior art made of record and not relied upon, see PTO-892, is considered pertinent to applicant's disclosure.

41. Examiner notes:

Smart cards or any mobile device, which incorporates an antenna to allow RFID communication with a terminal or Point of sale or another device is well described in "the RFID Handbook" which was published in March 1998 (http://rfid-handbook.de/the-book.html).

42. It is well known and routine in the art to conform to established standards, such as ISO/IEC 14443, in order to conduct a transaction and process the transaction using a contactless device. See attached reference ISO/IEC 14443.

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
06/01/2015

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/659,502	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,163,771 A	12-2000	Walker et al.	705/18
*	B	US-6,848,048 B1	01-2005	Holmes, William S.	713/162
*	C	US-7,911,643 B2	03-2011	Yamada et al.	358/1.9
*	D	US-5,590,197	12-1996	Chen et al.	705/65
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	RFID Handbook - Active Load Modulation
	V	Smart Card Technology Past Present and Future Mohammed 2004
	W	Understanding the Requirements of ISO IEC 14443
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14659502	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/02/2015								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O./	1	8548927	B2	2013-10-01	Beenau et al.	
/E.O./	2	8401539	B2	2013-03-19	Beenau et al.	
/E.O./	3	8126449	B2	2012-02-28	Beenau et al.	
/E.O./	4	8041815	B2	2011-10-18	Bahl et al.	
/E.O./	5	8004410	B2	2011-08-23	Martinez de Velasco Cortina et al.	
/E.O./	6	7980378	B2	2011-07-19	Jones et al.	
/E.O./	7	7844505	B1	2010-11-30	Arneson et al.	
/E.O./	8	7671746	B2	2010-03-02	Martinez de Velasco Cortina et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	9	7533809	B1	2009-05-19	Robinson et al.	
/E.O./	10	7487538	B2	2009-02-03	Mok	
/E.O./	11	7310734	B2	2007-12-18	Boate et al.	
/E.O./	12	7225337	B2	2007-05-29	Baessler	
/E.O./	13	7080819	B2	2006-07-25	Tojo	
/E.O./	14	7031946	B1	2006-04-18	Tamai et al.	
/E.O./	15	6975834	B1	2005-12-13	Forster	
/E.O./	16	6950013	B2	2005-09-27	Scaman et al.	
/E.O./	17	6894615	B2	2005-05-17	Look	
/E.O./	18	6850147	B2	2005-02-01	Prokoski	
/E.O./	19	6793134	B2	2004-09-21	Clark	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	20	6758405	B2	2004-07-06	Look	
/E.O./	21	6753759	B2	2004-06-22	Stegmaier et al.	
/E.O./	22	6698653	B1	2004-03-02	Diamond et al.	
/E.O./	23	6617961	B1	2003-09-09	Janssen et al.	
/E.O./	24	6570487	B1	2003-05-27	Steeves	
/E.O./	25	6427504	B1	2002-08-06	Janssen et al.	
/E.O./	26	6388579	B1	2002-05-14	Adcox et al.	
/E.O./	27	6360208	B1	2002-03-19	Ohanian et al.	
/E.O./	28	6340116	B1	2002-01-22	Cecil et al.	
/E.O./	29	6334059	B1	2001-12-25	Stilp et al.	
/E.O./	30	6276607	B1	2001-08-21	Sato	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	31	6275157	B1	2001-08-14	Mays et al.	
/E.O./	32	6269292	B1	2001-07-31	Kokubu et al.	
/E.O./	33	6268796	B1	2001-07-31	Gnadinger et al.	
/E.O./	34	6211790	B1	2001-04-03	Radomsky et al.	
/E.O./	35	6203952	B1	2001-03-20	O'Brien et al.	
	36					
	37					
/E.O./	38	6182894	B2	2001-02-06	Hackett et al.	
/E.O./	39	6175922	B1	2001-01-16	Wang	
/E.O./	40	6167333	A	2000-12-26	GEHLOT; NARAYAN L. et al.	
/E.O./	41	6157333	A	2000-12-05	Louagie et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	42	6140941	A	2000-10-31	Dwyer et al.	
/E.O./	43	6111506	A	2000-08-29	YAP; CHAS HOCK ENG et al.	
/E.O./	44	6104281	A	2000-08-15	HEINRICH; HARLEY KENT et al.	
/E.O./	45	6098879	A	2000-08-08	TERRANOVA; STEVEN N. et al.	
/E.O./	46	6073840	A	2000-06-13	MARION; KENNETH O. et al.	
/E.O./	47	6052068	A	2000-04-18	PRICE R et al.	
/E.O./	48	6025784	A	2000-02-15	Mish	
/E.O./	49	6025780	A	2000-02-15	BOWERS; JOHN H. et al.	
/E.O./	50	5974500	A	1999-10-26	MALETSKY; KERRY D. et al.	
/E.O./	51	5874896	A	1999-02-23	Lowe et al.	
/E.O./	52	5864580	A	1999-01-26	Lowe et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	53	5787174	A	1998-07-28	TUTTLE JOHN R	
/E.O./	54	5742618	A	1998-04-21	Lowe	
/E.O./	55	5657008	A	1997-08-12	Bantli	
/E.O./	56	5552789	A	1996-09-03	Schuermann	
/E.O./	57	4529870	A	1985-07-16	CHAUM DAVID	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O./	1	20100095130	A1	2010-04-15	Bertran et al.	
/E.O./	2	20100094754	A1	2010-04-15	Bertran et al.	
/E.O./	3	20050149764	A1	2005-07-07	Bahl et al.	
/E.O./	4	20030200227	A1	2003-10-23	Ressler	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	5	20030074317	A1	2003-04-17	Hofi	
/E.O./	6	20020109580	A1	2002-08-15	Shreve	
/E.O./	7	20020089434	A1	2002-07-11	Ghazarian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/E.O./	1	2004006165	WO	A1	2004-01-15	BNC IP SWITZERLAND GMBH		☐
/E.O./	2	2002042076	JP	A	2002-02-08	DAINIPPON PRINTING CO LTD		☒
/E.O./	3	19608757	DE	A1	1997-09-11	BROSOW, JOERGEN		☒
/E.O./	4	10042805	DE	A1	2002-03-14	BUNDESDRUCKEREI GMBH		☒
/E.O./	5	9843104	WO	A2	1998-10-01	PRICE, Frederick, J., R-W.		☐
/E.O./	6	0993999	EP	A2	2000-04-19	FORD MOTOR CO		☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

/E.O./	7	0977145	EP	A2	2000-02-02	KABUSHIKI KAISHA TOSHIBA		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	~~Atmel Corporation, Silicon solutions making smart cards smarter, 2000, 12 pages.~~	☐
	2	Extended European Search Report received in European patent application no. 10182033.0, dated January 13, 2012, 7 pages.	☐
	3	FANCHER, CAROL HOVENGA, In your pocket smartcards, February 1997, 7 pages.	☐
	4	~~RAKERS ET AL., Secure contactless smartcard ASIC with DPA protection, March 2001, 7 pages.~~	☐
	5	Japanese Office Action received in Japanese patent application no. 2004-519130, dated May 12, 2009, 3 pages (including partial English translation).	☒
	6	Anonymous, Read/write RFID offers standalone advantages, Security, August 1996, 1 page.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/El Mehdi Oussir/	Date Considered	06/02/2015

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

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/16/2015	Application Number	14659502 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-661CT2

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S26	51	S25 and @pd<"20020101"	US-PGPUB;	OR	ON	2015/05/18 16:26

			USPAT			
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S31	4128	((generate) near2 (key pin code token password)) with ((encrypt) near3 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S37	63	S35 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:24
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44

6/13/2015 6:36:34 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3012

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/659,502	03/16/2015	705	3685	116546-661CT2

APPLICANTS

Neology, Inc., Poway, CA;

INVENTORS

Francisco Martinez de Velasco Cortina, La Jolla, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

**** CONTINUING DATA ***************************

This application is a CON of 14/585,057 12/29/2014
which is a CON of 14/028,469 09/16/2013 PAT 8933807
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

03/25/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /EL MEHDI OUSSIR/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	24	16	2

ADDRESS

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101
UNITED STATES

TITLE

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

FILING FEE RECEIVED		
1740	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14659502	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	6/1/2015	EO
H04L	6/1/2015	EO

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705		6/1/2015	EO

SEARCH NOTES		
Search Notes	Date	Examiner
Consulted J. Hayes D.P rejection	6/2/2015	EO
Consulted Clavin H.	6/12/2015	EO
Google search	6/4/2015	EO
East search	6/4/2015	EO

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/EL MEHDI OUSSIR/ Examiner.Art Unit 3685	

PTO/AIA/01 (08-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 14/659,502 filed on March 16, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

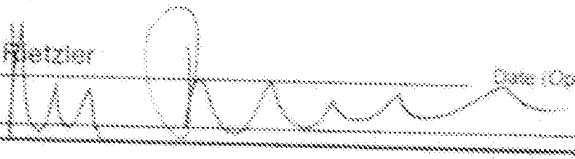
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Manfred Hietzler

Signature:  Date (Optional): _____

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/659,502

filed on March 16, 2015

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Francisco Martinez de Velasco Cortina Date (Optional): 5-12-2015

Signature:

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Acknowledgement Receipt

EFS ID:	22732469
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-661CT2
Receipt Date:	24-JUN-2015
Filing Date:	16-MAR-2015
Time Stamp:	18:25:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	116546_661CT2_Declarations_Signed.PDF	2275625 f2a97bd42ea961a44a7bbd36d75e1d0476c3fc3c	no	2

Warnings:

Information:

Total Files Size (in bytes):	2275625

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

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

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

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

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated with Customer Number: 27189

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☒ The address associated with Customer Number: 27189

OR

☐	Firm or Individual Name		
	Address		
	City	State	Zip
	Country		
	Telephone	Email	

Assignee Name and Address: NEOLOGY, INC.
12760 DANIELSON CT.
SUITE A
POWAY, CALIFORNIA 92064

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	10-30-2014
Name	Francisco Martinez de Velasco Cortina	Telephone	(858) 391-0260
Title	CEO of NEOLOGY, INC.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Acknowledgement Receipt

EFS ID:	22732769
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-661CT2
Receipt Date:	24-JUN-2015
Filing Date:	16-MAR-2015
Time Stamp:	18:46:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Assignment_signed_116546-661CT2.PDF	288064 2a05ba4ba62f9fcced1f146b7aa188abae05905d	no	2

Warnings:	
Information:	

2	Assignee showing of ownership per 37 CFR 3.73	373b_116546_661CT2.PDF	117303 6e3fdd101280fcd70e20bb409e6abcdea2093370	no	3
Warnings:					
Information:					
3	Power of Attorney	116546_680UT1_POA.PDF	504758 0409df170d3176c3b65f4034b556d9389a94e205	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	910125		

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

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

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

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

Assignment

WHEREAS, WE, **Francisco Martinez de Velasco Cortina** of La Jolla, California and **Manfred Rietzler** of Marktoberdorf, Germany (hereinafter called "ASSIGNORS"), have invented certain improvements in **SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS** for which we have prepared an application for Letters Patent of the United States of America; and

WHEREAS, **Neology, Inc.** (hereinafter called "ASSIGNEE), a corporation, with its principal place of business at 12760 Danielson Ct., Suite A, Poway, California 92064, desires to acquire the entire right, title, and interest in the application and invention, and to any United States patents to be obtained therefor;

We, the above named assignors, hereby sell, assign and transfer to the above named assignee, its successors and assigns, the entire right, title and interest in the application and the invention disclosed therein for the United States of America, including all divisions, and continuations thereof, and all Letters Patent of the United States that may be granted thereon, and all reissues thereof, and all countries foreign thereto, including rights of priority under the International Convention of Paris (1883) as amended, including the right to claim priority under 35 U.S.C. §119, and We request the Director of the U.S. Patent and Trademark Office to issue any Letters Patent granted upon the invention set forth in the application to the assignee, its successors and assigns; and We hereby agree that the assignee may apply for foreign Letters Patent on the invention and We will execute without further consideration all papers deemed necessary by the assignee in connection with the United States and foreign applications when called upon to do so by the assignee.

WE hereby authorize and request the attorneys of PROCOPIO, CORY, HARGREAVES & SAVITCH LLP of 525 B Street, Suite 2200, San Diego, California 92101, USA to insert here in parentheses (Application number 14/659,502 and Confirmation number 3012, filed March 16, 2015) the application number, confirmation number and filing date of said application when known.

*Date: 5-12-2015

s/ Francisco Martinez de Velasco Cortina

*Date:

s/ Manfred Rietzler

*Signatures must be dated.

(Legalization not required for recording but is prima facie evidence of execution under 35 U.S.C. §261)

Assignment

WHEREAS, WE, **Francisco Martinez de Velasco Cortina** of La Jolla, California and **Manfred Rietzler** of Marktoberdorf, Germany (hereinafter called "ASSIGNORS"), have invented certain improvements in **SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS** for which we have prepared an application for Letters Patent of the United States of America; and

WHEREAS, **Neology, Inc.** (hereinafter called "ASSIGNEE"), a corporation, with its principal place of business at 12760 Danielson Ct., Suite A, Poway, California 92064, desires to acquire the entire right, title, and interest in the application and invention, and to any United States patents to be obtained therefor;

We, the above named assignors, hereby sell, assign and transfer to the above named assignee, its successors and assigns, the entire right, title and interest in the application and the invention disclosed therein for the United States of America, including all divisions, and continuations thereof, and all Letters Patent of the United States that may be granted thereon, and all reissues thereof, and all countries foreign thereto, including rights of priority under the International Convention of Paris (1883) as amended, including the right to claim priority under 35 U.S.C. §119, and We request the Director of the U.S. Patent and Trademark Office to issue any Letters Patent granted upon the invention set forth in the application to the assignee, its successors and assigns; and We hereby agree that the assignee may apply for foreign Letters Patent on the invention and We will execute without further consideration all papers deemed necessary by the assignee in connection with the United States and foreign applications when called upon to do so by the assignee.

WE hereby authorize and request the attorneys of PROCOPIO, CORY, HARGREAVES & SAVITCH LLP of 525 B Street, Suite 2200, San Diego, California 92101, USA to insert here in parentheses (Application number 14/659,502 and Confirmation number 3012, filed March 16, 2015) the application number, confirmation number and filing date of said application when known.

*Date:

s/ Francisco Martinez de Velasco Cortina

*Date: 10/15/2015

s/ Manfred Rietzler

*Signatures may be dated

(Legalization not required for recording but is prima facie evidence of execution under 35 U.S.C. §261)

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office;U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of1995, no persons arerequired to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: NEOLOGY, INC.

Application No./Patent No.: 14659502 Filed/Issue Date: March 16, 2015

Titled: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

NEOLOGY,INC., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by37 CFR3.73(b). The information is required toobtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentialityis governed by35 U.S.C. 122and 37 CFR1.11 and1.14. Thiscollection is estimated to take 12 minutes to complete, including gathering, preparing, and submittingthe completed application form to the USPTO.Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent tothe Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.**SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

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

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Noel C. Gillespie/	June 26, 2015
Signature	Date
Noel C. Gillespie	47596
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that yoube given certain informationin connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, pleasebe advised that: (1) the general authority forthe collection of thisinformation is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and(3) the principal purpose forwhich the information isused by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent applicationor patent. If you do not furnish the requested information,the U.S. Patent and Trademark Office may not be able to process and/or examineyour submission,which may result in termination of proceedings or abandonment of the applicationor expiration of the patent.

The informationprovided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the informationin order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an InternationalApplication filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, arecord may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from thissystem of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2

CONFIRMATION NO. 3012

POA ACCEPTANCE LETTER

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

OC000000076040445

Date Mailed: 07/01/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/24/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/qtran/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2

CONFIRMATION NO. 3012

PUBLICATION NOTICE

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

OC000000076185540

Title:SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Publication No.US-2015-0193766-A1
Publication Date:07/09/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

OPAP AKIMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Francisco Martinez de Velasco Cortina		
Application No.:	14/659,502	Examiner:	OUSSIR, EL MEHDI
Filing Date:	March 16,2013	Group Art Unit:	3685
Confirm. No.	3012	Attorney Docket No.	116546-661CT2

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Sir:

In response to the Non-Final Office Action of June 22, 2015, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following submission, where:

LISTING OF CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 5 of this paper.

01/04/2016 EEKUBAY1 00000003 502075 14659502
01 FC:1202 80.00 DA

LISTING OF CLAIMS

What is claimed is:

1. (Original) A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. (Original) The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Currently Ameneded) The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device~~, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database~~.

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Original) The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Original) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. (Original) The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Original) The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

17. (New) A method for secure transactions using a mobile device, comprising:

storing biometric authentication information and payment information in memory;

reading biometric information using a biometric reader;

determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

encrypting the key and the payment information stored in memory; and

providing the encrypted key and payment information for use in a transaction.

18. (New) The method of claim 17, further comprising reading biometric information provided by a user to complete the transaction.

19. (New) The method of claim 17, wherein the payment information is associated with a primary account number.

20. (New) The method of claim 17, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

21. (New) The method of claim 17, wherein the biometric authentication information is stored separately from the payment information.

22. (New) The method of claim 17, wherein the payment information is stored in a memory accessible only by a secure module.

23. (New) The method of claim 17, wherein the payment information is provided using a short range RF circuitry.

REMARKS

The present communication is in response to the Non-Final Office Action dated June 22, 2015. In the present communication, claims 5-6 have been canceled and Claims 17-23 have been added. Claim 4 has been amended to clarify the subject matter regarded as the invention. No new matter has been added. Reconsideration and allowance are respectfully requested for all pending Claims 1-4 and 7-23.

Double Patenting

Claims 2-17 have been rejected under the judicially created doctrine of obviousness-type non-statutory double patenting as being unpatentable over Claims 1-16 of co-pending Application 14/659,502. Claims 2-17 have also been provisionally rejected on the ground of statutory double patenting as being unpatentable over Claims 1-16 of co-pending Application No. 14/639,034. It is believed that the Terminal Disclaimer filed herewith is sufficient to overcome the double patenting rejection.

Claim Rejections - 35 U.S.C. § 112, Second Paragraph

Claim 4 has been amended in a manner that is believed to overcome the Examiner's rejection of the claims under 35 U.S.C. § 112, second paragraph. Claims 5-6 have been cancelled and the Examiner's rejections of Claims 5-6 under 35 U.S.C. § 112, second paragraph, is therefore believed to have been rendered moot.

The Examiner has rejected Claims 10 and 13 under 35 U.S.C. § 112, second paragraph. The rejections are respectfully traversed. Independent Claim 10 is directed towards a system that includes a point of sale (POS) device. As such, neither Claims 10 nor 13 are rendered indefinite by reciting to matters directed towards the POS device. Accordingly, Applicant respectfully request withdrawal of the rejection under 35 U.S.C. § 112, second paragraph, with respect to Claims 10 and 13.

Claim Rejections - 35 U.S.C. § 101

The Examiner has rejected Claims 1-16 under 35 U.S.C. § 101 as being directed toward a judicial exception. Specifically, the Examiner purports that Claims 1-16 are directed towards the abstract idea of "conducing a payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency," which the Examiner categorizes as a fundamental economic practice. (Office Action, at p. 5). The Examiner further states that "additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself." (Office Action, at p. 5). Applicant respectfully disagrees with the Examiner's analysis and conclusion, particularly in light of *July 2015 Update: Subject Matter Eligibility* (July Update), which the Office has published to supplement the *2014 Interim Guidance on Subject Matter Eligibility* (2014 IEG).

The July Update clarified several key aspects of the two-part *Mayo* test that the Supreme Court adopted in *Alice Corp. v. CLS Bank.* First, with respect to the abstract idea inquiry (i.e. first step of the *Mayo* test), the July Update echoes the 2014 IED and urges comparison to concepts already found to be abstract in case law precedent. (July Update, at p. 3). In fact, the July Update insists that "a claimed concept is not identified as an abstract idea unless it is similar to at least one concept that the courts have identified as an abstract idea." (July Update, at p. 3, emphasis added). Even if the Examiner's description of the claimed concept is assumed to be correct, "conducing a payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency" is not similar to any of the concepts identified as abstract ideas in earlier cases.

The Examiner categorized the claimed concept as a fundamental economic practice. Yet the July Update defines fundamental economic practices to as foundational or basic practices that are analogous to abstract ideas that have been identified in previous court cases. Specifically, judicial precedents indicate that creating a contractual relationship, hedging, and mitigating settlement risks are abstract ideas that fall into the category of fundamental economic practices.

By contrast, Claims 1-16 are set forth a mechanism for securitizing the electronic payment information provided to complete a sales transaction, which bears no similarity to creating a contractual relationship, hedging, or mitigating settlement risks. As such, contrary to the Examiner's assertion, Claims 1-16 are not directed toward an abstract idea.

However, even assuming *arguendo* that securitizing electronic payment information is an abstract idea, Claims 1-16 recite additional elements that amount to significantly more than the abstract idea. With respect to the significantly more inquiry (i.e., second step of the *Mayo* test), the July Update instructs that "examiners should rely on what the courts have recognized, or those in the art would recognize, as elements that are well-understood, routine, and conventional." (July Update, at p. 7, emphasis added). Notably, independent Claims 1 and 10 recite specialized hardware that is not mere generic computer components or a general purpose computer. For example, independent Claims 1 and 10 each recite a biometric module configured to read biometric information and an authentication module configured to authenticate biometric information. Independent Claims 1 and 10 each further recite a secure module configured generate a key and encrypt the key and payment information in response to a successful authentication of the biometric information, and a short range radio frequency (RF) module configured to transmit the encrypted key and payment information.

But the July Update also stresses that a claim reciting a generic computer component performing a generic computer function is not *per se* patent ineligible. (July Update, at p. 7). To further clarify computer functions that are "well understood, routine, and conventional" when claimed in a merely generic manner, the July Update provides the following examples:

- Performing repetitive calculations,
- Receiving, processing, and storing data,
- Electronically scanning or extracting data from a physical document,
- Electronic recordkeeping,
- Automated mental tasks, and
- Receiving or transmitting data over a network, e.g., using the Internet to gather data.

Thus, even if assuming *arguendo* that Claims 1-16 set forth generic computer components, the claimed elements and functions are beyond those recognized by the courts as being well-understood, routine or conventional. Specifically, independent Claims 1 and 10 each recite reading and authenticating biometric information. Independent Claims 1 and 10 each further recite generating a key and encrypting the key and payment information in response to successfully authenticating the biometric information. In addition, the encrypted key and payment information are provided using short range RF circuitry. Accordingly, with reference to the foregoing list of judicially recognized "well understood, routine, and conventional" computer functions, Applicant respectfully submits that the claimed mechanism for securitizing electronic payment information provided to complete a transaction is not what the courts would recognize as well understood, routine, or conventional.

Furthermore, Applicant respectfully submits that the claimed concept is also beyond what those in the art would consider to be well understood, routine, and conventional. Contrary to the Examiner's assertion, the claims do recite an improvement to another technology or technical field besides business method or solutions. Specifically, conventional means of transmitting payment information are unsecured and susceptible to malicious interlopers. By contrast, Claims 1-16 sets forth a mechanism that ensures the security of payment information when such information is provided to complete a sales transaction. For instance, biometric information is required to be successfully authenticated prior to encryption and provision of payment information along with a key. As such, even if assuming that the concept claimed in Claims 1-16 are directed toward an abstract idea, Claims 1-16 recite elements that amounts to significantly more than the abstract idea.

For at least the foregoing reasons, Applicant respectfully requests that the Examiner's rejections of Claims 1-16 under 35 U.S.C. § 101 be withdrawn.

Claim Rejections - 35 U.S.C. § 103(a)

The Examiner has rejected Claims 1-6, 8-13, 15-16 under pre A.I.A. 35 U.S.C. 103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048) in further in view of Chen et al. (U.S. Patent No. 5,590,197). The

remaining claims stand rejected under 35 U.S.C. § 103(a) based on Walker, Holmes, and Chen as further combined with Voltmer et al. (U.S. Pub. No. 2002/0112177). The rejections are respectfully traversed.

According to the Examiner, with the exception of short range radio frequency (RF) circuitry, key encryption, and payment information storage, Walker discloses all of the limitations set forth in independent Claims 1 and 10. Applicant respectfully disagrees. First, to the extent that Walker discloses a biometric interface, biometric information is used to control access to a device such as a smartcard. For example, Walker states that "the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent Claims 1 and 10 each set forth that biometric information must be successfully authenticated in order for a secure module to "generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction." Thus, Walker fails to disclose using biometric information to control the generation, encryption, and transmission of a key and payment information.

Second, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. According to Walker, "the cardholder first inputs his PIN or biometric data to access the device [...]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number [...]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")." (Walker, at 6:18-25, emphasis added). Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt[ing...] the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as recited in each of independent Claims 1 and 10.

In addition, Walker describes generating a single-use credit card number, which "is distinct from the unchanging account number identifying the particular cardholder." (Walker, at 6:66-7:1). The single-use credit card number is formed by concatenating an encrypted nonce, an initialization vector, and the account number. Thus, contrary to the Examiner's rejection, Walker does not teach or suggest "provid[ing...] the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1 and 10.

The Examiner concedes that the combination of Walker and Holmes does not disclose key encryption and payment information storage, and proffers that Chen discloses these features set forth in independent Claims 1 and 10. (Office Action, at p. 7). Interestingly, the Examiner took a contradictory position on Page 7 of the Office Action mailed on May 29, 2015 for co-pending Application No. 14/639,034 where he appears to state that Holmes discloses both features. Nevertheless, Applicant respectfully submits that Walker, Holmes, and Chen, whether considered independently or in combination, do not teach or suggest "memory configured to store biometric authentication information and payment information; a biometric module configured to read biometric information; an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and a secure module configured to: generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1 and 10.

For at least the foregoing reasons, independent Claims 1 and 10 are believed to be allowable. The remaining claims depend, either directly or indirectly, on the aforementioned independent claims and are therefore believed to be allowable for the same reasons described above.

New Claims

New Claims 17-23 have been added. Claim 17 is an independent method claim and claims 18-23 depend therefrom. The subject matter of claims 17-23 is similar that of the previously pending claims. Accordingly, Applicant believes the claims are fully supported by the specification and are in condition for allowance for similar reasons as stated above.

CONCLUSION

Based on the above amendments and remarks, Applicant believes that the claims are in condition for allowance and such is respectfully requested. Applicant believes that no additional fees are necessitated by this response. The Commissioner is hereby authorized to charge any additional fees required by this response to our Deposit Account No. **502075** (Attorney Docket No. 116546-661CT2).

Respectfully submitted,

Dated: December 22, 2015

By: /Noel C. Gillespie/
Noel C. Gillespie, Reg. No. 47596

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900 (Phone)
(619) 235-0398 (Fax)
Customer No. 27189

OPAP AKIMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

12-24-15

1 fm

PTO/SB/21 (08-08)
Approved for use through 09/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	14/659,502
Filing Date	March 16, 2013
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [x] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation
- [ ] Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):
  1.) Excess Claim Fee Sheet;
  2.) Certificate of Mailing Under 37 CFR 1.8;
  3.) Postcard.

Remarks

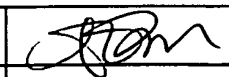
The Commissioner is hereby authorized to charge any additional fees and credit any overpayments required to Deposit Account No: 50-2075.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Procopio, Cory, Hargreaves & Savitch LLP		
Signature	/Michael C. Jones/		
Printed name	Michael C. Jones		
Date	December 22, 2015	Reg. No.	63266

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Ana Molina	Date	December 22, 2015

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

OPAP AKIMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

PTO/SB/17 (03-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if known	
Application Number	14659502
Filing Date	March 16, 2013
First Named Inventor	Francisco Martinez de Velasco Cortina
Examiner Name	OUSSIR, EL MEHDI
Art Unit	3685
Practitioner Docket No.	116546-661CT2

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

TOTAL AMOUNT OF PAYMENT ($)

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 502075 Deposit Account Name: Procopio

For the above-identified deposit account, the Director is hereby authorized to (check all that apply):

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayment of fee(s)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES (U = undiscounted fee; S = small entity fee; M = micro entity fee)

	FILING FEES			SEARCH FEES			EXAMINATION FEES			
Application Type	U ($)	S ($)	M ($)	U ($)	S ($)	M ($)	U ($)	S ($)	M ($)	Fees Paid ($)
Utility	280	140*	70	600	300	150	720	360	180	
Design	180	90	45	120	60	30	460	230	115	
Plant	180	90	45	380	190	95	580	290	145	
Reissue	280	140	70	600	300	150	2,160	1,080	540	
Provisional	260	130	65	0	0	0	0	0	0	

* The $140 small entity status filing fee for a utility application is further reduced to $70 for a small entity status applicant who files the application via EFS-Web.

2. EXCESS CLAIM FEES

Fee Description	Undiscounted Fee ($)	Small Entity Fee ($)	Micro Entity Fee ($)
Each claim over 20 (including Reissues)	80	40	20
Each independent claim over 3 (including Reissues)	420	210	105
Multiple dependent claims	780	390	195

Total Claims _____ -20 or HP = _____ Extra Claims x Fee ($) 80.00 = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

Indep. Claims _____ -3 or HP = _____ Extra Claims x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $400 ($200 for small entity) ($100 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets _____ / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S) Fees Paid ($)

Non-English specification, $130 fee (no small or micro entity discount) _____

Non-electronic filing fee under 37 CFR 1.16(t) for a utility application, $400 fee ($200 small or micro entity) _____

Other (e.g., late filing surcharge): Extension of Time (Separate Sheet Attached) _____

SUBMITTED BY

Signature	/Michael C. Jones/	Registration No. (Attorney/Agent) 63266	Telephone 6506459000
Name (Print/Type)	Michael C. Jones		Date 22DEC2015

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

OPAP AKIMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Docket No: 116546-661CT2

Francisco Martinez de Velasco Cortina

Appln. No.: 14659502

Group Art Unit: 3685

Confirmation No.: 3012

Examiner: OUSSIR, EL MEHDI

Filed: March 16, 2013

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

EXCESS CLAIM FEE PAYMENT LETTER

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

Sir:

An Amendment Under 37 C.F.R. § 1.111 is attached hereto for concurrent filing in the above-identified application. The resulting excess claim fee has been calculated as shown below:

	After Amendment		Highest No. Previously Paid For						
All Claims	23	-	0	=	1	X	$80.00	=	$80.00
Independent	3	-	3	=	0	X	$220.00	=	$.00
					TOTAL			=	**$80.00**

The statutory fee of $80.00 is being remitted. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 50-2075. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/Michael C. Jones/

PROCOPIO CORY HARGREAVES & SAVITCH LLP
Telephone: (619) 238-1900

Michael C. Jones
Registration No. 63,266

SAN DIEGO OFFICE
27189
CUSTOMER NUMBER

Date: December 22, 2015

OPAP AKUMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

PTO/SB/92 (07-09)
Approved for use through 07/31/2012. OMB 0561-0031
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

App No: 14/659, 502
Filed: March 16, 2013
Confirmation No: 3012
Examiner: El Mehdi Oussir
Art Unit: 3685
Docket No: 116546-661CT2

Transmittal (1 pg);
Fee Transmittal (1 pg);
Response to Non-Final Office Action (12 pgs);
Excess Claim Fee Sheet (1 pg);
Petition for Extension of Time (1 pg);
Postcard

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

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

on December 22, 2015
Date



Signature

Ana Molina

Typed or printed name of person signing Certificate

Registration Number, if applicable

6506459000
Telephone Number

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

This collection of information is required by 37 CFR 1.8. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1.8 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

OPAP AKIMA-2
DEC 2 3 2015
PATENT & TRADEMARK OFFICE

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 116546-661CT2

Application Number: 14659502

Filed: March 16, 2013

For: Francisco Martinez de Velasco Cortina

Art Unit: 3685

Examiner: OUSSIR, EL MEHDI

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1400.00
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 502075.

☐ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 63266.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Michael C. Jones/ — Signature

22DEC2015 — Date

Michael C. Jones — Typed or printed name

6506459000 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

01/04/2016 EEKUBAY1 00000002 502075 14659502

01 FC:1253 1400.00 DA

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/659,502	Filing Date 03/16/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/23/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 21	Minus	** 20	= 1	X $80 =	80
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**80**

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

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

LIE
/LINDA A. WASHINGTON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2	3012

27189 7590 05/16/2016

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/16/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 14/659,502	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/23/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-4 and 7-23* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-4 and 7-23* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *03/16/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This communication is **a Final Office action** in response to Applicant's response on 12/23/2015 to Examiner's Non-Final communication on 06/22/2015. Claims 17-23 are newly added. Claims 5-6 have been cancelled.

3. Claims 1-4, 7-23 have been examined in this application. No new information disclosure statements (IDS) has been filed.

Response to Arguments

4. Applicant's arguments, see pages 1-2, filed 12/23/2015, with respect to claim rejections under 35 U.S.C. §112 have been fully considered and are persuasive. The claim rejections have been withdrawn.

5. Applicant's arguments, see pages 2-5, filed 12/23/2015, with respect to claim rejections under 35 U.S.C. §101 have been fully considered but they are not persuasive. The applicant argues:

> **The Examiner categorized the claimed concept as a fundamental economic practice. Yet the July Update defines fundamental economic practices to as foundational or basic practices that are analogous to abstract ideas that have been identified in previous court cases. Specifically, judicial precedents indicate that creating a contractual relationship, hedging, and mitigating settlement risks are abstract ideas that fall into the category of fundamental economic practices. By contrast, Claims 1-4, 6-8, 10-12, 14-15, and 17-18 are set forth a mechanism for securitizing the electronic payment information provided to complete a sales**

transaction, which bears no similarity to creating a contractual relationship, hedging, or mitigating settlement risks. As such, contrary to the Examiner's assertion, Claims 1-4, 6-8, 10-12, 14-15, and 17-18 are not directed toward an abstract idea.

Thus, even if assuming arguendo that Claims 1-4, 6-8, 10-12, 14-15, and 17-18 set forth generic computer components, the claimed elements and functions are beyond those recognized by the courts as being well-understood, routine or conventional. Specifically, independent Claims 1 and 10 each recite reading and authenticating biometric information. Independent Claims 1 and 10 each further recite providing payment information in response to a successful authentication of the biometric information. In addition, the payment information is provided using RF cellular circuitry. Accordingly, with reference to the foregoing list of judicially recognized "well understood, routine, and conventional" computer functions, Applicant respectfully submits that the claimed mechanism for securitizing electronic payment information provided to complete a transaction is not what the courts would recognize as well understood, routine, or conventional.

Furthermore, Applicant respectfully submits that the claimed concept is also beyond what those in the art would consider to be well understood, routine, and conventional. Contrary to the Examiner's assertion, the claims do recite an improvement to another technology or technical field besides business method or solutions. Specifically, conventional means of transmitting payment information are unsecured and susceptible to malicious interlopers. By contrast, Claims 1-4, 6-8, 10-12, 14-15, and 17-18 sets forth a mechanism ensuring the security of payment information when such information is provided to complete a sales transaction. For

instance, biometric information is required to be successfully authenticated prior to the provision of payment information. As such, even if assuming that the concept claimed in Claims 1-4, 6-8, 10-12, 14-15, and 17-18 are directed toward an abstract idea, Claims 1-4, 6-8, 10-12, 14-15, and 17-18 recite elements amounting to significantly more than the abstract idea.

6. The Examiner respectfully disagrees with the Applicant's arguments. Based on the latest guidelines issued in July 2015, the claims do not contain recitations which amount to significantly more. The claims merely recite a secure way of conducting a transaction utilizing a mobile device which generates a key, encrypts it, and provides the key using a form of communication in order to settle the transaction. The key is generated once the user has supplied biometric information to the mobile device and the device authenticates the biometric data of the user based on stored biometric data. The claimed limitations are argued to recite significantly more because the device is able to read and authenticate the data, the device generating the key automatically, and encrypting the key before providing the key using RF circuitry. Such limitations result in no more than validation of data information and transmission of such data in order to settle a transaction, which does not result in significantly more. All of the limitations recited can simply be carried out utilizing a generic computer / device with executable instructions and any form of communication that is known in the industry including NFC, Bluetooth ®, etc. The simple generation of the key can be performed either by the user requesting the key to be generated after authentication or by the mobile device automatically generating the key; either way the result is the same and such a difference does not result in significantly more since it would be obvious to automate something that is done manually (see In re Venner, 120 USPQ 192,–it has been held that broadly providing a mechanical or automatic

means to replace manual activity which has accomplished the same result involves only routine skill in the art).

7. Examples of abstract ideas that relate to the claimed invention based on the concepts relating to the processes of comparing data, collecting and comparing known inforamtion, obtaining and comparing intangible data, and comparing new and stored information and using rules to identify options are all classified under an idea of itself [see Classen, Cybersource, and SmartGene]. Also, concepts relating to the claimed limitations include managing relationships or creating a contractual relationship; see buySAFE. These examples can be found by accessing the following link which will provide further details about the references examples [http://www.uspto.gov/sites/default/files/ct%20dec%20chrt%20sum.pdf].

8. The guidelines clearly recite that the Examiner may rely on "on the knowledge generally available to those in the art, on the case law precedent, on applicant's own disclosure, or on evidence." As a result, the Examiner has clearly noted that the claims do not amount to significantly more than the abstract idea because one of ordinary skill in the art would readily understand the claim limitations to readily implement them using a generic mobile device or computer with executable code.

9. The courts consider the determination of whether a claim is eligible… to be a question of law. Accordingly, courts do not rely on evidence that a claimed concept is a judicial exception, and in most cases resolve the ultimate legal conclusion on eligibility without making any factual findings. Such cases include, *Alice Corp., Myriad, Mayo, Bilski, Diehr, Flook and Benson.*

10. Also, the Interim Guidelines, see page 3 of "subject matter eligibility," recite that "judicial exceptions need not be old or long-prevalent, and that even newly discovered judicial

exceptions are still exceptions, despite their novelty… [the] Supreme Court's cited rationale for considering even "just discovered" judicial exception as exceptions stems from the concern that "without this exception, there would be considerable danger that the grant of patents would 'tie up' the use of such tools and thereby 'inhibit future innovation premised upon them.'"

In conclusion, the claims as a whole merely recite a secure method of authenticating a transaction between two entities utilizing a mobile device, which is a fundamental economic practice. One of ordinary skill in the art would utilize a generic computer or device, input executable code and result at the instant claims; thus rendering the claims not patent eligible. Moreover, the claims do not appear to improve the functioning of the system, device / computer, or effect an improvement in another technology or field; i.e. besides business method or solutions. Furthermore, the steps of capturing user data, generating the key, and sending the encrypted key to settle a transaction do not add a meaningful limitation to the claimed invention as they would be routinely used by those of ordinary skill in the art in order to apply the correlation.

11. Applicant's arguments, see pages 2-5, filed 12/23/2015, with respect to claim rejections under 35 U.S.C. §103 have been fully considered but they are not persuasive.

12. The Examiner disagrees with Applicant(s) arguments. Walker in view of Holmes and Chen along with Voltmer teach all of the claimed limitations. Walker does teach biometric information in relation to a transaction since the card is used to transmit payment information to the merchant in order to settle a transaction [see Figures 1-3 and related text]. It is clearly recited by Walker that the card is used for a transaction. The card requires the user to "input PIN/Biometric data to access the device" which is used to verify the user, and if the user is

granted access, then the card generates the single use credit card number [See figures 1-3 and related text]. Walker, in view of Holmes do not explicitly teach encrypt the key and the payment information stored in memory prior to the transaction module providing the payment information [...] for use in the transaction [Walker, Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Chen does (encrypting the ticket using a public key) [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]. As a result it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the generated key including the payment information in motivation of increasing security measures. Holmes teaches RF circuitry. See Holmes Col. 2, Ln. 38-53, Figures 1-3. Per newly entered claims, it is clearly recited that the combination of Walker and Chan do teach wherein the transaction module is further configured to provide the [...] key for use in the transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the biometric authentication information by the authentication module [Abstract, Col. 6, Ln. 14-38, 61-67, Col. 7, Ln. 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9] while Chen teaches an encrypted key [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]. It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the generated key in motivation of increasing security measures. Lastly, Voltmer explicitly teaches storing separately a plurality of information; see [Paragraphs 009-0091 and Figures 12A and 12B]. It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes and Chen to include the teachings of Voltmer to store the data in

partitions or separately in motivation of increasing security measures or facilitating the upload of information from the memory.

Claim Rejections - 35 USC § 101

13. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 1-4, 7-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

JUDICIAL EXCEPTIONS TO SECTION 101

15. The Supreme Court held that the patent claims in Alice Corporation Pry. Ltd. v. CLS Bank International, el al. ("Alice Corp. ") are not patent-eligible under 35 U.S.C. § 101. 10. The Supreme Court made clear in Alice Corp. that it applies the framework set forth in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. _ (2012) (Mayo), to analyze all claims directed to laws of nature, natural phenomena, and abstract ideas for subject matter eligibility under 35 U.S.C. § 101. This framework is currently being used by the USPTO to examine claims involving laws of nature, but had not been used for claims involving abstract ideas. Therefore, the following instructions differ from prior USPTO guidance in two ways:

16. Alice Corp. establishes that the same analysis should be used for all types of judicial exceptions, whereas prior USPTO guidance applied a different analysis to claims with abstract ideas (Bilski guidance in MPEP 2106(11) (B)) than to claims with laws of nature (Mayo guidance in MPEP 2106.01).

17. Alice Corp. also establishes that the same analysis should be used for all categories of claims (e.g., product and process claims), whereas prior guidance applied a different analysis to product claims involving abstract ideas (relying on tangibility in MPEP 2106(II) (A)) than to process claims (Bilski guidance).

ALICE V. CLS BANK: TWO-PART ANALYSIS

18. Following Alice Corp, all claims (product and process) having an abstract idea must be analyzed using the following two-part analysis set forth in Mayo. For additional guidance, see "2014 Interim Guidance on Patent Subject Matter Eligibility" December 16, 2014.

19. Limitations referenced in Alice Corp. that may be enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

a. Improvements to another technology or technical fields;

b. Improvements to the functioning of the computer itself;

c. Applying the judicial exception with, or by use of, a particular machine; effecting a transformation or reduction of a particular article to a different state or thing; adding a specific limitation other than what is well-understood, routine and conventional in the field, or adding unconventional steps that confine the claim to a particular useful application.

20. Limitations referenced in Alice Corp. that are not enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

d. Adding the words "apply it" (or an equivalent) with an abstract idea, or mere instructions to implement an abstract idea on a computer;

e. Requiting no more than a genetic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. See also, MPEP 2106(1).

21. Claims 1-4, 7-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

22. Claims 1-4, 7-23 are directed to essentially a payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice or an idea of itself. Examples of abstract ideas that relate to the claimed invention based on the concepts relating to the processes of comparing data, collecting and comparing known information, obtaining and comparing intangible data, and comparing new and stored information and using rules to identify options are all classified under an idea of itself [see Classen, Cybersource, and SmartGene]. These concepts are tied to the instant claims because it is through the comparing of the data that is received that a user is able to carry out the transaction. Also, concepts relating to the claimed limitations include managing relationships or creating a contractual relationship; see buySAFE. These examples can be found by accessing the following link which will provide further details about the references examples: [http://www.uspto.gov/sites/default/files/ct%20dec%20chrt%20sum.pdf].

23. Likewise, the additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself. The claims do not include limitations that meet the criteria required to determine the claims as a whole amounting to significantly more than the judicial exception itself (**see paragraph 19, a-c**). This is evident by the description; see Paragraphs 0002, reciting "RF Communications Device (e.g. Cellular Telephone)" and Paragraph 0080 reciting "computers (e.g., PC, PDA, cellular phone) connected to a network." Also, Paragraph 00116 recites "The RF … can comprise computer system components (e.g, remote readers/, verification scanners client server or thin client systems and networks, and application software and databases)."

24. The method steps amount to mere instructions to implement the idea on a generic computer or device that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry, which do not add meaningful limitations to the method as they would be routinely used by those of ordinary skill in the art in order to apply the correlation and yield predictable results. The functions performed by the "mobile device" and "module" appear to be conventional and routine carried out by a general purpose computer or device such as a cellular phone, PDA, smart card, etc. with instructions allow a user to carry out a transaction. The claimed limitations as a whole do not add significantly more to the abstract idea of using increased security measures to prevent unauthorized use of the content or distribution of the content. Moreover, the claims do not appear to improve the functioning of the "mobile device" or any of the "modules" or effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. One of

ordinary skill in the art is able to readily understand the invention and carry out the recited limitations in order to apply the correlation using a generic computer or portable device with instructions and communication protocols to carry out the recited limitations. Accordingly, the Examiner concludes that there are no meaningful limitations in the claims that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

Claim Rejections - 35 USC § 103

25. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 1-4, 8-13, 15-20, and 22-23 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. (herein after referred to as simply Walker), in view of U.S. Patent 6,848,048 to Holmes (herein after referred to as simply Holmes), in further view of U.S. Patent 5,590,197 to Chen et al. (herein after referred to as simply Chen).

28. Per claims 1 and 17, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio

frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

c. Memory (memory) configured to store biometric authentication information (biometric information) and payment information (account number) [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

d. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory (processor); and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6].

f. a secure module configured to (processor) [Walker, Abstract]:

g. generate a key (generates a single use credit card number) when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory [Col. 5, Ln. 49- , Col. 6, Ln. 1-38 and Figures 1-9];

h. Walker, in view of Holmes do not explicitly teach encrypt the key and the payment information stored in memory [Walker, Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Chen does (encrypting the ticket using a public key) [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the

generated key including the payment information in motivation of increasing security measures.

i. Walker does not explicitly teach provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches [...] via the short range RF circuitry [...] (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

Chen teaches provide, [...] the encrypted key and payment information for use in a transaction [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to provide a communication link that is a short range RF circuitry in motivation of increasing security measures.

Also, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Chen to provide over the communication link the encrypted key and payment information for use in a transaction in motivation of increasing security measures.

Examiner notes that the following limitation is an intended use limitation, "for use in a transaction."

29. Per claims 2, 11, and 18 Walker teaches wherein the biometric module is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-9].

30. Per claims 3, 12, 19, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

31. Per claim 4, Walker teaches [...] a point of sale (POS) device [...] (merchant terminal, a terminal is a device) [...] [Col. 6, Ln. 39-53, Col. 8, Ln. 33-39].

Walker does not explicitly teach wherein the secure module is configured to provide the encrypted key and payment information [...]; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to transmit the encrypted key to a point of sale terminal, have the terminal receive the encrypted data and transmit this data to a central database (account servicer) in motivation of increasing security measures.

The above limitation is an intended use limitation.

32. Per claim 20, walker teaches [...] a point of sale (POS) device (merchant terminal, a terminal is a device) [Col. 6, Ln. 39-53, Col. 8, Ln. 33-39].

Walker does not explicitly teach providing the encrypted key and payment information [...]; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to transmit the encrypted key to a point of sale terminal in motivation of processing or completing the transaction at an optimized security level.

33. Per claim 13, Walker does not explicitly teaches wherein the POS device includes an RF reader; however, Holmes does [Col. 1, Ln. 60-63, Col. 2, Ln. 34-61, Col. 4-5, Ln. 62-, 1-21 and Figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to insure that the POS includes an RF reader, in motivation of facilitating communication measures while enhancing security measures.

34. Per claim 6, Walker teaches wherein the central database (credit card issuer) is configured to validate the key and the payment information [Abstract, Col. 8, Ln. 33-67 and Figures 1-9].

35. Per claims 8, 15, and 22 Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the secure module (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

36. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes in order to utilize radio frequency identification as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

37. Per claim 23, Walker does not explicitly teach wherein the payment information is provided using a short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

38. Per claim 10, Walker teaches

a. A system, comprising [Abstract]:

b. a mobile device, comprising [Abstract]:

c. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

d. memory configured to store biometric authentication information and payment information, [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

e. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

f. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6]

g. a secure module configured to (processor) [Walker, Abstract]:

h. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; [Col. 6, Ln. 14-38 and Figures 1-3];

i. Walker, in view of Holmes do not explicitly teach encrypt the key and the payment information stored in memory [Walker, Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Chen does (encrypting the ticket using a public key) [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to encrypt the generated key including the payment information in motivation of increasing security measures.

j. Walker does not explicitly teach provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches [...] via the short range RF circuitry [...] (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

Chen teaches provide [...] the encrypted key and payment information for use in a transaction [Abstract, Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to provide a communication link that is a short range RF circuitry in motivation of increasing security measures.

Also, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Chen to provide over the communication link the encrypted key and payment information for use in a transaction in motivation of increasing security measures.

Examiner notes that the following limitation is an intended use limitation, "for use in a transaction."

k. Walker teach a point of sale (POS) device (terminal / merchant terminal) configured to [Col. 6, Ln. 39-53, Col. 8, Ln. 33-39]:

l. Walker does not explicitly teach receive, from the secure module, the encrypted key and payment information; however Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teaching of Chen to include the receiving from the secure module, the encrypted key and payment information in motivation of processing the transaction while increasing security measures.

m. Walker does not explicitly teach transmit, to a central database (account servicer), the encrypted key and payment information; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1]; and

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to transmit the encrypted key to a central database (account servicer) in motivation of increasing security measures.

n. Walker does not explicitly teach a central database configured to validate the key and the payment information; however, Chen does [Abstract, Col. 4, Ln. 14-22, Col. 5, 41-60, Col. 6, Ln. 1-5, 48-57 and Figure 1].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes to include the teachings of Chen to have the central database (account servicer) validate the key and payment information in motivation of increasing security measures.

39. Claims 7, 14, and 21 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes and Chen as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

40. Per claims 7, 14, and 21 Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes and Chen to include the teachings of Voltmer to store the data in partitions or separately in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

41. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and

approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

42. Claims 1-16 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14639034 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

43. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/639034 recite:

a. A mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is successfully authenticated;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

Claim 10:

a. A system, comprising:

b. a mobile device, comprising:

c. short range radio frequency (RF) circuitry;

d. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

e. a biometric module configured to read biometric information;

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

g. a secure module configured to:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

j. a point of sale (POS) device configured to:

k. receive, from the secure module, the encrypted key and payment information; and

l. transmit, to a central database, the encrypted key and payment information; and

m. a central database configured to validate the key and the payment information.

44. Claims 1 and 10 of co-pending application 14/639034 differ since they further recite additional claim limitations including associating the biometric authentication information with the payment information, authentication based biometric module associated with the payment information and stored biometric data. However, it would have been obvious to a person of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/639034 by removing the limitations directed to the memory and authentication resulting generally in the claims of the instant application since the claims of the instant application and the claim recited in co-pending application 14/639034 actually perform a similar function. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

45. Also, claims 1 and 10 of co-pending application 14/639034 differ since they fails to recite generating a key by determining that the biometric authentication information stored in memory corresponds to the biometric information read. Walker discloses generating a key once comparing the scanned biometric data to the stored biometric data matches (generating a single use credit card number once user scans biometrics, card compares to data in memory and generates single use credit card number) [Col. 5, Ln. 49-, Col. 6, Ln. 1-38 and Figures 1-9]. It would have been obvious to one of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/639034 and include the function of comparing the stored biometric data

to the scanned data to generate a key as taught by Walker in motivation of preventing unauthorized use of the device by those that are not permitted (increase security measures).

46. Claims 1-16 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 2-17 of copending Application No. 14/321781 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

47. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 2, 11, and 17 of co-pending application 14/321781 recite:

a. A mobile device, comprising:

b. radio frequency (RF) cellular circuitry;

c. memory configured to store biometric authentication information and payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is successfully authenticated;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the RF cellular circuitry, the encrypted key and payment information for use in a transaction

Claim 11:

a. A system, comprising:

b. a mobile device, comprising:

c. radio frequency (RF) cellular circuitry;

d. memory configured to store biometric authentication information and payment information;

e. a biometric module configured to read biometric information;

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

g. a secure module configured to:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and

i. provide, via the RF cellular circuitry, the encrypted key and payment information for use in a transaction; and

j. a point of sale (POS) device configured to:

k. receive, from the secure module, the encrypted key and payment information; and

l. transmit, to a central database, the encrypted key and payment information; and

m. a central database configured to validate the key and the payment information

48. Claims 2, 11, and 18 of co-pending application 14/321781 differ since they further recite additional claim limitations including associating the biometric authentication information with

the payment information, authentication based biometric module associated with the payment information and stored biometric data. However, it would have been obvious to a person of ordinary skill in the art to modify claims 2 and 11 of co-pending application 14/321781 by removing the limitations directed to the memory and authentication resulting generally in the claims of the instant application since the claims of the instant application and the claim recited in co-pending application 14/321781 actually perform a similar function. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

49. Also, claims 1 and 11 of co-pending application 14/321781 differ since they fails to recite generating a key by determining that the biometric authentication information stored in memory corresponds to the biometric information read. Walker discloses generating a key once comparing the scanned biometric data to the stored biometric data matches (generating a single use credit card number once user scans biometrics, card compares to data in memory and generates single use credit card number) [Col. 5, Ln. 49-, Col. 6, Ln. 1-38 and Figures 1-9]. It would have been obvious to one of ordinary skill in the art to modify claims 1 and 10 of co-pending application 14/321781 and include the function of comparing the stored biometric data to the scanned data to generate a key as taught by Walker in motivation of preventing unauthorized use of the device by those that are not permitted (increase security measures).

Conclusion

50. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

51. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

52. Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
04/30/2016

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("20060089912").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 11:07
S2	1	("7155414").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 11:08
S3	1	("5287408").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 11:55
S4	1	("5553143").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 11:58
S5	1	("5758068").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 11:58
S6	1	("20010039614").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 12:04
S7	1	("20140380499").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 12:05
S8	1	("20080046308").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 14:16
S9	1	("20030200184").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 14:29
S10	1	("5671412").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 14:33
S11	1	("7571143").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 14:55
S12	1	("20020154157").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 14:58
S13	1	("20090133131").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 15:02
S14	1	("20100131560").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 15:04
S15	1	("20060089912").PN.	US-PGPUB; USPAT	OR	OFF	2016/04/25 15:10
S16	1	("20080034231").PN.	US-PGPUB;	OR	OFF	2016/04/25 15:11

			USPAT			
S17	125	(router) near3 (aggregat$4) near3 (usage condition function$4 rights rules)	US-PGPUB; USPAT	OR	ON	2016/04/25 17:53
S18	1130	((computer near2 product) or content) near3 (aggregat$4) near3 (usage condition function$4 rights rules)	US-PGPUB; USPAT	OR	ON	2016/04/25 17:55
S19	515	((computer near2 product) or content) near2 (aggregat$4) near3 (usage condition function$4 rights rules)	US-PGPUB; USPAT	OR	ON	2016/04/25 17:56
S20	336	S19 and @pd<"20130101"	US-PGPUB; USPAT	OR	ON	2016/04/25 17:56
S21	342	S19 and @pd<"20130301"	US-PGPUB; USPAT	OR	ON	2016/04/25 17:56
S22	94	S21 AND ((G06Q30/02 OR G06Q10/10 OR G06Q30/04 OR G06Q30/0601 OR G06Q40/04 OR G06Q40/12 OR G06Q10/06 OR G06Q10/00 OR G06Q10/0637 OR G06Q30/06 OR G06Q30/0603 OR G06Q50/184 OR G06Q30/0275 OR G06Q20/102 OR G06Q30/0277 OR G06Q40/00 OR G06Q20/10 OR G06Q20/123 OR G06Q20/1235 OR G06Q20/14 OR G06Q30/0283 OR G06Q30/0641 OR G06Q50/18 OR G06Q50/22 OR G06Q10/04 OR G06Q10/087 OR G06Q20/367 OR G06Q20/382 OR G06Q20/3821 OR G06Q20/3829 OR G06Q20/383 OR G06Q30/0203 OR G06Q30/0273 OR G06Q50/188 OR G06Q50/24 OR G06Q10/0631 OR G06Q10/06311 OR G06Q10/0635 OR G06Q10/107 OR G06Q20/00 OR G06Q20/02 OR G06Q20/12 OR G06Q20/20 OR G06Q20/40 OR G06Q30/018 OR G06Q30/0204 OR G06Q30/0237 OR G06Q30/0241 OR G06Q30/0244 OR G06Q30/0245 OR G06Q30/0251 OR G06Q30/0253 OR G06Q30/0254 OR G06Q30/0257 OR G06Q30/0259 OR G06Q30/0282 OR G06Q30/0609 OR G06Q30/0621 OR G06Q30/0631 OR G06Q30/0633 OR G06Q30/0635 OR G06Q30/08 OR G06Q40/06 OR G06Q50/00 OR G06Q50/01).CPC.)	US-PGPUB; USPAT	OR	ON	2016/04/25 17:57
S23	162	S21 AND ((H04L67/02 OR H04L67/28 OR H04L69/329 OR H04L67/104 OR H04L29/06 OR H04L29/08306 OR H04L29/08324 OR H04L29/08333 OR H04L2463/101 OR H04L67/04 OR H04L12/2805 OR H04L67/12 OR H04L67/2819 OR H04L67/2823 OR H04L63/0823 OR H04L67/125 OR H04L67/327 OR H04L63/12 OR H04L67/2842 OR H04L67/34 OR H04L12/2827 OR H04L63/102 OR H04L67/2838 OR H04L67/306 OR H04L12/2803 OR H04L12/2812 OR H04L2012/2849 OR H04L65/4084 OR H04L67/2871 OR H04L69/18 OR H04L12/185 OR H04L67/18 OR H04L12/2832 OR H04L12/66 OR H04L41/509 OR H04L63/10 OR H04L63/18	US-PGPUB; USPAT	OR	ON	2016/04/25 17:58

		OR H04L65/4076 OR H04L67/22 OR H04L67/2804 OR H04L67/30 OR H04L9/32 OR H04L2209/608 OR H04L61/2592 OR H04L63/0209 OR H04L63/062 OR H04L63/08 OR H04L63/0869 OR H04L63/101 OR H04L67/1095 OR H04L12/2602 OR H04L12/2801 OR H04L12/2861 OR H04L2209/60 OR H04L2463/103 OR H04L41/5067 OR H04L43/0817 OR H04L63/0281 OR H04L63/0428 OR H04L63/0861 OR H04L65/605 OR H04L65/80 OR H04L67/10 OR H04L67/1097 OR H04L67/20 OR H04L67/32 OR H04L67/325 OR H04L9/083 OR H04L9/0897 OR H04L9/321 OR H04L9/3236 OR H04L12/14 OR H04L12/1428 OR H04L12/24 OR H04L12/4633 OR H04L1/0007 OR H04L1/0018 OR H04L2012/2841 OR H04L2012/2845 OR H04L2012/285 OR H04L2209/38 OR H04L2463/062 OR H04L29/12367 OR H04L29/1249 OR H04L29/12537 OR H04L41/00 OR H04L41/22 OR H04L41/5025 OR H04L41/5054 OR H04L41/5083 OR H04L43/00 OR H04L43/022 OR H04L43/026 OR H04L43/0876 OR H04L43/0882 OR H04L61/2514 OR H04L61/256 OR H04L61/2578 OR H04L63/0414 OR H04L63/045 OR H04L63/0457 OR H04L63/0464 OR H04L63/06 OR H04L63/0807 OR H04L63/0815 OR H04L63/104 OR H04L63/20 OR H04L67/00 OR H04L67/1008 OR H04L67/1014 OR H04L67/1021 OR H04L67/14 OR H04L67/141 OR H04L67/16 OR H04L67/26 OR H04L67/2833 OR H04L67/2847 OR H04L67/2861 OR H04L69/14 OR H04L12/1859 OR H04L12/2807 OR H04L12/2809 OR H04L12/2814 OR H04L12/581 OR H04L12/6418 OR H04L2209/80 OR H04L29/12594 OR H04L41/0246 OR H04L41/0253 OR H04L41/0893 OR H04L41/142 OR H04L41/50 OR H04L41/5038 OR H04L43/045 OR H04L43/06 OR H04L43/062 OR H04L43/0811 OR H04L43/12 OR H04L45/24 OR H04L45/306 OR H04L47/38 OR H04L51/04 OR H04L61/30 OR H04L63/083 OR H04L63/0884 OR H04L63/105 OR H04L63/1433 OR H04L63/30 OR H04L65/104 OR H04L65/4092 OR H04L65/601 OR H04L65/607 OR H04L67/06 OR H04L67/1002 OR H04L67/101 OR H04L67/1031 OR H04L67/1038 OR H04L67/24 OR H04L67/2852 OR H04L67/288 OR H04L67/36 OR H04L67/42 OR H04L9/3231 OR H04N21/43615 OR H04N21/812 OR H04N7/17318 OR H04N21/2541 OR H04N21/2665 OR H04N21/4622 OR H04N7/163 OR H04N21/25891 OR H04N21/84 OR H04N7/1675 OR H04N21/4131 OR H04N21/4627 OR H04N21/47202 OR H04N21/4722 OR H04N21/4782 OR H04N21/6125 OR H04N21/64322 OR					

		H04N21/6581 OR H04N21/8586 OR H04N21/2221 OR H04N21/2668 OR H04N21/6118 OR H04N21/835 OR H04N7/173 OR H04N21/235 OR H04N21/23608 OR H04N21/2365 OR H04N21/23655 OR H04N21/2407 OR H04N21/26208).CPC.)				
S24	44	S21 AND ((H04N21/266 OR H04N21/42204 OR H04N21/4316 OR H04N21/434 OR H04N21/4347 OR H04N21/435 OR H04N21/4532 OR H04N21/47 OR H04N21/4753 OR H04N21/482 OR H04N21/6587 OR H04N21/8126 OR H04N21/8352 OR H04N21/8543 OR H04N5/4401 OR H04N5/44543 OR H04N5/45 OR H04N5/50 OR H04N5/783 OR H04N7/17309 OR H04N7/17336 OR H04N21/23106 OR H04N21/23424 OR H04N21/2547 OR H04N21/258 OR H04N21/26283 OR H04N21/26291 OR H04N21/26603 OR H04N21/4147 OR H04N21/4181 OR H04N21/4331 OR H04N21/458 OR H04N21/462 OR H04N21/4623 OR H04N21/47217 OR H04N21/4788 OR H04N7/22 OR H04N21/2187 OR H04N21/222 OR H04N21/2343 OR H04N21/26606 OR H04N21/2747 OR H04N21/4113 OR H04N21/42203 OR H04N21/42684 OR H04N21/4333 OR H04N21/4394 OR H04N21/44213 OR H04N21/44222 OR H04N21/44236 OR H04N21/45455 OR H04N21/6168 OR H04N21/6543 OR H04N21/8358 OR H04N21/8456 OR H04N5/76 OR H04N7/165 OR H04N7/18 OR H04N7/20 OR H04N1/00244 OR H04N1/00307 OR H04N1/2179 OR H04N1/2183 OR H04N1/2191 OR H04N21/2181 OR H04N21/2223 OR H04N21/2225 OR H04N21/23103 OR H04N21/234309 OR H04N21/2347 OR H04N21/2353 OR H04N21/2381 OR H04N21/2402 OR H04N21/254 OR H04N21/2543 OR H04N21/25825 OR H04N21/25866 OR H04N21/26233 OR H04N21/4126 OR H04N21/41422 OR H04N21/42669 OR H04N21/4312 OR H04N21/4314 OR H04N21/4325 OR H04N21/4332 OR H04N21/4334 OR H04N21/4367 OR H04N21/44016 OR H04N21/466 OR H04N21/4668 OR H04N21/472 OR H04N21/4755 OR H04N21/4781 OR H04N21/4825 OR H04N21/4826 OR H04N21/4828 OR H04N21/485 OR H04N21/6143 OR H04N21/6175 OR H04N21/6373 OR H04N21/6405 OR H04N21/6582 OR H04N21/8355 OR H04N21/8455 OR H04N21/8545 OR H04N21/8583 OR H04N2201/0082 OR H04N2201/0084 OR H04N2201/0087 OR H04N2201/3226 OR H04N2201/3278 OR H04N5/775 OR H04N5/781 OR H04N5/913 OR H04N9/8205 OR H04N9/8227 OR H04N9/8233).CPC.)	US-PGPUB; USPAT	OR	ON	2016/04/25 17:58

S25	37	S22 and S23	US-PGPUB; USPAT	OR	ON	2016/04/25 17:58
S26	6	S24 and S25	US-PGPUB; USPAT	OR	ON	2016/04/25 17:58
S27	133	(consolidat$3 aggregat$4) with usage same license	US-PGPUB; USPAT	OR	ON	2016/04/26 11:13
S28	86	S27 and @pd<"20130301"	US-PGPUB; USPAT	OR	ON	2016/04/26 11:13
S29	14	S28 and (multiple near3 license)	US-PGPUB; USPAT	OR	ON	2016/04/26 11:14
S30	77289	((obtain$3 receiv$3 collect$3 request$3) near3 (payment pay money monitory)) same (content product media video music file data)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:35
S31	2387	(defer$4) near4 (payment pay money monitory collect$3)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:37
S32	2	((defer$4) near4 (payment pay money monitory collect$3)) with (establish$3 insur$3) same ((communicat$4 network) with (bank financial entity clearinghouse))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:43
S33	1	S30 and S32	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:43
S34	2387	((defer$4) near4 (payment pay money monitory collect$3))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:52
S35	20125	(establish$3 insur$3) with ((connect$3 communicat$4 network) with (bank financial entity clearinghouse))	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:53
S36	729	S30 and S34	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:54
S37	1421	8and S36	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:54
S38	57	S35 and S36	US-PGPUB; USPAT; EPO;	OR	ON	2016/04/26 13:54

			JPO			
S39	35	S38 and @pd<"20121206"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:54
S40	48	S38 and @rlad<"20121206"	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:54
S41	27	S39 and S40	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:54
S42	27	S41 AND ((G06Q20/10 OR G06Q30/06 OR G06Q20/28 OR G06Q50/01 OR G06Q30/0207 OR G06Q20/342 OR G06Q20/105 OR G06Q30/0215 OR G06Q10/101 OR G06Q20/04 OR G06Q20/12 OR G06Q20/227 OR G06Q20/354 OR G06Q30/0224 OR G06Q30/0226 OR G06Q30/0234 OR G06Q30/0235 OR G06Q40/02 OR G06Q20/02 OR G06Q20/102 OR G06Q20/40 OR G06Q30/02 OR G06Q20/06 OR G06Q20/351 OR G06Q30/0601 OR G06Q40/00 OR G06Q20/027 OR G06Q20/0425 OR G06Q20/29 OR G06Q20/32 OR G06Q20/34 OR G06Q20/3674 OR G06Q20/382 OR G06Q20/3825 OR G06Q20/387 OR G06Q30/04 OR G06Q10/087 OR G06Q20/14 OR G06Q20/20 OR G06Q20/322 OR G06Q20/3223 OR G06Q20/3227 OR G06Q20/3229 OR G06Q20/3255 OR G06Q20/3829 OR G06Q20/405 OR G06Q30/0222 OR G06Q30/0255 OR G06Q30/0603 OR G06Q30/0625 OR G06Q30/0643 OR G06Q40/025 OR G06Q40/08 OR G06Q50/22 OR G06Q50/24 OR G06F21/10 OR H04M2215/2026 OR H04M2215/32 OR H04W4/24).CPC.)	US-PGPUB; USPAT; EPO; JPO	OR	ON	2016/04/26 13:55
S43	1	"20060010075"	US-PGPUB; USPAT	OR	ON	2016/04/26 16:42
S44	2	"20110314556"	US-PGPUB; USPAT	OR	ON	2016/04/26 16:43
S45	2	"20090138380"	US-PGPUB; USPAT	OR	ON	2016/04/26 16:44
S46	1	"20130060661"	US-PGPUB; USPAT	OR	ON	2016/04/26 16:47
S47	118	(p2p shar$3) near3 (content) near4 (wifi wirelessly)	US-PGPUB; USPAT	OR	ON	2016/04/26 17:01
S48	63	S47 and @pd<"20121206"	US-PGPUB; USPAT	OR	ON	2016/04/26 17:02

S49	62	S47 and @rlad<"20121206"	US-PGPUB; USPAT	OR	ON	2016/04/26 17:02
S50	46	S48 and S49	US-PGPUB; USPAT	OR	ON	2016/04/26 17:02
S51	3	S50 and (mesh near3 network)	US-PGPUB; USPAT	OR	ON	2016/04/26 17:04
S52	30	S50 and (pay$4 bank clearinghouse financial)	US-PGPUB; USPAT	OR	ON	2016/04/26 17:06
S53	30	S50 and (pay$4 bank clearinghouse financial sell$3)	US-PGPUB; USPAT	OR	ON	2016/04/26 17:06
S54	23	S50 and (pay payment bank clearinghouse financial sell$3)	US-PGPUB; USPAT	OR	ON	2016/04/26 17:07
S55	1084	(peer near2 peer) near3 (shar$3) near3 (content)	US-PGPUB; USPAT	OR	ON	2016/04/27 11:53
S56	114	(peer near1 peer) near3 (shar$3) near3 (content)	US-PGPUB; USPAT	OR	ON	2016/04/27 11:53
S57	71	S56 and @pd<"20121206"	US-PGPUB; USPAT	OR	ON	2016/04/27 11:54
S58	63	S57 AND ((H04L67/104 OR H04L69/329 OR H04L67/1068 OR H04L67/108 OR H04L67/1095 OR H04L67/1046 OR H04L67/1093 OR H04L67/34 OR H04L29/06 OR H04L63/0823 OR H04L67/1044 OR H04L67/1048 OR H04L67/1082 OR H04L2463/101 OR H04L63/0428 OR H04L63/08 OR H04L63/126 OR H04L67/02 OR H04L67/107 OR H04L67/28 OR H04L67/2842 OR H04L12/2856 OR H04L29/12009 OR H04L63/105 OR H04L63/123 OR H04L67/04 OR H04L67/1042 OR H04L67/1057 OR H04L12/14 OR H04L12/58 OR H04L12/581 OR H04L41/509 OR H04L51/04 OR H04L63/061 OR H04L63/166 OR H04L65/4084 OR H04L67/1061 OR H04L67/1063 OR H04L67/1065 OR H04L67/18 OR H04L67/24 OR H04L67/322 OR H04L12/1425 OR H04L12/2859 OR H04L12/2861 OR H04L12/588 OR H04L29/12047 OR H04L29/12113 OR H04L29/12207 OR H04L29/12452 OR H04L29/12594 OR H04L29/12783 OR H04L29/12924 OR H04L41/5077 OR H04L45/34 OR H04L51/32 OR H04L61/1541 OR H04L61/20 OR H04L61/2546 OR H04L61/303 OR H04L61/3065 OR H04L61/35 OR H04L61/6063 OR H04L63/0209 OR H04L63/029 OR H04L63/0442 OR H04L63/10 OR H04L63/104 OR H04L63/145 OR H04L63/164 OR H04L67/1002 OR H04L67/1008 OR H04L67/1012 OR H04L67/1059 OR H04L67/1076 OR	US-PGPUB; USPAT	OR	ON	2016/04/27 11:54

		H04L67/1091 OR H04L67/16 OR H04L67/20 OR H04L67/22 OR H04L67/2814 OR H04L67/2823 OR H04L67/2852 OR H04L67/42 OR H04L69/28 OR H04L12/1482 OR H04L12/2876 OR H04L12/5885 OR H04L2209/603 OR H04L2463/102 OR H04L29/06027 OR H04L41/0213 OR H04L41/0896 OR H04L41/5003 OR H04L41/5022 OR H04L47/10 OR H04L47/2408 OR H04L47/31 OR H04L51/16 OR H04L63/12 OR H04L65/104 OR H04L65/80 OR H04L67/06 OR H04L67/10 OR H04L67/1072 OR H04L67/1085 OR H04L67/1089 OR H04L67/142 OR H04L67/306 OR H04L9/0822 OR H04L9/0825 OR H04L9/3268 OR H04L9/3273 OR G06Q30/02 OR G06Q10/10 OR G06Q50/01 OR G06Q30/0241 OR G06Q30/0251 OR G06Q30/0273 OR G06Q20/10 OR G06Q20/123 OR G06Q20/14 OR G06Q30/0201 OR G06Q30/0213 OR G06Q30/0214 OR G06Q30/0243 OR G06Q30/0249 OR G06Q30/0255 OR G06Q30/0256 OR G06Q30/0261 OR G06Q30/0269 OR G06Q30/0276 OR G06Q30/0283 OR G06Q30/04 OR G06Q40/12 OR H04N21/47202 OR H04N21/4788 OR H04N21/632 OR H04N7/17318 OR H04N21/2187 OR H04N21/4331 OR H04N21/4828 OR H04N21/6125 OR H04N21/6581 OR H04N1/4426 OR H04N1/4486 OR H04N21/214 OR H04N21/2221 OR H04N21/23103 OR H04N21/23109 OR H04N21/2408 OR H04N21/2541 OR H04N21/25883 OR H04N21/25891 OR H04N21/26258 OR H04N21/2668 OR H04N21/2743 OR H04N21/2747 OR H04N21/278 OR H04N21/41407 OR H04N21/42203 OR H04N21/4223 OR H04N21/43637 OR H04N21/437 OR H04N21/44029 OR H04N21/44204 OR H04N21/4425 OR H04N21/4621 OR H04N21/4622 OR H04N21/4627 OR H04N21/6375 OR H04N21/64792 OR H04N21/6582 OR H04N21/8106 OR H04N21/8153 OR H04N21/816 OR H04N21/8355 OR H04N21/84).CPC.)				
S59	118	(p2p shar$3) near3 (content) near4 (wifi wirelessly)	US-PGPUB; USPAT	OR	ON	2016/04/27 16:52
S60	63	S59 and @pd<"20121206"	US-PGPUB; USPAT	OR	ON	2016/04/27 16:52
S61	62	S59 and @rlad<"20121206"	US-PGPUB; USPAT	OR	ON	2016/04/27 16:52
S62	46	S60 and S61	US-PGPUB; USPAT	OR	ON	2016/04/27 16:52
S63	22	S62 and ((portion or sample) near2 (content))	US-PGPUB;	OR	ON	2016/04/27 16:52

			USPAT			
S64	2	"20100299762"	US-PGPUB; USPAT	OR	ON	2016/04/28 10:20

5/2/2016 2:58:23 PM
C:\Users\eoussir\Documents\EAST\Workspaces\13856982_deferring payment on product license until connection is established.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14659502	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/02/2015	04/30/2016							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	-							
	6	✓	-							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17		✓							
	18		✓							
	19		✓							
	20		✓							
	21		✓							
	22		✓							
	23		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14659502	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	6/1/2015	EO
H04L	6/1/2015	EO

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705		6/1/2015	EO

SEARCH NOTES		
Search Notes	Date	Examiner
Consulted J. Hayes D.P rejection	6/2/2015	EO
Consulted Clavin H.	6/12/2015	EO
Google search	6/4/2015	EO
East search	6/4/2015	EO

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Francisco Martinez de Velasco Cortina		
Application No.:	14/659,502	Examiner:	OUSSIR, EL MEHDI
Filing Date:	March 16, 2015	Group Art Unit:	3685
Confirm. No.	3012	Attorney Docket No.	116546-661CT2

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

PRE-APPEAL BRIEF ACCOMPANYING PRE-APPEAL BRIEF REQUEST FOR REVIEW

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

Sir:

Pursuant to the Final Office Action mailed on May 16, 2016, Applicant files this Pre-Appeal Brief Request for Review. This Request is accompanied by the filing of a Notice of Appeal. Applicant turns now to the rejections at issue:

Double Patenting

Upon the indication of allowable subject matter, and provided the double patenting rejection is still maintained and pertinent with respect to the otherwise allowable claims, Applicant will submit a terminal disclaimer to obviate that double patenting rejection. Accordingly, Applicant requests that the provisional double patenting rejection be held in abeyance pending the indication of allowable subject matter.

Claim Rejections - 35 U.S.C. § 101

The Examiner has rejected Claims 1-16 under 35 U.S.C. § 101 as being directed toward a judicial exception. Applicant respectfully disagrees with the Examiner's analysis and conclusion. The first step of the two part *Alice/Mayo* test is to determine whether the claim is directed to an . . . abstract idea. *See The 2014 Interim Guidance on Patent Subject Matter Eligibility* at Page 10. If it is determined that the claim is directed to an abstract idea, then the

second part of the *Mayo* test is to determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claims amount to significantly more than the abstract idea. *See Id.* at 20. Fundamental to the *Mayo* test is the premise that an analysis of the claim limitations must take place. As noted in *The 2014 Interim Guidance* on page 11, "[a] claim is directed to a judicial exception when . . . an abstract idea is recited (i.e., *set forth or described) in the claim* (emphasis added)." This requires an actual analysis and indication of where in the claim, i.e., what limitations combine to describe or set forth the abstract idea. Only then can one examine the remaining claim elements to ascertain whether they add significantly more than the abstract idea. As noted in *Enfish, LLC, v. Microsoft Corporation, et al.*, Slip Op. (2016), it is not sufficient to simply ask whether a claim involves a patent-ineligible concept, rather the proper inquiry asks whether the character of the claims as a whole and considered in light of the specification are directed to excluded subject matter. *See Id.* at page 10.

Unusual for such rejections, the supposed abstract idea provided is not some extremely high level summary of what the claim is directed to. Rather, the abstract idea as defined in the Action is extremely detailed revealing in and of itself that the claims are not directed to an abstract idea. As admitted in the Action the claims are directed to "a secure way of conducting a transaction utilizing a mobile device which generates a key, encrypts it, and provides a key using a form of communication in order to settle the transaction. The key is generated once the user has supplied biometric information to the mobile device and the device authenticates the biometric data of the user based on the stored biometric data." See paragraph 6 of the Final Action. There is nothing abstract about such a claim. One can argue whether it is patentable, but not whether it is abstract.

As pointed out in the *McRO* decision, whereas here the claims provide a particular solution to the problem, i.e., using a mobile device configured to provide a secure way of conducting a transaction by generating a key, encrypting it, and only after confirming a biometric, as opposed to merely claiming the idea of a solution, the claims are directed to patent eligible subject matter. *See the November 2, 2106, Memo to Patent Examining Corp Regarding: Recent Subject Matter Eligibility Decisions*, at Page 3.

Applicant previously pointed out several reasons, grounded in case law as to why the claims were not directed to an abstract idea under the first prong of the *Alice/Mayo* test. But the Examiner never addressed those arguments in the Final Action and in paragraph 6 simply

went to the second step of the *Alice/Mayo* test and stated that the claims don't add significantly more. Interestingly, this is where the Examiner provided the evidence that the claims are not abstract noting that the claims "recite a secure way of conducting a transaction utilizing (sic) a mobile device which generates a key, encrypts it, and provides the key using a form of communication in order to settle a transaction" and that "[t]he key is generated once the user has supplied biometric information to the mobile device." This is exactly the type of particular solution to a problem or particular way of achieving a desired outcome that elevates the claims above an abstract idea as note in the *McRO* decision. *See Memo to the Patent Examining Corps Regarding: Recent Subject Matter Eligibility Decisions* at page 3.

The Examiner then indicates that one reason the claims are not directed to significantly more is because they can be carried out generic computer/device. But of course this in and of itself is meaningless. The *Enfish* court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." See *Enfish* at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. *See Id*. Here the claims inarguably are directed to an improvement in the device/system, e.g., by providing increased security as admitted in the Action. As in *BASCOM*, the claimed combination provides a solution, grounded in technology that is significantly more than an abstract idea of comparing and storing information, even if the claims are implemented on what is otherwise generic computer components. Accordingly, Appellant respectfully submits that the claims pass step two of *Alice's* two-part framework because an inventive concept can be found in the ordered combination of claim limitations that transform the alleged abstract idea into a practical application thereof. Again, this is not a question of whether the claim is patentable, just whether it is patent eligible, which it inarguably is.

Moreover, paragraph 7 of the Examiner's response to Applicant's arguments in the Final Action then purports to provide a laundry list of abstract ideas that the claims are purportedly directed to including: comparing data, collecting and comparing known information, obtaining and comparing intangible data, comparing new, stored information using rules to identify options, managing relationships or creating contractual relationships. Throwing out a laundry list of potential abstract ideas such as in this Action has been seen as evidence the claims are in fact not directed to an abstract idea. In *DDR Holdings, LLC, v. Hotels.com, L.P, et al.*, (Slip op. at page 19), the Federal Circuit recently pointed to defendants

"varying formulation of the underlying abstract idea" as evidence that the claims may not in fact be directed to an abstract idea. There as here, an analysis of the claims revealed much more than any of the alleged abstract ideas the claims were supposed to embody.

It is worth noting here that any claim related to a financial transaction is not therefore automatically directed to the abstract idea of a fundamental economic practice. Fundamental economic practices are things like risk hedging an intermediate settlement, i.e., long standing and fundamental concepts. Using biometric information to authenticate payment information, a secure module to secure that information and providing it via RF circuitry with a mobile device does not fit the bill. As the court in *Alice* stated: "in applying §101 exception, we must distinguish between patents that claim the 'buildin[g] blocks' of human ingenuity and those that integrate the building blocks into something more." *See Alice Corp. V. CLS Bank Int'l,* 573 U.S. ___ (Slip Op. at page 8) (2014), *citing to Mayo* 566 U.S. at __ (Slip Op. at 20). In this case we clearly have something more.

As further evidence that these claims include statutory subject matter, Applicant presents features recited in claim 1 from issued patent 8,933,807 (the '807 patent) which is a priority application of this application:

> *1. A mobile device, comprising:*
> *radio frequency (RF) cellular circuitry;*
> *short range RF circuitry;*
> *memory configured to store biometric authentication .....;*
> *a biometric reading device configured to .....;*
> *an authentication module configured to authenticate .....; and*
> *a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.*

Pending claim 1, includes many of the features in claim 1 of the '807 patent including: the short range RF circuitry, the memory storing biometric authentication information, and an authentication module. The claims in the '807 patent and the pending claims include nearly identical features for all intents and purposes under 35 U.S.C §101. Since the '807 patent was allowed after the Alice case, and 101 rejections were never raised, it is respectfully submitted that if the claims of the '807 are patentable, and they are in fact patented, then so are the pending claims. The only real difference between the issued claim 1 and pending claim 1 is the use of the "secure module" versus the "transaction module". The Office Action essentially asserts that it was the transaction module in the '807 that made those claims

directed to patentable subject matter, but replacing the transaction module with the secure module removes it from patentability. Applicant respectfully disagrees with the Examiner's analysis and conclusion.

Claim Rejections - 35 U.S.C. § 103(a)

Detailed arguments traversing these rejections were presented on pages 9-11 in the response filed December 22, 2015 and the Examiner is directed to reconsider those arguments. Synopses of these arguments are presented here. Instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory as recited in each of independent Claims 1 and 10.

The Examiner concedes that the combination of Walker and Holmes does not disclose key encryption and payment information storage, and proffers that Chen discloses these features set forth in independent Claims 1 and 10. (Office Action, at p. 7). Page 11 of the December 22, 2015 response presents details regarding the Applicant's belief that the Examiner is incorrect in stating that Chen discloses these features. For at least the foregoing reasons, independent Claims 1 and 10 are believed to be allowable. The remaining claims depend, either directly or indirectly, on the aforementioned independent claims and are therefore believed to be allowable for the same reasons described above.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: November 16, 2016

/Noel C. Gillespie/
Noel C. Gillespie
Reg. No. 47,596

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): 116546-661CT2

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____.

Signature _____

Typed or printed name _____

In re Application of: Francisco Martinez de Velasco Cortina

Application Number	Filed
14/659,502	March 16, 2015

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Art Unit	Examiner
3685	OUSSIR, EL MEHDI

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800

☐ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ _____

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☑ Payment by credit card. Form PTO-2038 is attached.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 502075.

☑ Payment made via EFS-Web.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant

☑ attorney or agent of record
Registration number 47596

☐ attorney or agent acting under 37 CFR 1.34
Registration number _____

Signature /Noel C. Gillespie/

Typed or printed name Noel C. Gillespie

Telephone Number 6192381900

Date November 16 2016

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: AP.PRE.REQ

PTO/AIA/33 (03-13)
Approved for use through 07/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
116546-661CT2

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on _____

Signature _____

Typed or printed name _____

Application Number	Filed
14/659,502	March 16, 2015

First Named Inventor: Francisco Martinez de Velasco Cortina

Art Unit	Examiner
3685	OUSSIR, EL MEHDI

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 47596.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Noel C. Gillespie/
Signature

Noel C. Gillespie
Typed or printed name

(619) 238-1900
Telephone number

November 16 2016
Date

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie/cindy guido
Attorney Docket Number:	116546-661CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
NOTICE OF APPEAL	1401	1	800	800
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**2200**

Electronic Acknowledgement Receipt

EFS ID:	27534923
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie
Filer Authorized By:	
Attorney Docket Number:	116546-661CT2
Receipt Date:	16-NOV-2016
Filing Date:	16-MAR-2015
Time Stamp:	18:58:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2200
RAM confirmation Number	111716INTEFSW18592100
Deposit Account	502075
Authorized User	cindy guido
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Pre-Brief Conference request	116546_661CT2_Pre_Appeal_Brief.PDF	63688 e5e507c619b8dde40762bc1500d0f9fb04fcffea	no	5
Warnings:					
Information:					
2	Notice of Appeal Filed	Notice_of_Appeal_116546_661CT2.PDF	235926 7868a4c51be66ef6bc7af119d8b359ddd2570c6f	no	2
Warnings:					
Information:					
3	Pre-Brief Conference request	Pre_Appeal_Brief_Conference_Request_116546_661CT2.PDF	188996 65d06275ea5bb5ab812bfd4c6f68f7842d2d5dd0	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32448 3ca011a6666b81cf400e1d95f89b4d21a5452c2c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	521058		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2	3012

27189 7590 11/30/2016

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
11/30/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of Panel Decision from Pre-Appeal Brief Review	Application No. 14/659,502	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner EL MEHDI OUSSIR	Art Unit 3685

This is in response to the Pre-Appeal Brief Request for Review filed 16 November, 2016.

1. ☐ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☒ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☒ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1-4, 7-23*.
Claim(s) withdrawn from consideration: _____.

3. ☐ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☐ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:		
(1) *EL MEHDI OUSSIR*.		(3) *Mamon Obeid*.
(2) *John Hayes*.		(4)_____.
/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/Mamon Obeid/ Primary Examiner, Art Unit 3685	/JOHN HAYES/ Supervisory Patent Examiner, Art Unit 3685

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIALS AND APPEALS BOARD

In re application of: NEOLOGY, INC. Docket No: 116546-661CT2

Appln. No.: 14/659,502 Group Art Unit: 3685

Confirmation No.: 3012 Examiner: OUSSIR, EL MEHDI

Filed: March 16, 2015

For: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant respectfully submits this Appeal Brief in response to the Final Office Action ("Office Action") dated May 16, 2016.

Table of Contents

I. REAL PARTY IN INTEREST 2
II. RELATED APPEALS, INTERFERENCES, AND TRIALS 3
III. SUMMARY OF THE CLAIMED SUBJECT MATTER 4
IV. ARGUMENT 7
V. CONCLUSION 17
CLAIMS APPENDIX 18
EVIDENCE APPENDIX 22

I. REAL PARTY IN INTEREST

Neology, Inc. of Poway, California, is the real party in interest.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

To the knowledge and belief of Appellant, the Assignee, and the Appellant's legal representative, there are no other prior or pending appeals, interferences, trials before the Board, or judicial proceedings that will directly affect or be affected by the Board's decision in the instant Appeal.

III. SUMMARY OF THE CLAIMED SUBJECT MATTER

The summary of the invention in connection with claims 1-4 and 7-16 in relation to exemplary embodiments are set forth below. The paragraph and line numbers refer to the paragraph and line numbers of the specification as filed.

The present embodiments provide systems and methods for improved management and profitability of take-out ordering through order sharing.

1. A mobile device, comprising:

short range radio frequency (RF) circuitry (¶¶ [0013] - [0014]);

memory (FIG. 2, ¶ [0014], line 14) configured to store biometric authentication information and payment information (¶ [0069]);

a biometric module configured to read biometric information (¶ [0067]);

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory (¶ [0073]); and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory (¶ [0053], "*Secure Identification*");

encrypt the key and the payment information stored in memory (¶ [0053], "*Secure Identification*" and "*Secure Transaction*"); and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction (¶ [0053], "*Secure Transaction*" and "*Secure Data Base*").

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry (¶¶ [0013] - [0014]);

memory (FIG. 2, ¶ [0014], line 14) configured to store biometric authentication information and payment information (¶ [0069]);

a biometric module configured to read biometric information (¶ [0067]);

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory (¶ [0073]); and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory (¶ [0053], "*Secure Identification*");

encrypt the key and the payment information stored in memory (¶ [0053], "*Secure Identification*" and "*Secure Transaction*"); and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction (¶ [0053], "*Secure Transaction*" and "*Secure Data Base*"); and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information (¶¶ [0053] and [0059]-[0064]); and

transmit, to a central database, the encrypted key and payment information (¶¶ [0053], "*Secure Transaction*" and "*Secure Data Base*"); and

a central database configured to validate the key and the payment information(¶¶ [0053], "*Secure Transaction*" and "*Secure Data Base*").

17. A method for secure transactions using a mobile device, comprising:

storing biometric authentication information and payment information (¶ [0069]) in memory (FIG. 2, ¶ [0014], line 14);

reading biometric information using a biometric reader (¶ [0067]);

determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory (¶ [0073]);

generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory (¶ [0053], "*Secure Identification*");

encrypting the key and the payment information stored in memory (¶ [0053], "*Secure Identification*" and "*Secure Transaction*"); and

providing the encrypted key and payment information for use in a transaction (¶ [0053], "*Secure Transaction*" and "*Secure Data Base*").

IV. ARGUMENT

By way of summary, Claims 1-4 and 7-23 are pending in the present application and stand rejected. **Claims 1-4, 7-23** stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. **Claims 1-4, 8-13, 15-20, and 22-23** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048) in further view of Chen et al. (U.S. Patent No. 5,590,197). **Claims 7, 14 and 21** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Holmes in view of Chen and in further view of Voltmer et al. (U.S. Patent Application Publication 2002/0112177). **Claims 1-4 and 7-16** stand provisionally rejected on the ground of nonstatutory double patenting over claims 1-16 of copending Application No. 14/639,034 in view of U.S. Patent 6,163,771 to Walker. Appellant respectfully submits that each of these rejections is in error for at least the reasons set forth below.

Rejection under 35 U.S.C. 101 – Claims 1-16

Claims 1-4, 7-23 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant traverses the rejection because the claims are not directed to an abstract idea, and even if they were, they do add significantly more.

The first step of the two part Alice/Mayo test is to determine whether the claim is directed to an . . . abstract idea. See *The 2014 Interim Guidance on Patent Subject Matter Eligibility* at Page 10. If it is determined that the claim is directed to an abstract idea, then the second part of the Mayo test is to determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claims amount to significantly more

than the abstract idea. *See Id.* at 20. Fundamental to the *Mayo* test is the premise that an analysis of the claim limitations must take place. As noted in *The 2014 Interim Guidance* on page 11, "[a] claim is directed to a judicial exception when . . . an abstract idea is recited (i.e., set forth or described) in the claim (emphasis added)." This requires an actual analysis and indication of where in the claim, i.e., what limitations combine to describe or set forth the abstract idea. Only then can one examine the remaining claim elements to ascertain whether they add significantly more than the abstract idea. As noted in *Enfish, LLC, v. Microsoft Corporation*, et al., Slip Op. (2016), it is not sufficient to simply ask whether a claim involves a patent-ineligible concept, rather the proper inquiry asks whether the character of the claims as a whole and considered in light of the specification are directed to excluded subject matter. *See Id.* at page 10. The court went on to explain that it is improper to simply summarize the entire claim at a high level of abstraction as being directed to, e.g., an abstract idea, untethered from the actual language of the claims. *See Id.* at page 14.

Here, as is often the case with such *Alice* rejections, the Office Action fails to properly identify the abstract idea through analyzing and identifying the limitation or limitations that describe or set forth the abstract idea. Not only is this an incorrect application of the first step of the *Mayo* test, as noted in *Enfish*, it prevents any meaningful application of the second step. Moreover, the claims are not directed to an abstract idea, even if the *Mayo* test is applied correctly.

Unusual for such rejections, the supposed abstract idea provided is not some extremely high level summary of what the claim is directed to. Rather, the abstract idea as defined in the Action is extremely detailed revealing in and of itself that the claims are not

directed to an abstract idea. As admitted in the Action the claims are directed to "a secure way of conducting a transaction utilizing a mobile device which generates a key, encrypts it, and provides a key using a form of communication in order to settle the transaction. The key is generated once the user has supplied biometric information to the mobile device and the device authenticates the biometric data of the user based on the stored biometric data." See paragraph 6 of the Office Action. There is nothing abstract about such a claim. One can argue whether it is patentable, but not whether it is abstract.

As pointed out in the *McRO* decision, whereas here the claims provide a particular solution to the problem, i.e., using a mobile device configured to provide a secure way of conducting a transaction by generating a key, encrypting it, and only after confirming a biometric, as opposed to merely claiming the idea of a solution, the claims are directed to patent eligible subject matter. See the *November 2, 2106, Memo to Patent Examining Corp Regarding: Recent Subject Matter Eligibility Decisions*, at Page 3.

Applicant previously pointed out several reasons, grounded in case law as to why the claims were not directed to an abstract idea under the first prong of the *Alice/Mayo* test. But the Examiner never addressed those arguments in the Office Action and in paragraph 6 simply went to the second step of the *Alice/Mayo* test and stated that the claims don't add significantly more. Interestingly, this is where the Examiner provided the evidence that the claims are not abstract noting that the claims "recite a secure way of conducting a transaction utilizing (sic) a mobile device which generates a key, encrypts it, and provides the key using a form of communication in order to settle a transaction" and that "[t]he key is generated once the user has supplied biometric information to the mobile device." This is exactly the type of particular solution to a problem or particular way of achieving a desired

outcome that elevates the claims above an abstract idea as note in the *McRO* decision. See *Memo to the Patent Examining Corps Regarding: Recent Subject Matter Eligibility Decisions* at page 3.

The Examiner then indicates that one reason the claims are not directed to significantly more is because they can be carried out generic computer/device. But of course this in and of itself is meaningless. The *Enfish* court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." *See Enfish* at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. *See Id*. Here the claims inarguably are directed to an improvement in the device/system, e.g., by providing increased security as admitted in the Action. As in *BASCOM*, the claimed combination provides a solution, grounded in technology that is significantly more than an abstract idea of comparing and storing information, even if the claims are implemented on what is otherwise generic computer components. Accordingly, Appellant respectfully submits that the claims pass step two of *Alice's* two-part framework because an inventive concept can be found in the ordered combination of claim limitations that transform the alleged abstract idea into a practical application thereof. Again, this is not a question of whether the claim is patentable, just whether it is patent eligible, which it inarguably is.

Moreover, paragraph 7 of the Examiner's response to Applicant's arguments in the Office Action then purports to provide a laundry list of abstract ideas that the claims are purportedly directed to including: comparing data, collecting and comparing known information, obtaining and comparing intangible data, comparing new, storing information

using rules to identify options, managing relationships or creating contractual relationships. Throwing out a laundry list of potential abstract ideas such as in this Action has been seen as evidence the claims are in fact not directed to an abstract idea. In *DDR Holdings, LLC, v. Hotels.com, L.P., et al.*, (Slip op. at page 19), the Federal Circuit recently pointed to defendants "varying formulation of the underlying abstract idea" as evidence that the claims may not in fact be directed to an abstract idea. There as here, an analysis of the claims revealed much more than any of the alleged abstract ideas the claims were supposed to embody.

It is worth noting here that any claim related to a financial transaction is not therefore automatically directed to the abstract idea of a fundamental economic practice. Fundamental economic practices are things like risk hedging an intermediate settlement, i.e., long standing and fundamental concepts. Using biometric information to authenticate payment information, a secure module to secure that information and providing it via RF circuitry with a mobile device does not fit the bill. As the court in *Alice* stated: "in applying §101 exception, we must distinguish between patents that claim the 'buildin[g] blocks' of human ingenuity and those that integrate the building blocks into something more." *See Alice Corp. V. CLS Bank Int'l, 573 U.S.* (Slip Op. at page 8) (2014), citing to *Mayo* 566 U.S. at (Slip Op. at 20). In this case we clearly have something more.

As further evidence that these claims include statutory subject matter, Applicant presents features recited in claim 1 from issued patent 8,933,807 (the '807 patent) which is a priority application of this application:

> *1. A mobile device, comprising:*
>
> *radio frequency (RF) cellular circuitry;*

short range RF circuitry;

memory configured to store biometric authentication .....;

a biometric reading device configured to .....;

an authentication module configured to authenticate .....; and

a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module.

Pending claim 1, includes many of the features in claim 1 of the '807 patent including: the short range RF circuitry, the memory storing biometric authentication information, and an authentication module. The claims in the '807 patent and the pending claims include nearly identical features for all intents and purposes under 35 U.S.C. §101. Since the '807 patent was allowed after the Alice case, and 101 rejections were never raised, it is respectfully submitted that if the claims of the '807 are patentable, and they are in fact patented, then so are the pending claims. The only real difference between the issued claim 1 and pending claim 1 is the use of the "secure module" versus the "transaction module". Thus, the Office Action essentially asserts that it was the transaction module in the '807 that made those claims directed to patentable subject matter, but replacing the transaction module with the secure module removes it from patentability. Applicant respectfully disagrees with the Examiner's analysis and conclusion.

Rejection under 35 U.S.C. 103(a) – Claims 1-4 and 7-23

Claims 1-4, 8-13, 15-20, and 22-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048) in further view of Chen et al. (U.S. Patent No. 5,590,197). Claims 7, 14 and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Holmes in view of Chen and in further view of Voltmer et al. (U.S. Patent Application Publication 2002/0112177).

According to the Examiner, with the exception of short range radio frequency (RF) circuitry, key encryption, and payment information storage, Walker discloses all of the limitations set forth in independent Claims 1, 10 and 17. Applicant respectfully disagrees. First, to the extent that Walker discloses a biometric interface, biometric information is used to control access to a device such as a smartcard. For example, Walker states that "the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent Claims 1, 10 and 17 each set forth that biometric information must be successfully authenticated in order for a secure module to "generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction." Thus, Walker fails to disclose using biometric information to control the generation, encryption, and transmission of a key and payment information.

Second, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1, 10 and 17, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. According to Walker, "the cardholder first inputs his PIN or biometric data to access the device [...]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number [...]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")." (Walker, at 6:18-25, emphasis added). Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt[ing...] the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as recited in each of independent Claims 1, 10 and 17.

In addition, Walker describes generating a single-use credit card number, which "is distinct from the unchanging account number identifying the particular cardholder." (Walker, at 6:66-7:1). The single-use credit card number is formed by concatenating an encrypted nonce, an initialization vector, and the account number. Thus, contrary to the Examiner's rejection, Walker does not teach or suggest "provid[ing...] the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1, 10 and 17.

The Examiner concedes that the combination of Walker and Holmes does not disclose key encryption and payment information storage, and proffers that Chen discloses these features set forth in independent Claims 1, 10 and 17. (Office Action, at p. 13, Item

"h", and at p. 18, Item "i"). Interestingly, the Examiner took a contradictory position on Page 7 of the Office Action mailed on May 29, 2015 for co-pending Application No. 14/639,034 where he appears to state that Holmes discloses both features. Nevertheless, Applicant respectfully submits that Walker, Holmes, and Chen, whether considered independently or in combination, do not teach or suggest "memory configured to store biometric authentication information and payment information; a biometric module configured to read biometric information; an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and a secure module configured to: generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1, 10 and 17.

For at least the foregoing reasons, independent Claims 1, 10 and 17 are believed to be allowable. The remaining claims depend, either directly or indirectly, on the aforementioned independent claims and are therefore believed to be allowable for the same reasons described above.

Double Patenting

Claims 1-4 and 7-16 stand provisionally rejected on the ground of nonstatutory double patenting over claims 1-16 of copending Application No. 14/639,034 in view of U.S.

Patent 6,163,771 to Walker. Upon the indication of allowable subject matter, and provided the double patenting rejection is still maintained and pertinent with respect to the otherwise allowable claims, Applicant will submit a terminal disclaimer to obviate that double patenting rejection.

V. CONCLUSION

The statutory fee (37 C.F.R. §41.37(a) and 1.17(c)) is being remitted. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 502075. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/ Daniel K. Robertson /
Daniel K. Robertson
Registration No. 48,077

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900 (Phone)
(619) 235-0398 (Fax)

27189
CUSTOMER NUMBER

Date: April 18, 2017

CLAIMS APPENDIX

CLAIMS 1-4 and 7-23 ON APPEAL:

1. A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

5. (Canceled)

6. (Canceled)

7. The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. The system of claim 10, wherein the payment information is associated with a primary account number.

13. The system of claim 10, wherein the POS device includes an RF reader.

14. The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

17. A method for secure transactions using a mobile device, comprising:
storing biometric authentication information and payment information in memory;
reading biometric information using a biometric reader;
determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;
generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;
encrypting the key and the payment information stored in memory; and
providing the encrypted key and payment information for use in a transaction.

18. The method of claim 17, further comprising reading biometric information provided by a user to complete the transaction.

19. The method of claim 17, wherein the payment information is associated with a primary account number.

20. The method of claim 17, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

21. The method of claim 17, wherein the biometric authentication information is stored separately from the payment information.

22. The method of claim 17, wherein the payment information is stored in a memory accessible only by a secure module.

23. The method of claim 17, wherein the payment information is provided using a short range RF circuitry.

EVIDENCE APPENDIX

Pursuant to 37 C.F.R. § 41.37(c)(1)(ix), submitted herewith are copies of any evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellant in the appeal.

NONE.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Daniel K. Robertson/cindy guido
Attorney Docket Number:	116546-661CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 4 months with $0 paid	1254	1	2200	2200
Miscellaneous:				
			Total in USD ($)	**2200**

Electronic Acknowledgement Receipt

EFS ID:	28960176
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/cindy guido
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-661CT2
Receipt Date:	18-APR-2017
Filing Date:	16-MAR-2015
Time Stamp:	17:33:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2200
RAM confirmation Number	041917INTEFSW17350100
Deposit Account	502075
Authorized User	cindy guido
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	Appeal_Brief_116546-661CT2.PDF	86872 dc5776912f9ae3a3fd03683a82d4326e61d0f6ca	no	22
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30833 59b905e7db7aecec7654a615513bb805954f40b9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	117705		

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

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

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

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6934861	B2	2005-08-23	Haala	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070022058	A1	2007-01-25	Labrou	
	2	20060020558	A1	2006-01-26	Bonalle	
	3	20040128249	A1	2004-07-01	Hoffman	
	4	20020112177	A1	2002-08-15	Voltmer	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ATMEL, Atmel Smart Card ICs, Silicon solutions making smart cards smarter, 12 pages.	
	2	Extended European Search Report, European Patent Application No. 10182033.0, dated 13 January 2012, 7 pages.	
	3	FANCHER, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE SPECTRUM, February 1997, 7 pages.	
	4	RAKERS, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	
	5	Japanese Office Action, Japanese Patent Application No. 2004-519130, dated 12 May 2009, 10 pages.	X
	6	ANONYMOUS, Read/write RFID offers standalone advantages, Security, August 1996; 33, 8; ProQuest, 1 page.	☐
	7	Response to Office Action filed on May 2, 2017 for US patent application no. 15/372,317.	☐
	8	US Office Action dated February 2, 2017 received in US patent application no. 15/372,317.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	9		☐
	10	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	☐
	11	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	☐
	12	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	☐
	13	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	☐
	14	US Notice of Allowance dated July 11, 2014 received in US patent application no. 14/022,135.	☐
	15	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	☐
	16	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	☐
	17	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	☐
	18	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	☐
	19	Appeal Brief filed February 9, 2017 for US patent application no. 14/585,057.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	20	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	☐
	21	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 9, 2016 for US patent application no. 14/585,057.	☐
	22	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	☐
	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	☐
	24	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	☐
	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	☐
	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	☐
	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	☐
	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	☐
	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	☐
	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	31	US Office Action dated April 3, 2014 received in US patent application no. 14/028,469.	☐
	32	Response to Office Action filed on March 14, 2014 for US patent application no. 14/028,469.	☐
	33	US Office Action dated March 6, 2014 received in US patent application no. 14/028,469.	☐
	34	Response to Office Action filed on February 3, 2014 for US patent application no. 14/028,469.	☐
	35	US Office Action dated December 6, 2013 received in US patent application no. 14/028,469.	☐
	36	Appeal Brief filed January 30, 2017 for US patent application no. 14/639,034.	☐
	37	Pre-Brief Appeal Conference Decision dated July 21, 2016 and received in US patent application no. 14/639,034.	☐
	38	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on June 30, 2016 for US patent application no. 14/639,034.	☐
	39	US Office Action dated December 30, 2015 received in US patent application no. 14/639,034.	☐
	40	Response to Office Action filed on November 30, 2015 for US patent application no. 14/639,034.	☐
	41	US Office Action dated May 29, 2015 received in US patent application no. 14/639,034.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	42	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	☐
	43	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	☐
	44	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	☐
	45	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 7, 2016 for US patent application no. 14/724,593.	☐
	46	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	☐
	47	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	☐
	48	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-03
Name/Print	Daniel K. Robertson	Registration Number	48077

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Daniel K. Robertson/gloria mimi choi
Attorney Docket Number:	116546-661CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	29103913
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/gloria mimi choi
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-661CT2
Receipt Date:	03-MAY-2017
Filing Date:	16-MAR-2015
Time Stamp:	15:12:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$180
RAM confirmation Number	050417INTEFSW15132400
Deposit Account	502075
Authorized User	Gloria Choi

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	NPL_Atmel_Smart_Card_ICs.PDF	3746165 4862be31ab88fe24fd7e58d14c50958ef0eee5b9	no	12
Warnings:					
Information:					
2	Non Patent Literature	NPL_EESR_EP101820330.PDF	317763 68c8d8533e174701d6a8817cd26a4ea7ba36a018	no	7
Warnings:					
Information:					
3	Non Patent Literature	NPL_Fancher_In_your_pocket_smartcards.PDF	1969305 b9269a1b51049e246d75166e113ae54d39cb90c9	no	7
Warnings:					
Information:					
4	Non Patent Literature	NPL_Rakers_Secure_Contactless_Smartcard_ASIC_with_DPA_Protection.PDF	655066 ce772b672ba90fd289cc285f25f435ee27ab3be4	no	7
Warnings:					
Information:					
5	Non Patent Literature	NPL_JP_OA_JP2004519130.PDF	1158006 71c35b56c987b1acbfcae2d92f46ca9d1f10c9b6	no	10
Warnings:					
Information:					
6	Non Patent Literature	NPL_Anonymous_ReadWrite_RFID_Offers_Standalone.PDF	173548 c0f146328abb3362dac83e497dcd7f6c3b5b49a6	no	1
Warnings:					
Information:					

7		NPL_15372317_Rejections_and_Amendments.PDF	559675 6e2132f6156a8e358b3740650cfc594605ad2c68	yes	19

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	11
	Non Patent Literature	12	19

Warnings:

Information:

8		NPL_14321781_Rejections_and_Amendments.PDF	3697373 36aec421706a841c03ac4c3b65ef9ce60ba869b4	yes	97

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	16
	Non Patent Literature	17	43
	Non Patent Literature	44	74
	Non Patent Literature	75	97

Warnings:

Information:

9		NPL_14022135_Rejections_and_Amendments.PDF	1536852 79921e073d780349bcd5776b899b8d476c82cb72	yes	45

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	10
	Non Patent Literature	11	17
	Non Patent Literature	18	27
	Non Patent Literature	28	34

	Non Patent Literature		35	45	
Warnings:					
Information:					
10		NPL_14585057_Rejections_and_Amendments.PDF	3499096 1dc64e89387a504a23f327e389f4781426c6c214	yes	94
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	16	
	Non Patent Literature		17	18	
	Non Patent Literature		19	27	
	Non Patent Literature		28	56	
	Non Patent Literature		57	69	
	Non Patent Literature		70	94	
Warnings:					
Information:					
11		NPL_14028469_Rejections_and_Amendments.PDF	4322660 77ad3bf14f3aa49a053ede8b281047eb20dbe67f	yes	120
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	8	
	Non Patent Literature		9	16	
	Non Patent Literature		17	28	
	Non Patent Literature		29	46	
	Non Patent Literature		47	60	
	Non Patent Literature		61	68	

	Non Patent Literature		69	82	
	Non Patent Literature		83	89	
	Non Patent Literature		90	98	
	Non Patent Literature		99	106	
	Non Patent Literature		107	120	
Warnings:					
Information:					
12		NPL_14639034_Rejections_and_Amendments.PDF	3120565 d76fc6256d9d9cded3c2ae7c9abebac8fa8ac21e	yes	82
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	17	
	Non Patent Literature		18	19	
	Non Patent Literature		20	29	
	Non Patent Literature		30	52	
	Non Patent Literature		53	63	
	Non Patent Literature		64	82	
Warnings:					
Information:					
13		NPL_14724593_Rejections_and_Amendments.PDF	3891697 c904b0c7dc2ee6cba8ce4b97f09fd98dc08e3963	yes	106
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	8	
	Non Patent Literature		9	30	

	Non Patent Literature	31	32	
	Non Patent Literature	33	41	
	Non Patent Literature	42	70	
	Non Patent Literature	71	82	
	Non Patent Literature	83	106	
Warnings:				
Information:				
14	Information Disclosure Statement (IDS) Form (SB08)	IDS_SB08_TBF_116546-661CT2.PDF	613466 46e9258e25e57a2fdbfb3dc4185a50db3dc67180	no	8
Warnings:				
Information:				
15	Fee Worksheet (SB06)	fee-info.pdf	30646 07da66ea588c657e704e3d56bb062d29f74abf38	no	2
Warnings:				
Information:				
		Total Files Size (in bytes):	29291883	

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2	3012

27189 7590 07/26/2017

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/26/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Application Number: 14/659,502
Filing Date: March 16, 2015
Appellant(s): MARTINEZ DE VELASCO CORTINA ET AL.

Daniel K. Robertson Reg. No. 48,077
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/18/2017 ("Brief") appealing from the office action mailed 05/16/2016 ("Final Rejection").

1) Grounds of Rejection to be Reviewed on Appeal

Every ground of rejection set forth in the Office action dated December 31, 2015 (hereinafter "the Office Action") from which the appeal is taken is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(2) Response to Argument

The Appellant's argument in regards to claim rejections under 35 U.F.C. §101 have been reviewed but are not persuasive.

The Appellant's argument in regards to claim rejections under 35 U.F.C. §103(a) have been reviewed but are not persuasive.

In the Appeal Brief, filed on February 09, 2017 Appellant makes the following arguments:

I. Claims 1-4, 7-16: Double Patenting.

The Appellant asserts on pages 15-16 of the Brief the following:

Upon the indication of allowable subject matter, and provided the double patenting rejections are still maintained and pertinent with respect to the otherwise allowable claims, Applicant will submit a terminal disclaimer to obviate that double patenting rejection.

Examiner's Response:

The Examiner acknowledges the above and will hold the rejection in abeyance.

II. Claims 1-4, 7-23: §101 Rejection Based on Non-Statutory Subject Matter.

The Appellant asserts on pages 7-12 of the Brief the following:

i. **Unlike most recent Alice rejections, the supposed abstract idea provided in the Action is not an extremely high level summary of what the claim is directed to. Rather, the abstract idea as defined in the Action is extremely detailed revealing in and of itself that the claims are not directed to an abstract idea. As admitted in the Action the claims are directed to "a mobile device used in payment transaction with a point of sale terminal using security measures to increase security and operate using short range radio frequency." There is nothing abstract about such a claim.**

A. The Examiner respectfully disagrees. Throughout prosecution, the Examiner has applied the two step Alice/Mayo analysis set forth by the Supreme Court

in order to determine whether the claims individually or as a whole amount to an abstract idea. The Examiner clearly carried out the two step analysis set by the Court.

The Examiner disagrees with the Applicant arguments that a prima facie case was not established and that the proper analysis to determine whether the claims are abstract or not. The Examiner considered the claims in part and as a whole in order to apply the Mayo test to determine if the claims are rejected under 35 U.S.C. 101 for claiming an abstract idea. Once the determination was made that the claims are directed to a judicially recognized exception, the Examiner then considered the claims individually and as a whole to determine whether or not they amount to significantly more than the abstract idea. The claims are not found to include the significance of any additional element(s) which include improving another technology or technical field, improve the functioning of a computer itself, applied the abstract idea with, or by use of, a particular machine (not a generic computer, not adding the words "apply it" or words equivalent to "apply the abstract idea", not mere instructions to implement an abstract idea on a computer), effects a transformation or reduction of a particular article to a different state or thing, adds a specific limitation other than what is well understood, routine and conventional in the field, adds unconventional steps that confine the claim to a particular useful application, or adds meaningful limitations that amount to more than generally linking the use of the abstract idea to a particular

technological environment. The Examiner thus clearly applied the Court's two step analysis to determine if the claims as a whole are abstract.

The interim guidance provides examples of instances where courts have held certain ideas to be abstract. It was through these examples that the examiner determined, by analogy to the provided examples, that the claims in the present application contain an abstract idea. As such the Examiner contends that a prima facie case has been established and examiner has met the burden of providing support to the 35 USC 101 rejection.

The Claims are directed to an abstract idea of essentially carrying out a financial transaction between two entities. The Examiner detailing the claim limitations is required because every single limitation and the limitations as a whole must be considered when determining whether a claim is abstract. The details of the rejection were done to show without doubt how such a claim is abstract instead of what the Applicant believes is a reason why the claim is not an abstract idea.

Using generic off the shelf device, such as a phone, a computer, or a smart card with a biometric reader and having communications means (none of which the Applicant invented) does not transform the claim(s) into significantly more. Furthermore, using such a device to carry out "extremely detailed" limitations that involve storing data, receiving data, comparing data, and sending data does not in any way transform such "extremely detailed" limitations into significantly more because they are merely routine computer

functions. The claim limitations when considered individually or as a whole do not transform the claim into significantly more. As a result, a clear analysis of the claims, using the two step analysis set by the Court has been carried out and thus a prima facie case has been established in which the claims of this Application are abstract.

ii. **As pointed out in the McRO decision, whereas here the claims provide a particular solution to the problem, i.e., using a mobile device equipped with the ability to store and provide transaction information as well as a biometric sensor configured to provide increased security with respect to such transaction information, as opposed to merely claiming the idea of a solution, the claims are directed to patent eligible subject matter. See the November 2, 2106, Memo to Patent Examining Corp Regarding: Recent Subject Matter Eligibility Decisions, at Page 3.**

B. The Examiner respectfully disagrees. Throughout prosecution, the Examiner has applied the two step Alice/Mayo analysis set forth by the Supreme Court in order to determine whether the claims individually or as a whole amount to an abstract idea. The Applicant's arguments regarding other case law other than Alice/Mayo as set forth by the Court are moot since the basis of the rejection was not in relation to such case law.

However, in McRO, the claims were directed to rules automatically set a keyframe at the correct point to depict more realistic speech, whereas an animator would otherwise have to

manually, and thus subjectively identify the problematic sequence and manually fix it by adding an appropriate keyframe, at the point a phoneme was pronounced to represent a morph target as a starting point further necessitating fine tuning, without evaluating sub-sequences, generating transition parameters or applying transition parameters to create a final morph weight set (see McRO Inc. v. Bandai Namco Games Am. Inc. U.S. Court of Appeals Federal Circuit, Nos. 2015-1080,-1081,-1082,-1083,-1084,-1086,-1087,-1088,-1089,-1090,-1092,-1093,-1094,-1095,-1096,-1097,-1098,-1099,-1100,-1101, September 13, 2016, 2016 BL 297537, 837 F.3d 1299, 120 USPQ2d 1091."

McRO improvement accounted for "rules that define output morph weight set stream as a function of phoneme sequence and time of said phoneme sequence" that "adjust for the fact that a phoneme may look different when spoken depending on the phonemes preceding and/or following it" varying by character as, for example, "a swamp monster will use different rules than a tight-lipped cat" (see McRO page 1098 ¶2-¶4).

The instant claims do not claim such limitations and are not directed to solving the same problem as McRO and that the instant claims are only targeted at conducting a transaction using a device, communication means and data.

iii. **The Examiner then indicates that one reason the claims are not directed to significantly more is because they can be carried out generic computer/device. But of course this in and of itself is meaningless. The Enfish court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." See Enfish at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. See Id. Here the claims inarguably are directed to an improvement in the device/system, e.g., by providing increased security as admitted in the Action.**

C. The Examiner disagrees. The Claims are directed to an abstract idea of essentially carrying out a financial transaction between two entities using data and a communication method. The interim guidance provides examples of instances where courts have held certain ideas to be abstract. It was through these examples that the examiner determined, by analogy to the provided examples, that the claims in the present application contain an abstract idea. Examples of abstract ideas that relate to the claimed invention based on the concepts relating to the processes of comparing data, collecting and comparing known information, obtaining and comparing intangible data, and comparing new and stored information and using rules to identify options are all classified under an idea of itself [see Classen, Cybersource, and

SmartGene]. Also, concepts relating to the claimed limitations include managing relationships or creating a contractual relationship; see buySAFE.

The guidelines clearly recite that the Examiner may rely on "on the knowledge generally available to those in the art, on the case law precedent, on applicant's own disclosure, or on evidence." As a result, the Examiner has clearly noted that the claims do not amount to significantly more than the abstract idea because one of ordinary skill in the art would readily understand the claim limitations to readily implement them using a generic mobile device or computer with executable code.

The courts consider the determination of whether a claim is eligible… to be a question of law. Accordingly, courts do not rely on evidence that a claimed concept is a judicial exception, and in most cases resolve the ultimate legal conclusion on eligibility without making any factual findings. Such cases include, *Alice Corp., Myriad, Mayo, Bilski, Diehr, Flook and Benson.*

Also, the Interim Guidelines, see page 3 of "subject matter eligibility," recite that "judicial exceptions need not be old or long-prevalent, and that even newly discovered judicial exceptions are still exceptions, despite their novelty… [the] Supreme Court's cited rationale for considering even "just discovered" judicial exception as exceptions stems from the concern that "without this exception, there

would be considerable danger that the grant of patents would 'tie up' the use of such tools and thereby 'inhibit future innovation premised upon them.'"

Again, the claims as a whole merely recite a secure method of authenticating a transaction between two entities utilizing a mobile device, which is a fundamental economic practice or an abstract idea of itself. Applicant argues that because the Examiner noted that the method steps are "secure" that the claims result in significantly more. This is not true nor is it true that the Applicant invented the method of obtaining a biometric, comparing it and causing a result based on the comparison. Using biometric means to identify an individual in order to provide enhanced security measures is no different than using other forms of security measures that would yield the same result. The importance here is that the security measure that is implemented is not a method invented by the Applicant (not novel) and even if it was novel, the claim elements as a whole must result in significantly more to determine whether they amount to an abstract idea or not. Using other security measures such as passwords or IRIS scans or the like would merely result in providing further security measures in order to advance a transaction by authenticating the user.

The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more

than significantly more than the abstract idea itself. The claims recite the additional elements of a “device,” “memory,” “RF circuitry,” “biometric module," “authentication module,” “transaction module,” “Internet site.” The “device,” “memory,” “RF circuitry,” “biometric module," “authentication module,” “transaction module,” “Internet site” are only recited at a high level of generality and only perform generic functions of obtaining data, storing data, processing data, comparing data, and transmitting data. Generic computers performing generic computer functions, without an inventive concept, do not amount to significantly more than the abstract idea. The limitations directed to the “device,” “memory,” “RF circuitry,” “biometric module," “authentication module,” “transaction module,” “Internet site” are simply generic and are recited to attempt to limit the abstract idea to a particular technological environment. The type of information being manipulated and obtained does not impose meaningful limitations or render the idea less abstract. Looking at the elements as a combination does not add anything more than the elements analyzed individually. Therefore, the claims do not amount to significantly more than the abstract idea itself. The claim is not patent eligible.

As a result, the claims and each claimed limitation amount to mere instructions to implement the idea on a generic computer or device, router, or smart card for example that serves to perform

generic computer functions that are well-understood, routine, and conventional activities previously known in the pertinent industry, which do not add meaningful limitations to the method. The functions performed by the "device," "memory," "RF circuitry," "biometric module," "authentication module," "transaction module," and "Internet site" appear to be conventional and routine carried out by a general purpose computers or devices such as an off the shelf computers, cellular phones, PDAs, smart cards, routers etc. with instructions to allow execution of the programmed software in-order to process a payment transaction using devices, communication means, and the sending and receiving of data. The claimed limitations as a whole do not add significantly more to the abstract idea of using computer technology, software, and data collection / data comparison, communication means, and code or logic to increase security measures of implementing rules per user account and data to reduce fraud in payment transactions.

Moreover, the claims do not appear to improve the functioning of the "device," "memory," "RF circuitry," "biometric module," "authentication module," "transaction module," "Internet site" or effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. Accordingly,

the Examiner concludes that there are no meaningful limitations in the claims that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

Applicant argues Enfish, however, the Examiner simply notes that the basis of the rejection was not based on Enfish and instead was based on the Court's Mayo / Alice two step analysis. However, the Examiner notes that in *Enfish*, the claims were "directed to a specific improvement to the way computers operate" to store and retrieve data based on a specific manner requiring a self-referential table for a computer database (see 822 F. 3d at 1366). The instant claims do not relate or come close to reciting any form of specific improvement on how computers operate by including a self-referential table to allow the computer database to execute the claimed limitations.

iv. **Paragraph 7 of the Examiner's response to Applicant's arguments in the Office Action then purports to provide a laundry list of abstract ideas that the claims are purportedly directed to. Throwing out a laundry list of potential abstract ideas such as in this Action has been seen as evidence the claims are in fact not directed to an abstract idea. In DDR Holdings, LLC, v. Hotels.com, L.P, et al., (Slip op. at page 19), the Federal Circuit recently pointed to defendants "varying formulation of the underlying abstract idea" as evidence that the claims may not in fact be directed to an abstract idea.**

D. Applicant argues DDR Holdings, however, the Examiner simply notes that the basis of the rejection was not based on DDR Holdings and instead was based on the Court's Mayo / Alice two step analysis; therefore such arguments are moot. However, in regards to the arguments to DDR holdings, the claims are summarized as being directed to a solution involving a composite web page that displays product information from third party merchants, "giving the viewer of the page the impression that she is viewing pages served by the host." The Federal Circuit explained that the claimed solution modified the routine and conventional functioning of webpages by introducing an '"outsource provider' having a web server which directs the visitor to an automatically-generated hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website" such that "rather than instantly losing visitors to the third-party's website, the host website can instead send its visitors to a website on the outsource provider's server that 1) incorporates 'look and feel' elements from the host website, and 2) provides visitors with the opportunity to purchase products from the third-party merchant without actually entering that merchant's website."

The instant claims are not found to be similar or directed to enhancing another technology of field such as the case with the DDR Holdings claim limitations.

v. **The claims in the '807 patent and the pending claims include identical features for all intents and purposes under 35 U.S.C §101. The '807 patent was allowed after the Alice case, and 101 rejections were never raised. It is respectfully submitted that if the claims of the '807 are patentable, and they are in fact patented, then so are the pending claims.**

E. Applicant's arguments directed to other applications are moot. The instant Application was examined and thus only this Application is prosecuted. Relating this Application or trying to tie this Application to other applications is not relevant since each application is prosecuted individually. Furthermore, the MPEP does not note determining whether to reject claims of an instant application must depend on whether such rejections were also given in other related applications. Therefore, the applicant's arguments tied to other applications besides this application are moot.

III. Claims 1-4, 7-23: §103 Rejection Based on Non-Statutory Subject Matter

The Appellant asserts on pages 13-15 of the Brief the following:

i. **Thus, Walker fails to disclose using biometric information to control the generation, encryption, and transmission of a key and payment information.**

A. The Examiner disagrees with Applicant's arguments that the reference to Walker does not teach the claimed limitations as outlined in the arguments. The entire reference to Walker is based on the user using a device which requires biometric input, the biometric input is then authenticated by comparing the received input to a stored biometric data. Once the biometric data is authenticated, the device generates a code which is utilized to complete a transaction. The code is transmitted or provided to the merchant for example to settle the transaction. The code includes all of the necessary information to complete the transaction. Walker also teaches using encryption means and the mere fact that the generated code does not actually contain the user's real account information or any other information that would otherwise be compromised when the user conducts a transaction, results in proving the encryption of such transaction sensitive data. Encryption has long been held as an obvious measure in order to secure the transmission of information. The code generated by Walker, if obtained by a fraudster, would not reveal any sensitive data that the fraudster may use to conduct fraudulent transactions. The entire reference's objective is to provide increased security measures through implementation of a device that requires a user's unique biometric

data, generation of information tied to the user's account that is finally utilized to settle a transaction. Overall, the reference to Walker does explicitly teach "encrypted credit card number." See Walker, at least Abstract, Figures 1-3, 8-9, 13 and all related text.

ii. Walker does not teach automatically generation of a single use credit card.

B. Examiner disagrees. First, merely automating something which is taught by a reference that teaches implementing the same thing manually does not render the claim as having patentable weight. See *In re Venner*, 120 USPQ 192 (CCPA 1958), *In re Smith*, 73 USPQ 394 (CCPA 1947). Second, the claims never recite automatically generating a key. Even if the claims did recite such language, Walker still teaches that the one time use credit card or the generated code can obviously be automatically generated. More specifically, Figure 8 recites clearly an algorithm which results in a single use credit card number being displayed without any input from the user; therefore, the process is automatic. An 'invention' is not tied to broadly provide a mechanical or automatic means to replace manual activity which has accomplished the same result.

iii. Walker in view of Homes do not disclose key encryption and payment information storage.

C. Examiner disagrees. Walker teaches "data elements stored in memory..." and that the device's memory "stores data representing a plurality of predetermined single-use financial account identifiers, data representing a

status for each of the predetermined single-use financial account identifiers, and data representing a pointer to one of the predetermined single-use financial account identifiers" including "the private key 601, the nonce 602, the initialization variable 704 and the account number 501." The Examiner merely relies on Chin to explicitly teach encrypt the key and the payment information stored in memory in order to show that encryption of such data is obvious in motivation of increasing security measures. See both Walker Col. 4, Ln. 5-12; Col. 6, Ln. 61-67; Col. 8, Ln. 9-36 and Figures 1-3, 8-9 and 10 and Chin Col. 4, Ln. 14-22, Col. 6, Ln. 1-5 and Figure 1 and related text.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/El Mehdi Oussir/

Examiner, Art Unit 3685

Conferees:

/MAMON OBEID/
Primary Examiner, Art Unit 3685

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

Requirement to pay appeal forwarding fee. In order to avoid dismissal of the instant appeal in any application or ex parte reexamination proceeding, 37 CFR 41.45 requires payment of an appeal forwarding fee within the time permitted by 37 CFR 41.45(a), unless appellant had timely paid the fee for filing a brief required by 37 CFR 41.20(b) in effect on March 18, 2013.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O/	1	6934861	B2	2005-08-23	Haala	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O/	1	20070022058	A1	2007-01-25	Labrou	
	2	20060020558	A1	2006-01-26	Bonalle	
	3	20040128249	A1	2004-07-01	Hoffman	
	4	20020112177	A1	2002-08-15	Voltmer	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/E.O/	1	ATMEL, Atmel Smart Card ICs, Silicon solutions making smart cards smarter, 12 pages.	
	2	Extended European Search Report, European Patent Application No. 10182033.0, dated 13 January 2012, 7 pages.	
	3	FANCHER, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE SPECTRUM, February 1997, 7 pages.	
	4	RAKERS, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	
	5	Japanese Office Action, Japanese Patent Application No. 2004-519130, dated 12 May 2009, 10 pages.	X
	6	ANONYMOUS, Read/write RFID offers standalone advantages, Security, August 1996; 33, 8; ProQuest, 1 page.	☐
	7	Response to Office Action filed on May 2, 2017 for US patent application no. 15/372,317.	☐
	8	US Office Action dated February 2, 2017 received in US patent application no. 15/372,317.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

	9		☐
/E.O/	10	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	☐
	11	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	☐
	12	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	☐
	13	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	☐
	14	US Notice of Allowance dated July 11, 2014 received in US patent application no. 14/022,135.	☐
	15	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	☐
	16	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	☐
	17	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	☐
	18	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	☐
	19	Appeal Brief filed February 9, 2017 for US patent application no. 14/585,057.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-661CT2

/E.O/	20	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	☐
	21	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 9, 2016 for US patent application no. 14/585,057.	☐
	22	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	☐
	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	☐
	24	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	☐
	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	☐
	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	☐
	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	☐
	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	☐
	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	☐
	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

/E.O/	31	US Office Action dated April 3, 2014 received in US patent application no. 14/028,469.	☐
	32	Response to Office Action filed on March 14, 2014 for US patent application no. 14/028,469.	☐
	33	US Office Action dated March 6, 2014 received in US patent application no. 14/028,469.	☐
	34	Response to Office Action filed on February 3, 2014 for US patent application no. 14/028,469.	☐
	35	US Office Action dated December 6, 2013 received in US patent application no. 14/028,469.	☐
	36	Appeal Brief filed January 30, 2017 for US patent application no. 14/639,034.	☐
	37	Pre-Brief Appeal Conference Decision dated July 21, 2016 and received in US patent application no. 14/639,034.	☐
	38	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on June 30, 2016 for US patent application no. 14/639,034.	☐
	39	US Office Action dated December 30, 2015 received in US patent application no. 14/639,034.	☐
	40	Response to Office Action filed on November 30, 2015 for US patent application no. 14/639,034.	☐
	41	US Office Action dated May 29, 2015 received in US patent application no. 14/639,034.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

/E.O/	42	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	☐
	43	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	☐
	44	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	☐
	45	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 7, 2016 for US patent application no. 14/724,593.	☐
	46	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	☐
	47	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	☐
	48	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	07/17/2017

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-661CT2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-03
Name/Print	Daniel K. Robertson	Registration Number	48077

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-661CT2	3012

27189 7590 08/11/2017

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/11/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
14/659,502	16 March, 2015	MARTINEZ DE VELASCO CORTINA ET AL.	116546-661CT2

		EXAMINER	
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP 525 B STREET SUITE 2200 SAN DIEGO, CA 92101		EL MEHDI OUSSIR	
		ART UNIT	PAPER
		3685	20170727

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

Please note the following correction on the cover sheet on the Examiner's anser to appeal brief (filled July 26, 2017): The cover sheet notes the appeal brief filling date as 04/18/2017. The date should instead be noted as 11/16/2016.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/MAMON OBEID/ Primary Examiner, Art Unit 3685

PTO-90C (Rev.04-03)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIALS AND APPEALS BOARD

In re application of: NEOLOGY, INC. Docket No: 116546-613CT14

Appln. No.: 14/659,502 Group Art Unit: 3685

Confirmation No.: 3012 Examiner: OUSSIR, EL MEHDI

Filed: 03-16-2015

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

REPLY BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a Reply to the Examiner's Answer filed on July 26, 2017.

ARGUMENTS

I. Claim Rejections under 35 U.S.C. §101

The Examiner's Answer states on page 5 that the claims are directed to an abstract idea of "essentially" carrying out a financial transaction between two entities. This is representative of the fundamental flaws in the Section 101 analysis provided throughout prosecution of these claims. First, Applicant is not sure what is meant by "essentially carrying . . .?" The Alice/Mayo test does not direct that one determine what the claims are "essentially" drawn to? The Alice/Mayo test requires that one consider the claims in part and in whole in order to determine whether they are directed to an abstract idea.

While the Answer claims the requisite analysis was performed in the prior Action, the proper analysis could not have been performed if the conclusion is that the claims are "essentially" directed to a financial transaction between two parties. Here is claim 1 – verbatim:

1. A mobile device, comprising:

short range radio frequency (RF) circuitry (¶¶ [0013] - [0014]);

memory (FIG. 2, ¶ [0014], line 14) configured to store biometric authentication information and payment information (¶ [0069]);

a biometric module configured to read biometric information (¶ [0067]);

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory (¶ [0073]); and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory (¶ [0053], "*Secure Identification*");

encrypt the key and the payment information stored in memory (¶ [0053], "*Secure Identification*" and "*Secure Transaction*"); and

> provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction (¶ [0053], *"Secure Transaction"* and *"Secure Data Base"*).

To determine that this claim is "essentially" carrying out a transaction between two parties after looking at each of the limitations in claim 1, alone and in combination – defies logic. In fact, as pointed out in the Appeal Brief, the prior Action admitted that the claim is directed to "a secure method of authenticating a transaction between two entities utilizing a mobile device." This is more than "essentially" carrying out a financial transaction and is well beyond what can reasonably be consider abstract when the case law is properly applied.

The truth is that certain art groups have been stretching the Alice decision and its progeny beyond all reasonable recognition in order to allege that virtually all claims presented to these art groups are directed to un-patentable subject matter. As a result, as here the rejections emanating from these groups have struggled to articulate rationales for the rejections that can be supported by the case law and leads to shifting rationales that attempt, but fail to justify such rejections based on the case law. The problem, again as here of course is that most claims submitted to these groups are in fact, when the case law is properly applied, directed to patentable subject matter. A fundamental characteristic of the improper analysis being performed is the naked application of the conclusions of various cases, without any analysis of why those conclusions are applicable. This improper analysis is repeated in this case, but the Examiner's Answer evidences a whole new level of misunderstanding of the case law, its purpose, how to apply it as well as a misunderstanding or at least misapplication of Patent Office guidance.

A first error in the application of the case law presented it the Answer is the refusal to consider pertinent case law. The Answer acknowledges that the Interim Guidance directs that when applying the two step Alice/Mayo test the Examiner is to look at examples provided by subsequent cases to determine whether the claims are or are not directed to an abstract idea, and the Last Action in fact points to certain of these cases, i.e., Classen, Cybersource, Smartgene, and buySAFE. But when Applicant pointed to other precedent

including DDR Holdings and Enfish to point out how the rejections actually fail to comport with the case law, The Answer respond by noting that the rejection was not based on these cases and that instead it is based on the Alice/Mayo two part test? Under this logic, Classen, Cybersource, Smartgene, and buySAFE, all cited in the Answer and the Last Action, would have absolutely no application in the present case, because the Examiner is applying the Alice/Mayo test and not any of these other precedents. This is clearly wrong and the Examiner does not get to simply ignore inconvenient precedent.

A second error is that the Action and the Answer fail to actually apply these subsequent precedents, i.e., Classen, Cybersource, Smartgene, and buySAFE, as directed buy the Interim Guidance. As noted above, applying these case does not comprise summing up the conclusion of the case and then applying it nakedly to the claims at issue. Yet that is precisely what the Action and the Answer do. For example, on page 8 of the Answer, the Examiner notes that simply comparing data has been found to be an abstract idea. The Answer goes on to present a laundry list of other abstract ideas that are purportedly present in the claims, and then list the above cases to support the idea that the items in the laundry list have been found to be abstract ideas. But there is absolutely no analysis of how the claims at issue in those cases are similar to the claims at issue here.

The Final Office Action alleged without analysis that the present claims were similar to those in four prior cases Classen, Cybersource, SmartGene and buySAFE. The Action applies the conclusion in those cases, i.e., simply comparing data or collecting and comparing known information or using rules to identify options are abstract, to the claims at issue here without any explanation or analysis. However, had the Action actually analyzed the claims at issue in those cases and compared them to the claims at issue in this case, the Action would have properly concluded that the claims are *not* directed to an abstract idea. The Examiner's Answer similarly lacks the requisite analysis.

The claims at issue in Cybersource are nothing like the claims at issue here. Claim 3 in Cybersource is directed to obtaining information about transactions, building a map of credit card numbers based on that information and using the map to determine whether a transaction is valid – that is it, no more. Here is claim 3:

3. A method for verifying the validity of a credit card transaction over the Internet comprising the steps of:

a) obtaining information about other transactions that have utilized an Internet address that is identified with the credit card transaction;

b) constructing a map of credit card numbers based upon the other transactions and;

c) utilizing the map of credit card numbers to determine if the credit card transaction is valid.

The court determined that this claim simply and literally was directed to obtaining and comparing data in the abstract. The court then determined that claim 2 was directed to the same abstract idea, but implemented on a computer. The court found that merely indicating that an abstract idea can be implemented on a computer was not sufficient to make it not abstract. But clearly the current claims are not merely directed to obtaining and comparing data as with claim 3 above.

The claims at issue in Classen, are directed to determining whether an immunization schedule affects the incidence or severity of a chronic immune-mediated disorder in a treatment group of mammals, relative to a control group of mammals. Without any analysis, it is hard to see how that is relevant to the claims at issue in this case? But it is informative to look at which claims in Classen were found to be directed to an abstract idea and which weren't. Below are the claims at issue:

The '283 patent claim:

A method of determining whether an immunization schedule affects the incidence or severity of a chronic immune-mediated disorder in a treatment group of mammals, relative to a control group of mammals, which comprises immunizing mammals in the treatment group of mammals with one or more doses of one or more immunogens, according to said immunization schedule, and comparing the incidence, prevalence, frequency or severity of

said chronic immune-mediated disorder or the level of a marker of such a disorder, in the treatment group, with that in the control group.

The '739 patent claim:

1. A method of immunizing a mammalian subject which comprises:

(I) screening a plurality of immunization schedules, by

(a) identifying a first group of mammals and at least a second group of mammals, said mammals being of the same species, the first group of mammals having been immunized with one or more doses of one or more infectious disease-causing organism-associated immunogens according to a first screened immunization schedule, and the second group of mammals having been immunized with one or more doses of one or more infectious disease-causing organism-associated immunogens according to a second screened immunization schedule, each group of mammals having been immunized according to a different immunization schedule, and

(b) comparing the effectiveness of said first and second screened immunization schedules in protecting against or inducing a chronic immune-mediated disorder in said first and second groups, as a result of which one of said screened immunization schedules may be identified as a lower risk screened immunization schedule and the other of said screened schedules as a higher risk screened immunization schedule with regard to the risk of developing said chronic immune mediated disorder(s),

(II) immunizing said subject according to a subject immunization schedule, according to which at least one of said infectious disease-causing organism-associated immunogens of said lower risk schedule is administered in accordance with said lower risk screened immunization schedule, which administration is associated with a lower risk of development of said chronic immune-mediated disorder(s) than when said immunogen was administered according to said higher risk screened immunization schedule.

The court found the claims of the ‘283 Patent to be patent ineligible but found that the claims of the ‘739 Patent are patent eligible and not abstract. It is not clear, because no

analysis was ever provided why the Action determined the claims in the present application are more like the claims of the '283 Patent in Classen and not more like the claims of the '739 Patent? But it is also important to note that the Patent Owner in Classen alleged that the claims of the '283 patent were infringed "when a person reviews relevant information, whether the person is a producer of vaccines, a health care provider, or a concerned parent." Clearly the claims at issue here involve much more than merely reviewing relevant information.

As with Classen, it is difficult absent any analysis to determine how the present claims are similar to those in SmartGene, which are directed to guiding the selection of a therapeutic treatment regime for a patient; however, it is important to note that Judge Taranto found that each step of claim 1 involved "well-understood, routine, conventional activity previously engaged in by researchers in the field." That is not the case here. As the Action admitted, the claims at issue here are directed to "a mobile device used in payment transaction with a point of sale terminal using security measures to increase security and operate using short range radio frequency." Thus, the claims are not directed to something that was being done before, they are directed to improved security for mobile transactions and devices configured to provide such.

Finally the BuySAFE case. Below is claim 1:

> 1. A method, comprising:
>
> receiving, by at least one computer application program running on a computer of a safe transaction service provider, a request from a first party for obtaining a transaction performance guaranty service with respect to an online commercial transaction following closing of the online commercial transaction;
>
> processing, by at least one computer application program running on the safe transaction service provider computer, the request by underwriting the first party in order to provide the transaction performance guaranty service to the first party,
>
> wherein the computer of the safe transaction service provider offers, via a computer network, the transaction performance guaranty service that

> binds a transaction performance guaranty to the online commercial transaction involving the first party to guarantee the performance of the first party following closing of the online commercial transaction.

Here the district court concluded that the patent claimed a well-known, and widely-understood concept—a third party guarantee of a sales transaction—and then applied that concept using conventional computer technology and the Internet." buySAFE, 964 F.Supp.2d at 335-36. It makes no difference, the court added, that the guarantee of the underlying transaction attaches only when that transaction closes. Id. at 336. Finally, the court explained, the claims "do not require specific programming" and are not "tied to any particular machine." Id. In these circumstances, the court ruled, the claims are outside section 101.

Again, there is no analysis provided to allow one to determine how the claims at issue here would be similar to the claims at issue in buySAFE. But the claims at issue here would require specific programming to carry out the improved security to which the claims are admittedly directed.

An actual analysis and comparison of the claims at issue in the cases cited in the Final Office Action makes clear that the claims at issue here are not comparable and are therefore not directed to an abstract idea.

The Answer actually does provide an analysis of the claims in McRO and concludes that the claims at issue here are not directed solving the same problem as in McRO. But of course the claims are also not directed to solving the same problems as the claims of Classen, Cybersource, SmartGene or buySAFE. Thus, using the logic provided with respect to McRO, one cannot conclude that the claims are directed to an abstract idea based on any of the cases cited, because the present claims are not directed to any of the problems at issue in the claims of those cases.

There simply is no analysis presented, other than nakedly citing to the conclusion of various cases and alleging those conclusions apply here, to support a prima facie case that the claims are directed to ineligible subject matter. Moreover, even a cursory analysis of the claims and the case law shows that the claims are in fact patent eligible.

A third error in the Final Action and Answer is reliance on the courts determination that whether a claim is patent eligible is a question of law and that evidence is therefore not relied on. This can be found on page 9 of the answer and it appears that the Examiner is relying on this statement to insulate his findings as being beyond argument, simply because he has determined, erroneously that the claims are directed to an abstract idea. Of course what the court means is that as a question of law, the court does not entertain evidence such as expert witnesses, inventor testimony, etc., because no facts are at issue, merely application of the law. But that does not mean that the court does not entertain attorney argument or that an Examiner's determination that a claim is directed to an abstract idea is beyond question, even where here that determination is erroneous.

A fourth error is in the application of the second prong of the Alice/Mayo test. The Action and the Answer appear to make the wrong conclusion that if each step of the claims is carried out by an off the shelf component that applicant did not invent, then the claims fail the second prong. See Page 10 of the Answer. Whether or not Applicant invented the methods claimed is an analysis to be carried out under Sections 102 and 103 of the Patent Act and have no place in the analysis of whether the claims are directed to patentable subject matter under Section 101.

Of course, if the test were that the claim limitations had to be carried out by components that could not be purchased "off the shelf" or that were themselves invented by applicant, then no inventions that are carried out on a computer or processing system could ever be patentable. But of course this is not the case. The Enfish court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." See Enfish at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. See Id. Here the claims inarguably are directed to an improvement in the device/system, e.g., by providing increased security as admitted in the Action. As in BASCOM, Amdocs as Enfish, the claimed combination provides a solution, grounded in technology that is significantly more than an abstract idea of comparing and storing information, even if the claims are implemented on what is otherwise generic

computer components. And it is not enough to claim that these precedents don't apply because the claims are being examined under Alice/Mayo and not Enfish et al.

A final error in the Answer is the erroneous conclusion that the fact that similar claims in multiple other applications by Applicant were found to be directed to patentable subject matter is somehow irrelevant? It is inarguable that Applicant is required to provide any information relevant to patentability that may arise in the prosecution of a sister case that is before another examiner. Information that is relevant to patentability includes information that tends to show the claims are not patentable as well as information that tends to show the claims are patentable. Applicant is required to provide such information precisely because it is relevant and to avoid conflicting results in prosecution. If there is no significant difference in the claims in the two cases for Section 101 purposes, then some rational should be provided as to why the claims would be patentable in one instance and not in another. As Applicant pointed out, the only real difference between the issued claim 1 in the '807 Patent and pending claim 1 is the use of the "secure module" versus the "transaction module". Thus, the Office Action essentially asserts that it was the transaction module in the '807 that made those claims directed to patentable subject matter, but replacing the transaction module with the secure module removes it from patentability. Rather than trying to ignore the findings related to the claims of the '807 Patent, the Examiner should explain why the inclusion of the Transaction Module leads to patentable claim scope, but inclusion of the secure module does not.

The claims at issue here are admittedly directed to an improvement to the device grounded in technology that provides, as admitted, improved security for a mobile transaction and the rejection under Section 101 should be reversed.

II. Claim Rejection under 35 U.S.C. §103(a)

In the Appeal Brief, Applicant very clearly pointed out that to the extent that Walker discloses a biometric interface, biometric information is used to control access to a device such as a smartcard. For example, Walker states that "the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent

Claims 1, 10 and 17 each set forth that biometric information must be successfully authenticated in order for a secure module to "generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction." Thus, Walker fails to disclose using biometric information to control the generation, encryption, and transmission of a key and payment information.

Second, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1, 10 and 17, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. According to Walker, "the cardholder first inputs his PIN or biometric data to access the device [...]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number [...]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")." (Walker, at 6:18-25, emphasis added). Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt[ing...] the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as recited in each of independent Claims 1, 10 and 17.

In response, the Answer seems to indicate that if prior art system could do something, then would be obvious to do it. But this is a misstatement of the law, and smacks of hindsight. There is no question that in the system of Walker, the single-use credit card information after querying the user, and receiving an input directing the generation of thereof. This is not the same as the claim which requires "generat[ing] a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory . . . ."

In addition, Walker describes generating a single-use credit card number, which "is distinct from the unchanging account number identifying the particular cardholder." (Walker, at 6:66-7:1). The single-use credit card number is formed by concatenating an encrypted nonce, an initialization vector, and the account number. Thus, contrary to the Examiner's rejection, Walker does not teach or suggest "provid[ing...] the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1, 10 and 17.

The Examiner concedes that the combination of Walker and Holmes does not disclose key encryption and payment information storage, and proffers that Chen discloses these features set forth in independent Claims 1, 10 and 17. (Office Action, at p. 13, Item "h", and at p. 18, Item "i"). Interestingly, the Examiner took a contradictory position on Page 7 of the Office Action mailed on May 29, 2015 for co-pending Application No. 14/639,034 where he appears to state that Holmes discloses both features, and now says the Chen was merely included to show encryption.

Nevertheless, Applicant respectfully submits that Walker, Holmes, and Chen, whether considered independently or in combination, do not teach or suggest "memory configured to store biometric authentication information and payment information; a biometric module configured to read biometric information; an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and a secure module configured to: generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory; encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1, 10 and 17.

For at least the foregoing reasons, independent Claims 1, 10 and 17 are believed to be allowable. The remaining claims depend, either directly or indirectly, on the aforementioned independent claims and are therefore believed to be allowable for the same reasons described above.

CONCLUSION

Accordingly, Appellant respectfully requests complete reversal of the Examiner's rejections to place the present application in condition for immediate allowance. Please apply any necessary charges or credits to Deposit Account 502075, referencing the above attorney docket number.

Respectfully submitted,

PROCOPIO, CORY, HARGREAVES & SAVITCH

Dated: September 26, 2017

By: /Noel C. Gillespie/
Noel C. Gillespie
Reg. No. 47,596

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900
Customer No. 27189

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie/Helen Glenister
Attorney Docket Number:	116546-613CT14

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
APPEAL FORWARDING FEE	1413	1	2000	2000
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2000**

Electronic Acknowledgement Receipt

EFS ID:	30479213
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/Helen Glenister
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-613CT14
Receipt Date:	26-SEP-2017
Filing Date:	16-MAR-2015
Time Stamp:	19:09:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2000
RAM confirmation Number	092717INTEFSW19095100
Deposit Account	502075
Authorized User	Helen Glenister
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reply Brief Filed	116546-613CT3_Reply_Brief_as_filed_09_26_2017.PDF	87874 82004881fff703c8672f067e6f2b0347c8affd98	no	13
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30298 af149dd557978db38a6f0333a8c1ab47db6b24cc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	118172		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

27189 7590 10/03/2017

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
10/03/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

Appeal No: 2017-011851
Application: 14/659,502
Appellant: Francisco Martinez de Velasco Cortina et al.

Patent Trial and Appeal Board Docketing Notice

Application 14/659,502 was received from the Technology Center at the Board on September 29, 2017 and has been assigned Appeal No: 2017-011851.

In all future communications regarding this appeal, please include both the application number and the appeal number.

The mailing address for the Board is:

PATENT TRIAL and APPEAL BOARD
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Patent Trial and Appeal Board.

BAE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

27189 7590 05/10/2019

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/10/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte FRANCISCO MARTINEZ DE VELASCO CORTINA and MANFRED RIETZLER

Appeal 2017-011851
Application 14/659,502
Technology Center 3600

Before ERIC B. CHEN, NABEEL U. KHAN, and MICHAEL M. BARRY, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants[1] appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–4 and 7–23, which constitute all pending claims (claims 5 and 6 have been cancelled). *See* Final Act. 1–2 *and* App. Br. 18–21 (Claims App'x). We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

[1] Appellants identify the Applicant, Neology, Inc. as the real party in interest. App. Br. 2.

Introduction

Appellants' disclosed embodiments and claimed invention relate generally to providing secure identification solutions. Spec. ¶ 1. Disclosed embodiments include cryptographic "credit and debit exchange keys" that provide for security of payment information and for protecting use of "personal information (e.g., biometrics) contained in [a] device." Spec. ¶ 53. A key is generated when an individual's biometric stored in the device, such as a fingerprint, is matched with the output of a biometric reader, e.g., at a point of sale. Spec. ¶¶ 65–73. Encryption using the key enables protecting both the individual's biometric information and stored payment information, such as a credit card number, for a point of sale transaction. *Id.*

Claim 1, which recites limitations for a mobile device, and claim 17, which recites analogous requirements for a method for secure transactions using a mobile device, are illustrative:

> 1. A mobile device, comprising:
>
> short range radio frequency (RF) circuitry;
>
> memory configured to store biometric authentication information and payment information;
>
> a biometric module configured to read biometric information;
>
> an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
>
> a secure module configured to:
>
> generate a key when the biometric information read by the biometric reading device is determined by the

authentication module to correspond to the biometric authentication information stored in memory;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

17. A method for secure transactions using a mobile device, comprising:

storing biometric authentication information and payment information in memory;

reading biometric information using a biometric reader;

determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

encrypting the key and the payment information stored in memory; and

providing the encrypted key and payment information for use in a transaction.

App. Br. 18, 20 (Claims App'x).[2]

[2] There is a third independent claim—claim 10—which recites a system that includes a mobile device with the same limitations as claim 1, along with a "point of sale (POS) device" configured, *inter alia*, to receive the encrypted key and payment information from the mobile device. *See* App. Br. 19–20 (Claims App'x).

Rejections[3] *and References*

All pending claims stand rejected under 35 U.S.C. § 101 as directed to an abstract idea, without reciting significantly more. Final Act. 8–12; *see also id.* at 2–6.

Claims 1–4, 8–13, 15–20, 22, and 23 stand rejected as unpatentable under 35 U.S.C. § 103 over Walker (US 6,163,771; Dec. 19, 2000), Holmes (US 6,848,048 B1; Jan. 25, 2005), and Chen (US 5,590,197; Dec. 31, 1996). Final Act. 12–20; *see also id.* at 6–7.

Claims 7, 14, and 21 stand rejected as unpatentable under 35 U.S.C. § 103 over Walker, Holmes, Chen, and Voltmer (US 2002/0112177 A1; Aug. 15, 2002). Final Act. 20.

ANALYSIS

General Law for the § 101 Rejection, and The 2019 Guidance

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. The Supreme Court, however, has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *E.g.*, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Supreme Court's two-step framework, described in *Mayo*

---

[3] The Examiner rejected all pending claims based on the doctrine of nonstatutory, obviousness-type double patenting. Final Act. 21–27. In response to Appellants' representation in the Appeal Brief that a terminal disclaimer will be filed upon the indication of allowable subject matter, the Examiner agreed to hold that rejection in abeyance. App. Br. 15–16; Ans. 3. In view of this, our decision does not address that double patenting rejection.

and *Alice*. *See Alice*, 573 U.S. at 217–18 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *Id.* at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

Concepts determined to be abstract ideas, and, thus, patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 69 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as "molding rubber products" (*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)); "tanning, dyeing, making water-proof cloth, vulcanizing India rubber, smelting ores" (*id.* at 182 n.7 (quoting *Corning v. Burden*, 56 U.S. 252, 267–68 (1853))); and manufacturing flour (*Benson*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Supreme Court held that "[a] claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula." *Diehr*, 450 U.S. at 176; *see also id.* at 191 ("We view respondents' claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula."). Having said that, the Supreme Court also indicated that a claim "seeking patent

protection for that formula in the abstract . . . is not accorded the protection of our patent laws, . . . and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment." *Id.* (citing *Benson* and *Flook*); *see also id.* at 187 ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.").

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (internal citation omitted). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

The PTO recently published revised guidance on the application of § 101. *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50–57 (Jan. 7, 2019) ("the 2019 Guidance"). According to the 2019 Guidance, we first look to whether the claim recites:

> (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activity such as a fundamental economic practice, or mental processes); and

> (2) additional elements that integrate the judicial exception into a practical application (*see* MPEP § 2106.05(a)–(c), (e)–(h)).[4]

See the 2019 Guidance at 52, 55–56. Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, does the office then look to whether the claim:

> (3) adds a specific limitation beyond the judicial exception that are not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); or
>
> (4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

See the 2019 Guidance at 56.

Our Analysis

For the § 101 rejection, Appellants argue all claims together as a group, contending, that the claims are *not* directed to an abstract idea pursuant to the *Alice/Mayo* framework. App. Br. 7–12. For our analysis, we select independent claim 17 as representative. 37 C.F.R. § 41.37(c)(1)(iv).

Alice/Mayo Step One

When we assess what the claims are directed to, we must do so at the same level of generality or abstraction expressed in the claims themselves. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1337 (Fed. Cir. 2016). Here, claim 17 recites "[a] method for secure transactions using a mobile device" by (1) "storing biometric authentication information and payment information," (2) "reading biometric information," (3) "determining whether the biometric information . . . corresponds to the [stored] biometric authentication information," (4) "generating a key when the biometric information . . . is determined to correspond to the biometric authentication

[4] All references to the MPEP are to Rev. 08.2017 (Jan. 2018).

information stored," (5) "encrypting the key and the payment information," and (6) "providing the encrypted key and payment information for use in a transaction."

Considering the steps collectively, we conclude claim 17 is directed to using biometric authentication and encryption for a secure payment transaction. This is not an abstract idea, because it is neither a mathematical concept, nor a mental process, nor a method of organizing human activity, nor a combination of those categories. *See Alice*, 573 U.S. at 216; *Mayo*, 566 U.S. at 71; *see also* the 2019 Guidance at 51–55.

Thus, the Examiner errs in determining the claims are directed to an abstract idea in step one of the *Alice/Mayo* framework. Accordingly, we do not sustain the § 101 rejection of claims 1–4 and 7–23.

A. The § 103 Rejections

In the § 103 rejection of the independent claims, the Examiner finds Walker teaches the disputed limitation of "generat[ing] a key . . . when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information," as recited. Final Act. 13, 18 (citing Walker col. 5, l. 49–col. 6, l. 38, Figs. 1–9). Appellants contend Walker does not teach the disputed limitation because Walker teaches using biometric authentication simply to allow access to the device, and any key generation is a separate process triggered when the device user subsequently requests generation of single-use credit card information. App. Br. 13–14. In other words, Appellants contend the Examiner errs because Walker does not teach generating the key *when* the biometric information is authenticated. Appellants' argument is persuasive.

The Examiner responds by finding Walker teaches that "[o]nce the biometric data is authenticated, the device generates a code which is utilized to complete a transaction." Ans. 16 (citing Walker Abstract, Figs. 1–3, 8, 9, 13, and "all related text"). The Examiner does not explain, however, nor do we discern from the record before us, how or why this finding teaches or suggests the "when" requirement of the disputed limitation.

Walker's only described purpose for biometric authentication is to access the device. *See, e.g.*, Walker Fig. 3B *and* col. 6, ll. 14–20. Walker teaches that when access is granted based on successful authentication, "the device responds by querying the cardholder on display **102** whether it should generate a single-use credit card number." Walker col. 6, ll. 20–22; *see also* col. 6, l. 60–col. 7, l. 25 (disclosing an embodiment that uses key-based encryption for generating a single-use card number). Thus, generation of a key as part of generating the single-use card number takes place only after the user provides input in response to the prompt, which in turn is only provided after the end of successful biometric authentication. Because there necessarily is a delay between the conclusion of biometric authentication and the request to generate a key, Appellants persuade us that artisans of ordinary skill would have understood that generating a key in Walker takes place *after* the biometric information is authenticated, not *when* it is authenticated (as required by the disputed limitation).

Thus, we agree with Appellants that the Examiner's findings do not establish that Walker teaches (or suggests) all requirements of the disputed limitation. Accordingly, the Examiner has not established a prima facie case of obviousness for the independent claims and, therefore, we do not sustain

the § 103 rejections of claims 1, 10, and 17, and, likewise, of their dependent claims 2–4, 7–9, 11–16, and 18–23.

DECISION

We reverse the Examiner's 35 U.S.C. § 101 rejection of claims 1–4 and 7–23.

We reverse the Examiner's 35 U.S.C. § 103 rejections of claims 1–4 and 7–23.

REVERSED

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	14659502
Filing Date	16-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Attorney Docket Number	116546-613CT14
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Neology, Inc.	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

14321781 filed on 07/01/2014

14585057 filed on 12/29/2014

14639034 filed on 03/04/2015

14724593 filed on 05/28/2015

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request. ○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ○ Small Entity ○ Micro Entity ◉ Regular Undiscounted I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 64279 ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this request	
Signature	/Mark W. Catanese/
Name	Mark W. Catanese

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT14

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14659502

Filing Date: 16-Mar-2015

Applicant/Patent under Reexamination: Martinez de Velasco Cortina

Electronic Terminal Disclaimer filed on May 14, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	36010229
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT14
Receipt Date:	14-MAY-2019
Filing Date:	16-MAR-2015
Time Stamp:	17:20:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	051519INTEFSW17204000
Deposit Account	502075
Authorized User	Helen Glenister

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	36127 bf3230d9d048514b9a1e8fe79448ccbef862e759	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30507 329dc8afbd88952ceee314b19522f33b65e928e5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	66634		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT14

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5627544	A	1997-05-06	SNODGRASS CHARLES K et al.	
	2	5819234	A	1998-10-06	SLAVIN et al.	
	3	5940006	A	1999-08-17	MACLELLAN et al.	
	4	6089284	A	2000-07-18	KAEHLER DAVID L et al.	
	5	6570488	B2	2003-05-27	Kucharczyk et al.	
	6	6934689	B1	2005-08-23	Ritter et al.	
	7	7081819	B2	2006-07-25	Martinez de Velasco Cortina et al.	
	8	7096363	B2	2006-08-22	Kon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	9	7987501	B2	2011-07-26	Miller et al.	
	10	8237568	B2	2012-08-07	Martinez de Velasco Cortina et al.	
	11	8325044	B2	2012-12-04	Martinez de Velasco Cortina et al.	
	12	8587436	B2	2013-11-19	Martinez de Velasco Cortina et al.	
	13	9558385	B2	2017-01-31	Martinez de Velasco Cortina et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020109580	A1	2002-08-15	Shreve et al.	
	2	20020112171	A1	2002-08-15	Ginter et al.	
	3	20020123325	A1	2002-09-05	Cooper	
	4	20020157029	A1	2002-10-24	French et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	5	20020193142	A1	2002-12-19	Stavenow et al.	
	6	20020194499	A1	2002-12-19	Audebert et al.	
	7	20030018522	A1	2003-01-23	Denimarck et al.	
	8	20030019929	A1	2003-01-30	Stewart et al.	
	9	20030137403	A1	2003-07-24	Carrender et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Preliminary Amendment filed on August 28, 2018 in US Patent Application no. 16/051,751. (6 pages)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	2	US Office Action dated February 4, 2019 received in US Patent Application no. 16/051,751.(17 pages)	
	3	Response to Office Action filed on April 30, 2019 in US Patent Application no. 16/051,751.(8 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2019-05-14
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT14

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	240	240
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	36011042
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT14
Receipt Date:	14-MAY-2019
Filing Date:	16-MAR-2015
Time Stamp:	17:22:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$240
RAM confirmation Number	051519INTEFSW17231600
Deposit Account	502075
Authorized User	Helen Glenister

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	IDS_NPL_16051751__Preliminary_Amendment_filed_Aug_28__2018.PDF	72881 0aa7bfe3890543057e72ef4e298c86aea130c56e	no	6
Warnings:					
Information:					
2	Non Patent Literature	IDS_NPL_16051751__Non-Final_Rejection__Mail_Date_2_4_2019.PDF	693027 bc6954b3ef37055c1b2dc3763b1dd85f20b290ec	no	17
Warnings:					
Information:					
3	Non Patent Literature	IDS_NPL_Resp_to_NFOA_dated_Feb_4__2019_in_US_16051751.PDF	102254 d8f376001acfee19109340309e78ae91bf640902	no	8
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	116546-613CT14_SUPP_IDS_SB08_Draft.PDF	612920 9a9775110651a49174a70db957b696acf3e608fd	no	6
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30650 17af27fbe7e00ab9bb52dd4d9c2870cd794fd76c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1511732		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	14659502
Filing Date	16-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Attorney Docket Number	116546-613CT14
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Neology, Inc.	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

16051751 filed on 08/01/2018

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○	I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

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

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 64279

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Mark W. Catanese/
Name	Mark W. Catanese

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT14

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14659502

Filing Date: 16-Mar-2015

Applicant/Patent under Reexamination: Martinez de Velasco Cortina

Electronic Terminal Disclaimer filed on May 15, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	36023655
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT14
Receipt Date:	15-MAY-2019
Filing Date:	16-MAR-2015
Time Stamp:	17:23:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	051619INTEFSW17234900
Deposit Account	502075
Authorized User	Helen Glenister

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	34090 bcc473536b0fd535e76c1d0d4642758d816d25a7	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30506 c0ecc3d534aeec40afff3e28413b637b97fa3e30	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64596		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

27189 7590 05/28/2019

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 05/28/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	08/28/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27189 7590 05/28/2019

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	08/28/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
OUSSIR, EL MEHDI	3685	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

27189 7590 05/28/2019

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 05/28/2019

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/659,502	Applicant(s) Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 05/10/2019.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-4 and 7-23 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

This communication is in response to the USPTO Patent Trial and Appeal Board rendered decision on 05/10/2019. The Board Decision reversing Examiner rejection under 35 U.S.C. §103.

Claims 1-4, 7-23 are pending.

Reasons for Allowance

Claims 1-4, 7-23 are allowed.

The following is an Examiner's statement of reasons for allowance:

The primary reason for allowance of claims 1-4 and 7-23 is Patent Trial and Appeal Board rendered decision on 05/10/2019 reversing examiner' rejection under 35 U.S.C. 103.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

El Mehdi Oussir

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
05/13/2019

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Examiner-Initiated Interview Summary	**Application No.** 14/659,502	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicant's representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 13 May 2019.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☑ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: NA.

Identification of prior art discussed: NA.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Examiner requested a terminal disclaimer for applications 14/585057, 14/321781, 14/639034, and 14/724593. Applicant agrees to file an electronic terminal disclaimer.

Examiner requested a terminal disclaimer for application 16/051751 on 5/15/2019. Applicant's representative agrees to file an electronic terminal disclaimer.

Notice of References Cited	Application/Control No. 14/659,502	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5590197-A	12-1996	Chen; James F.	G06Q20/04	380/30
*	B	US-6163771-A	12-2000	Walker; Jay S.	G06Q20/04	705/18
*	C	US-20020112171-A1	08-2002	Ginter, Karl L.	G06F21/10	713/185
*	D	US-20020123325-A1	09-2002	Cooper, Gerald M.	H04L63/0492	455/411
*	E	US-20020157029-A1	10-2002	French, Jennifer	G06F21/31	726/21
*	F	US-20020193142-A1	12-2002	Stavenow, Bengt	G06F21/41	455/556.1
*	G	US-20020194499-A1	12-2002	Audebert, Yves Louis Gabriel	H04L63/0853	726/35
*	H	US-20030018522-A1	01-2003	Denimarck, Paul	G06Q20/40145	705/14.23
*	I	US-6848048-B1	01-2005	Holmes; William S.	G06F21/64	713/162
*	J	US-6934689-B1	08-2005	Ritter; Rudolf	G06Q20/04	705/16
*	K	US-20060020558-A1	01-2006	Bonalle; David S.	G06Q20/341	705/64
*	L	US-20060204048-A1	09-2006	Morrison; Robert A.	G06F21/31	382/115
*	M	US-20070022058-A1	01-2007	Labrou; Yannis	G06Q20/32	705/67

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Ewa Syta, S. K. (2010). RFID-based Authentication Middleware for Mobile Devices. IEEE, 1-10. Retrieved from http://www.cs.ccsu.edu/~stan/research/pervasive/pubs/hicss2010rfidam.pdf
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/659,502	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20070198436-A1	08-2007	Weiss; Kenneth P.	G06F21/32	705/75
*	B	US-7911643-B2	03-2011	Yamada; Makoto	H04N1/33307	358/1.15
*	C	US-9858566-B2	01-2018	Mardikar; Upendra S.	G06Q20/1085	1/1
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/659,502	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	6/1/2015	EO
H04L	6/1/2015	EO
G06K9	05/13/2019	EO

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705		6/1/2015	EO

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Consulted J. Hayes D.P rejection	6/2/2015	EO
Consulted Clavin H.	6/12/2015	EO
Google search	6/4/2015	EO
East search	6/4/2015	EO
East search update	05/13/2019	EO
Consulted John H. and Neha P.	05/13/2019	EO
Interference search	05/13/2019	EO
inventor search	05/13/2019	EO
Assignee search	05/13/2019	EO
NPL search	05/13/2019	EO

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/659,502	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06Q20	G06Q20	05/13/2019	EO

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/659,502	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

CPC						
Symbol					**Type**	**Version**
G06F	/	21	/	35	F	2013-01-01
H04W	/	4	/	80	I	2018-02-01
G06F	/	21	/	34	I	2013-01-01
G06F	/	21	/	32	I	2013-01-01
G06F	/	21	/	31	I	2013-01-01
G06K	/	7	/	0008	I	2013-01-01
G06K	/	19	/	0723	I	2013-01-01
G06K	/	19	/	07758	I	2013-01-01
G06K	/	19	/	0776	I	2013-01-01
G06K	/	19	/	07764	I	2013-01-01
G06K	/	19	/	10	I	2013-01-01
G07C	/	9	/	00087	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04W	/	12	/	08	I	2013-01-01
G06K	/	7	/	10	I	2013-01-01
G06K	/	7	/	10316	I	2013-01-01
G06K	/	7	/	10366	I	2013-01-01
G06K	/	19	/	025	I	2013-01-01
G06Q	/	2220	/	00	A	2013-01-01
H04L	/	63	/	0861	A	2013-01-01
H04M	/	2203	/	6009	A	2013-01-01
H04M	/	2203	/	6054	A	2013-01-01
H04W	/	12	/	00522	A	2019-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	13 May 2019	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	14

U.S. Patent and Trademark Office — Part of Paper No.: 20190513

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/659,502	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

INTERNATIONAL CLASSIFICATION					
CLAIMED					
	/		/		

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
705	71

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	13 May 2019	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	14

U.S. Patent and Trademark Office — Part of Paper No.: 20190513

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/659,502	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	8	10	17	19										
2	2	9	11	18	20										
3	3	10	12	19	21										
4	4	11	13	20	22										
-	5	12	14	21	23										
-	6	13	15												
5	7	14	16												
6	8	15	17												
7	9	16	18												

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	13 May 2019	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685		O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	14

U.S. Patent and Trademark Office Part of Paper No.: 20190513

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S26	51	S25 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:26
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S31	4128	((generate) near2 (key pin code token	US-PGPUB;	OR	ON	2015/06/12

		password)) with ((encrypt) near3 (key pin code token password))	USPAT			16:22
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S37	63	S35 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:24
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44
S40	0	(("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/30 16:19
S42	66	("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" |	US-PGPUB; USPAT	OR	ON	2015/09/30 16:20

		"6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.				
S43	2	"20070022058"	US-PGPUB; USPAT	OR	ON	2016/04/21 15:56
S44	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 10:38
S45	0	S44 and ((biometric near4 associat$4) with (payment))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S46	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S47	24	S46 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 10:41
S48	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S49	3	S48 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S50	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S51	34	S50 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S52	21	S51 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 14:47
S53	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2017/05/24 11:05
S54	1	S53 and (encrypt$4 with key with payment)	US-PGPUB; USPAT	OR	ON	2017/05/24 11:06
S55	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2017/05/25 10:48
S56	0	S55 and (RF near3 device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S57	1	S55 and (RF with device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S58	0	(2014/0040628).CCLS.	US-PGPUB; USPAT	OR	OFF	2017/05/25 16:15
S59	0	(2014/0040628).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:15
S60	3	("20140040628").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:16

S61	0	("("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2017/07/19 11:59
S62	22	("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/07/19 11:59
S63	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	OFF	2019/02/15 16:19
S64	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S65	7	S64 and (prompt$4 ask$4 requir$4)	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S66	7	S64 and ((prompt$4 ask$4 requir$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S67	5	S64 and ((prompt$4 ask$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S68	3	S64 and ((prompt$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S69	82023	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:25
S70	108452	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 19:25
S71	2980	S70 and ((prompt$4) with (user customer) with (biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:26
S72	2518	S71 and ((mobile electronic) near3 (device phone pda))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S73	18	S72 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S74	68297	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:36
S75	76623	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:36
S76	2479	S75 and ((prompt$4) with (user customer) with (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:38
S77	13	S76 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:39

S78	2422	S75 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S79	1910	S76 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S80	11	S79 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:42
S81	5053	(prompt$4 dialog$3 form window popup pop$up) with (range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:22
S82	326	S81 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:23
S83	730	S81 same (biometric pin code iris fingerprint authenticat$4 password passcode)	US-PGPUB; USPAT	OR	ON	2019/02/15 20:24
S84	30	S83 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:24
S85	8880	(prompt$4 dialog$3 form window popup pop$up) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:26
S86	92	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:29
S87	154	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location connect$4 area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:32
S88	0	(2002/0157029).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41
S89	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41
S90	1	("20020194499").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:54
S91	24	("1239630").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:13
S92	5	("0797,359").PN.	US-PGPUB;	OR	OFF	2019/02/15

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			21:14
S93	2	("20020123325").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:15
S94	0	(2002/0112171).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:57
S95	1	("20020112171").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:58
S96	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 15:00
S97	1	("6934689").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 17:11
S98	3	(contactless near2 (payment transaction) and biometric) and @ay<"2003"	US-PGPUB; USPAT	OR	OFF	2019/02/21 17:21
S99	1	("8766772").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/26 13:14
S100	360414	(generat$3 near3 (code OTP PIN (random near2 number)))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:38
S101	0	S100 and (generat$3 with (response and "to"))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:39
S102	2624	S100 and (generat$3 with (authenticat$3) with (biometric finger print iris))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:39
S103	0	S102 and (authomatic$5 near4 generat$4)	US-PGPUB; USPAT	OR	ON	2019/05/09 17:40
S104	168	S102 and ((authomatic automatically) near5 (generate generating))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:40
S105	57	S104 and @pd<"20120709"	US-PGPUB; USPAT	OR	ON	2019/05/09 17:41
S106	18	S105 AND ((G06Q20/3676 OR G06Q20/3821 OR G06Q20/385 OR G06Q20/40 OR G06Q20/40145 OR G06Q30/06 OR G06Q40/02 OR G06Q50/22 OR G06Q20/401 OR G06Q20/102 OR G06Q20/3674 OR G06Q20/382 OR G06Q10/06 OR G06Q10/10 OR G06Q20/20 OR G06Q20/206 OR G06Q20/3672 OR G06Q20/4012 OR G06Q30/02 OR G06Q10/103 OR G06Q20/341 OR G06Q20/347 OR G06Q20/367 OR G06Q40/04 OR G06Q50/24).CPC.)	US-PGPUB; USPAT	OR	ON	2019/05/09 17:41
S107	1	("20040034784").PN.	US-PGPUB;	OR	OFF	2019/05/10

			USPAT; USOCR			14:15
S108	1	("20060204048").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/10 14:16
S109	8	("0000002" | "0000004" | "20020035690" | "20080141032" | "20100313026" | "20130166912" | "20140068268" | "20140075192").PN.	US-PGPUB; USPAT	OR	ON	2019/05/10 16:49
S113	1	("20070198436").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/13 15:41
S114	95	((("Neology") near3 ("Inc"))).AS,AANM.	USPAT	OR	ON	2019/05/13 15:50
S115	7	S114 and (RF with circuitry)	USPAT	OR	ON	2019/05/13 15:51
S116	1	S115 and (biometric)	USPAT	OR	ON	2019/05/13 15:51
S117	34	S114 and (biometric)	USPAT	OR	ON	2019/05/13 15:51
S118	3	S117 and (generate near2 key)	USPAT	OR	ON	2019/05/13 15:51
S119	30	((("Martinez") near3 ("de") near3 ("Velasco") near3 ("Cortina") near3 ("Francisco"))).INV.	USPAT	OR	ON	2019/05/13 15:52
S120	185	((("MARTINEZ") near3 ("DE") near3 ("VELASCO") near3 ("CORTINA") near3 ("Francisco")) OR (("RIETZLER") near3 ("Manfred"))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2019/05/13 15:52
S121	19	S120 and (biometric)	USPAT	OR	ON	2019/05/13 15:52
S122	1	("9858566").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/13 16:23

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S123	826132	(mobile near2 device)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:54
S124	11100	S123 and (short near2 range near2 radio)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:54
S125	15	S124 and (store near2 biometric near2 information)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55
S126	83	S124 and (stor$3 near4 biometric near4 information)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55
S127	27	S126 and (generat$4 with key with biometric)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55

5/ 13/ 2019 4:54:18 PM
C:\ Users\ eoussir\ Documents\ EAST\ Workspaces\ 14639034_Mobile device RFID transaction biometric POS.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT14

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5627544	A	1997-05-06	SNODGRASS CHARLES K et al.	
	2	5819234	A	1998-10-06	SLAVIN et al.	
	3	5940006	A	1999-08-17	MACLELLAN et al.	
	4	6089284	A	2000-07-18	KAEHLER DAVID L et al.	
	5	6570488	B2	2003-05-27	Kucharczyk et al.	
	6	6934689	B1	2005-08-23	Ritter et al.	
	7	7081819	B2	2006-07-25	Martinez de Velasco Cortina et al.	
	8	7096363	B2	2006-08-22	Kon et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	9	7987501	B2	2011-07-26	Miller et al.	
	10	8237568	B2	2012-08-07	Martinez de Velasco Cortina et al.	
	11	8325044	B2	2012-12-04	Martinez de Velasco Cortina et al.	
	12	8587436	B2	2013-11-19	Martinez de Velasco Cortina et al.	
	13	9558385	B2	2017-01-31	Martinez de Velasco Cortina et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020109580	A1	2002-08-15	Shreve et al.	
	2	20020112171	A1	2002-08-15	Ginter et al.	
	3	20020123325	A1	2002-09-05	Cooper	
	4	20020157029	A1	2002-10-24	French et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	5	20020193142	A1	2002-12-19	Stavenow et al.	
	6	20020194499	A1	2002-12-19	Audebert et al.	
	7	20030018522	A1	2003-01-23	Denimarck et al.	
	8	20030019929	A1	2003-01-30	Stewart et al.	
	9	20030137403	A1	2003-07-24	Carrender et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Preliminary Amendment filed on August 28, 2018 in US Patent Application no. 16/051,751. (6 pages)	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14659502
	Filing Date	2015-03-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT14

	2	US Office Action dated February 4, 2019 received in US Patent Application no. 16/051,751.(17 pages)	
	3	Response to Office Action filed on April 30, 2019 in US Patent Application no. 16/051,751.(8 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	05/15/2019

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14659502
Filing Date	2015-03-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT14

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2019-05-14
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

7590 09/13/2019

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	
NOTIFICATION DATE	DELIVERY MODE
09/13/2019	ELECTRONIC

Notice of Abandonment

This application is abandoned in view of:

1. ☐ The applicant's failure to timely file a proper reply to the Office letter mailed on _____.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the expiration of the period for reply (including a total extension of ____ month(s)) which expired on _____.
   (b) ☐ No reply has been received.
2. ☒ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____.
   The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☒ The issue fee and publication fee, if applicable, has not been received.
3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawing have been received.
4. ☐ Applicant's failure to timely file the inventor's oath or declaration no later than the date on which the issue fee was paid as required by the Notice Requiring Inventor's Oath or Declaration (PTO-2306).
   (a) ☐ An inventor's oath or declaration was received on _____ (with a Certificate of Mailing or Transmission date _____), which is after the date on which the issue fee was paid.
   (b) ☐ While an oath or declaration (or substitute statement) for one or more inventors was received, an oath or declaration (or substitute statement) for at least one other inventor has not been received.
   (c) ☐ No inventor's oath or declaration has been received.
5. ☐ Drawings received on _____ were disapproved by examiner. See examiner's response dated _____.
6. ☐ Corrected drawings were received on _____ , which is after the expiration of the one-month period for reply set in examiner's response dated _____.
7. ☐ No corrected drawings have been received in reply to one-month period set in examiner's response dated _____.
8. ☐ The reason(s) below:

Petitions to revive under 37 CFR 1.137(a) or request to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

Brian Dyke for

(571)-272-4200 or 1(888)-786-0101
Patent Publication Branch
Office of Data Management

FORM PTO-ABN0 (Rev. 03/17)

Doc Code: PET.OP
Document Description: Petition for Review by the Office of Petitions

PTO/SB/64 (01-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(a)

Page 1 of 2

Docket Number (Optional)
116546-613CT14

First named inventor: Francisco Martinez de Velasco Cortina

Application No.: 14/659,502 Art Unit: 3685

Filed: 03-16-2015 Examiner: OUSSIR, El Mehdi

Title: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Attention: Office of Petitions
Mail Stop Petition
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX (571) 273-8300

NOTE: If information or assistance is needed in completing this form, please contact the Office of Petitions at (571) 272-3282.

The above-identified application became abandoned for failure to file a timely and proper reply to a notice or action by the United States Patent and Trademark Office. The date of abandonment is the day after the expiration date of the period set for reply in the Office notice or action plus any extensions of time actually obtained.

APPLICANT HEREBY PETITIONS FOR REVIVAL OF THIS APPLICATION.

NOTE: A grantable petition requires the following items:

(1) Petition fee;
(2) Reply and/or issue fee;
(3) Terminal disclaimer with disclaimer fee – required for all utility and plant applications filed before June 8, 1995, and for all design applications; and
(4) Statement that the entire delay was unintentional.

1. **Petition fee**

☐ Small entity fee $ _____ (37 CFR 1.17(m)). Applicant asserts small entity status. See 37 CFR 1.27.

☐ Micro entity fee $ _____ (37 CFR 1.17(m)). Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☒ Undiscounted fee $ 2000.00 (37 CFR 1.17(m)).

2. **Reply and/or fee**

A The reply and/or fee to the above-noted Office notice or action in the form of

_____ (identify the type of reply):

☐ has been filed previously on _____.

☐ is enclosed herewith.

B The issue fee and publication fee (if applicable) of $ 1000.00

☐ has been paid previously on _____.

☒ is enclosed herewith.

This collection of information is required by 37 CFR 1.137(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 1 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PET.OP
Document Description: Petition for Review by the Office of Petitions

PTO/SB/64 (01-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 CFR 1.137(a)

3. **Terminal disclaimer with disclaimer fee**

☒ Since this utility/plant application was filed on or after June 8, 1995, no terminal disclaimer is required.

☐ A terminal disclaimer (and disclaimer fee (37 CFR 1.20(d)) of $ _____) disclaiming the required period of time is enclosed herewith (see PTO/SB/63).

4. **STATEMENT:** The entire delay in filing the required reply from the due date for the required reply until the filing of a grantable petition under 37 CFR 1.137(a) was unintentional. [NOTE: The United States Patent and Trademark Office may require additional information if there is a question as to whether either the abandonment or the delay in filing a petition under 37 CFR 1.137(a) was unintentional (MPEP 711.03(c), subsections (III)(C) and (D)).]

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

/Mark W. Catanese/	September 20, 2019
Signature	Date
Mark W. Catanese	64,279
Typed or Printed Name	Registration Number, if applicable
C/o Procopio, Cory, Hargreaves & Savitch LLP	(619) 238-1900
Address	Telephone Number
525 B Street, #2200, San Diego, CA 92101	
Address	

Enclosures:

☒ Fee Payment

☒ Reply

☐ Terminal Disclaimer Form

☐ Additional sheet(s) containing statements establishing unintentional delay

☐ Other: _____

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ Deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Petition, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450.

☐ Transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (571) 273-8300.

_____	_____
Date	Signature
	_____
	Typed or printed name of person signing certificate

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14659502
Filing Date:	16-Mar-2015
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT14

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PET. REVIVE ABANDON APP, DELAY PYMT-RESP	1453	1	2000	2000
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
UTILITY APPL ISSUE FEE	1501	1	1000	1000
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**3000**

Electronic Acknowledgement Receipt

EFS ID:	37226057
Application Number:	14659502
International Application Number:	
Confirmation Number:	3012
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT14
Receipt Date:	20-SEP-2019
Filing Date:	16-MAR-2015
Time Stamp:	14:17:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$3000
RAM confirmation Number	E20199JE18295351
Deposit Account	502075
Authorized User	Helen Glenister

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	116546-613CT14_Issue_Fee_Transmittal_09_20_2019.PDF	108483 4203f85e66a6f4f98af234a83032e4803bc6dec4	no	1
Warnings:					
Information:					
2	Petition for review by the Office of Petitions	116546-613CT14_Petition_to_revive_IF_.PDF	225568 239b7050dd5c0c3ae679df490d978c79b7c0f7d4	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32125 180231a500b3e26e9186ab65e44548f421468fd2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	366176		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27189 7590 05/28/2019
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	08/28/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
OUSSIR, EL MEHDI	3685	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Procopio, Cory,
2 Hargreaves & Savitch LLP
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: NEOLOGY, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): San Diego, California

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ☒ Corporation or other private group entity ❑ Government

4a. Fees submitted: ☒ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 50-2075

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Mark W. Catanese/ Date September 20, 2019

Typed or printed name Mark W. Catanese Registration No. 64,279

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	03/16/2015	Francisco Martinez de Velasco Cortina	116546-613CT14	3012

27189 7590 07/29/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/29/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTONotifications@procopio.com
docketing@procopio.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Application of	:	
Martinez de Velasco Cortina et al.	:	
Application No. 14/659,502	:	
Filed: 16 Mar 2015	:	DECISION ON PETITION
For: SYSTEM AND METHOD FOR	:	
PROVIDING SECURE	:	
TRANSACTIONAL SOLUTIONS	:	

This is a decision on the petition under the unintentional provisions of 37 CFR 1.137(a), filed 09/20/2019, to revive the above-identified application.

The petition is **GRANTED**.

This application became abandoned for failure to timely pay the issue and publication fees on or before 08/28/2019, as required by the Notice of Allowance and Fee(s) Due and the Notice of Allowability, mailed 05/28/2019. Accordingly, the date of abandonment of this application is 08/29/2019.

The petition satisfies the requirements of 37 CFR 1.137(a) in that petitioner has supplied (1) the reply in the form of payment of the issue fee and the publication fee of $1000, (2) the petition fee of $2000; and (3) a proper statement of unintentional delay.

This application is being referred to the Office of Data Management for processing into a patent.

Telephone inquiries concerning this decision should be directed to Schene Gray at (571) 272-2581 or in her absence, the undersigned at (571)272-6692.

/Christopher Bottorff/

Christopher Bottorff
Petitions Examiner
Office of Petitions

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/659,502	09/01/2020	10762187	116546-613CT14	3012

27189 7590 08/12/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 533 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Francisco Martinez de Velasco Cortina, La Jolla, CA;
Neology, Inc., Poway, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Midland Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
7:26-cv-00075	3/4/2026	Western District of Texas, Midland Division

PLAINTIFF	DEFENDANT
MOBILITY IP HOLDINGS, INC.	APPLE INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,151,345	4/3/2012	
2	8,548,924	10/1/2013	
3	8,766,772	7/1/2014	
4	8,933,807	1/13/2015	
5	10,235,513	3/19/2019	
6	10,706,412	7/7/2020	
7	10,762,187	9/1/2020	

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:26-cv-00157	2/27/2026	Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
MOBILITY IP HOLDINGS, INC.	SAMSUNG ELECTRONICS CO. LTD. SAMSUNG ELECTRONICS AMERICA, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,151,345	4/3/2012	
2	8,548,924	10/1/2013	
3	8,766,772	7/1/2014	
4	8,933,807	1/13/2015	
5	10,235,513	3/19/2019	
6	10,706,412	7/7/2020	
7	10,762,187	9/1/2020	

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**