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.
14/028,469	01/13/2015	8933807	116546-6601UT	3712

27189 7590 12/23/2014

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 0 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;
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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27189 7590 12/03/2014

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

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	$960	$0	$0	$960	03/03/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRIEU, VAN THANH	2685	340-572400

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Procopio, Cory, Hargreaves & Savitch LLP
2
3 Noel C. Gillespie

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: NEOLOGY, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): POWAY, CA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 502075 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: 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 /Noel C. Gillespie/ Date December 4, 2014

Typed or printed name Noel C. Gillespie Registration No. 47596

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	14028469
Filing Date:	16-Sep-2013
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:	116546-6601UT

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**960**

Electronic Acknowledgement Receipt	
EFS ID:	20873084
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	116546-6601UT
Receipt Date:	04-DEC-2014
Filing Date:	16-SEP-2013
Time Stamp:	21:34:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$960
RAM confirmation Number	6741
Deposit Account	502075
Authorized User	GILLESPIE, NOEL C.
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	Issue Fee Payment (PTO-85B)	116546_6601UT_Issue_Fee_Payment.PDF	184114 854436691dc6115ab0e1d981e0889c329bab1daa	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30300 dbbe79e81e67bdb32826f5d66b9ba6cf1c035742	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	214414		

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 12/03/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
TRIEU, VAN THANH

ART UNIT	PAPER NUMBER
2685	

DATE MAILED: 12/03/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

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	$960	$0	$0	$960	03/03/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27189 7590 12/03/2014

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

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	$960	$0	$0	$960	03/03/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRIEU, VAN THANH	2685	340-572400

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

❑ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

❑ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: 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. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

27189 7590 12/03/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

DATE MAILED: 12/03/2014

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 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the Amendment filed on 10/31/2014*.
   ☐ 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 *1-6,8-12,14,16-22 and 24-27*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
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 _____.

DETAILED ACTION

Allowable Subject Matter

1. The following is an examiner's statement of reasons for allowance: there are no prior arts teaching or suggesting of a mobile device comprising a cellular circuitry and storing biometric authentication information that is associated with transaction information, authenticating that the biometric information input by a user corresponds to the biometric authentication information associated with the transaction information, and providing the transaction information when the user upon successful authentication of the biometric information.

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

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Beenau et al discloses the apparatus and method for using a sensor to register biometrics for use with a transponder-reader system, and more particularly, to using a sensor to register biometrics for biometric security. [US 8,548,927]

3. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 11/26/2014

Notice of References Cited	Application/Control No. 14/028,469	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner VAN TRIEU	Art Unit 2685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-8,548,927	10-2013	Beenau et al.	705/76
	B	US-			
	C	US-			
	D	US-			
	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	
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	453095	(obtain$3 or read$3 or receiv$3 or scan$4) near9 (biometric or eye or face$4 or fingerprint)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:07
L2	930	(1 or biometric or eye or face$4 or fingerprint) near5 (associat$3 or relat$3 or regard$3) near5 (financial or money$5 or transaction)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:09
L3	64738	(allow$3 or permit$4 or authentication or authoriz$3) near5 (financial or money$5 or transaction)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:11
L4	620	1 and 2 and 3	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:11
L5	204211	(3 or allow$3 or permit$4 or authentication or authoriz$3) near9 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:12
L6	157	4 and 5	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:12
L7	5641	(1 or 2) near9 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:13
L8	51	6 and 7	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:13
L9	2386	(allow$3 or permit$4 or authentication or authoriz$3) near5 (financial or money$5 or transaction) near5 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:30
L10	29	8 and 9	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:32
L11	7	(("8237518") or ("8004410") or ("7671746") or ("7081819") or ("6850147") or ("6175922") or ("7980378")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:37
L12	0	11 and 10	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:41

L13	0	11 and 8	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:41
L14	2	11 and 9	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/06 09:41

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L15	355947	(obtain$3 or read$3 or receiv$3 or scan$4) near9 (biometric or eye or face$4 or fingerprint)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:48
L16	944	(15 or biometric or eye or face$4 or fingerprint) near5 (associat$3 or relat$3 or regard$3) near5 (financial or money$5 or transaction)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:48
L17	65971	(allow$3 or permit$4 or authentication or authoriz$3) near5 (financial or money$5 or transaction)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:49
L18	628	15 and 16 and 17	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:49
L19	203296	(17 or allow$3 or permit$4 or authentication or authoriz$3) near9 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:49
L20	2415	(allow$3 or permit$4 or authentication or authoriz$3) near5 (financial or money$5 or transaction) near5 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:49
L21	34	18 and 19 and 20	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:49
L23	5624	(15 or 16) near9 (handheld or mobile or PDA or portable)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:50
L24	29	21 and 23	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/06 09:50

11/6/2014 9:51:58 AM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace (Flat Panel).wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	("8548927").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 16:49
L2	1	1 and (authority or authoriz$4 or allow$4 or permit$4) with (biometric or facial or eye$3 or fingerprint)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 16:51
L3	1	2 and party	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 16:51
L4	0	2 and party near9 ("no" or none or without)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 16:56
L5	1	1 and party near9 (eliminat$3 or "no" or none or without or bypass$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 16:58
L6	4515	transaction near9 (authentication or authoriz$5) near9 (biometr$4 or facial$2 or fingerprint or eye$4 or security)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:11
L7	19933	(handheld or mobile or cellular or fob or PDA or portable or RFID) near9 (PBK or transaction)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:12
L8	53886	(handheld or mobile or cellular or fob or PDA or portable or RFID) near9 (authority or authoriz$5 or authentication)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:12
L9	1328	6 and 7 and 8	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:20
L10	215	9 and party near9 (eliminat$3 or "no" or none or without or bypass$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:20
L11	8	6 with party near9 (eliminat$3 or "no" or none or without or bypass$3)	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:20
L12	7	10 and 11	US-PGPUB; USPAT; USOCR	OR	OFF	2014/11/25 17:21

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L13	4589	transaction near9 (authentication or authoriz$5) near9 (biometr$4 or facial$2 or fingerprint or eye$4 or security)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:21
L14	20178	(handheld or mobile or cellular or fob or PDA or portable or RFID) near9 (PBK or transaction)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:21
L15	54305	(handheld or mobile or cellular or fob or PDA or portable or RFID) near9 (authority or authoriz$5 or authentication)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:21
L16	682	13 and party near9 (eliminat$3 or "no" or none or without or bypass$3)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:22
L18	9	13 with party near9 (eliminat$3 or "no" or none or without or bypass$3)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:22
L19	219	14 and 15 and 16	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:23
L20	8	18 and 19	US-PGPUB; USPAT; UPAD	OR	OFF	2014/11/25 17:23

11/25/2014 5:24:00 PM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace (Flat Panel).wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent under Reexamination	
	14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner	Art Unit	
	VAN TRIEU	2685	

ISSUE CLASSIFICATION

ORIGINAL			CROSS REFERENCE(S)						
CLASS	SUBCLASS	CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						
340	572.4	340	572.1	539.11					
INTERNATIONAL CLASSIFICATION									
G 0 8 B	13/14								
	/								
	/								
	/								
	/								

(Assistant Examiner) (Date)	/Van T. Trieu/ 11/26/2014 (Primary Examiner) (Date)	Total Claims Allowed: 23	
(Legal Instruments Examiner) (Date)		O.G. Print Claim(s): 1	O.G. Print Fig.: 13

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		31		61		91		121		151		181
2	2		32		62		92		122		152		182
3	3		33		63		93		123		153		183
4	4		34		64		94		124		154		184
5	5		35		65		95		125		155		185
6	6		36		66		96		126		156		186
	7		37		67		97		127		157		187
7	8		38		68		98		128		158		188
9	9		39		69		99		129		159		189
10	10		40		70		100		130		160		190
11	11		41		71		101		131		161		191
12	12		42		72		102		132		162		192
	13		43		73		103		133		163		193
13	14		44		74		104		134		164		194
	15		45		75		105		135		165		195
14	16		46		76		106		136		166		196
16	17		47		77		107		137		167		197
17	18		48		78		108		138		168		198
20	19		49		79		109		139		169		199
21	20		50		80		110		140		170		200
18	21		51		81		111		141		171		201
19	22		52		82		112		142		172		202
	23		53		83		113		143		173		203
22	24		54		84		114		144		174		204
8	25		55		85		115		145		175		205
15	26		56		86		116		146		176		206
23	27		57		87		117		147		177		207
	28		58		88		118		148		178		208
	29		59		89		119		149		179		209
	30		60		90		120		150		180		210

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14028469	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
340	539.1, 539.11, 539.13, 568.1, 568.7, 572.1, 572.4, 572.7, 5.52, 5.53, 5.8, 5.82, 5.83, 5.86	12/2/13	vt
235	379, 380, 381	12/2/13	vt
455	419	12/2/13	vt
713	175, 176, 186, 189	12/2/13	vt
705	35, 44, 64	3/29/14	vt

SEARCH NOTES		
Search Notes	Date	Examiner
Update Search	2/27/14	vt
Update Search	7/1/14	vt
Update Search	11/06/14	vt
Update Search	11/25/14	vt

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
340	539.11, 572.1, 572.4	11/25/14	vt

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	8/8/14	11/26/14							
1	1	/	=							
2	2	/	=							
3	3	/	=							
4	4	/	=							
5	5	/	=							
6	6	/	=							
	7	/	-							
7	8	/	=							
9	9	/	=							
10	10	/	=							
11	11	/	=							
12	12	/	=							
	13	/	-							
13	14	/	=							
	15	/	-							
14	16	/	=							
16	17	/	=							
17	18	/	=							
20	19	/	=							
21	20	/	=							
18	21	/	=							
19	22	/	=							
	23	/	-							
22	24	/	=							
8	25	/	=							
15	26	/	=							
23	27	/	=							
	28									
	29									
	30									
	31									
	32									
	33									
	34									
	35									
	36									
	37									
	38									
	39									
	40									
	41									
	42									
	43									
	44									
	45									
	46									
	47									
	48									
	49									
	50									

Claim		Date								
Final	Original									
	51									
	52									
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/13	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

EXAMINER	
Van Thanh TRIEU	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
October 31, 2014	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

SUPPLEMENTAL RESPONSE TO NON-FINAL OFFICE ACTION

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

Commissioner:

This is a Supplemental Response to the NON-Final Office Action dated August 8, 2014, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Response, where:

AMENDMENTS TO THE CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 6 of this paper.

Document Number: 2040298

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

[[a]] memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in [[the]] memory; 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.

2. (Original) The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. (Previously Presented) The mobile device of claim 1, wherein the transaction information is generated based at least in part on credit card information.

4. (Previously Presented) The mobile device of claim 1, wherein the transaction information is generated based at least in part on rewards card information.

5. (Original) The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. (Original) The mobile device of claim 5, wherein the security block is a cryptographic block.

7. (Cancelled)

8. (Previously Presented) The mobile device of claim 1, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

9. (Currently Amended) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

[[a]] memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in [[the]] memory;

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 by the authentication module as being associated with the transaction information by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. (Original) The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. (Previously Presented) The mobile device of claim 9, wherein the transaction information is generated based at least in part on credit card information.

12. (Previously Presented) The mobile device of claim 9, wherein the transaction information is generated based at least in part on rewards card information.

13. (Cancelled)

14. (Original) The mobile device of claim 9, wherein the security block is a cryptographic block.

15. (Cancelled)

16. (Previously Presented) The mobile device of claim [[15]] 9, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

17. (Currently Amended) A cellular telephone, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

[[a]] memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in [[the]] memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module.

18. (Previously presented) The cellular telephone of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. (Previously Presented) The cellular telephone of claim 17, wherein the transaction information is generated based at least in part on credit card information.

20. (Previously Presented) The cellular telephone of claim 17, wherein the transaction information is generated based at least in part on rewards card information.

21. (Previously presented) The cellular telephone of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. (Previously presented) The cellular telephone of claim 21, wherein the security block is a cryptographic block.

23. (Cancelled)

24. (Previously Presented) The cellular telephone of claim 17, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

25. (Currently Amended) The mobile device of claim 1, wherein the transaction module configured to provide [[only]] the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

26. (Currently Amended) The mobile device of claim 9, wherein the transaction module configured to provide [[only]] the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

27. (Currently Amended) The cellular phone of claim 17, wherein the transaction module configured to provide [[only]] the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

REMARKS

Status of the Application

Claims 1-6, 8-12, 14, 16-22, and 24-27 were pending in the application. Claims 1, 9, and 17 are the independent claims. Claims 25-27 have been amended to clarify the subject matter regarded as the invention. Accordingly, Claims 1-6, 8-12, 14, 16-22, and 24-27 are now pending in the application.

Claim Rejections

Claims 1-3, 5-11, 13-19, and 21-24 — 35 U.S.C. § 103(a)

The Examiner has rejected Claims 1-3, 5-11, 13-19, and 21-24 under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,850,147 to Prokoski et al. ("Prokoski") in view of U.S. Patent No. 6,175,922 to Wang ("Wang"). The remaining claims stand rejected under 35 U.S.C. § 103(a) based on Prokoski and Wang as combined with U.S. Patent No. 7,980,378 to Jones et al. ("Jones"). Applicant respectfully traverses the rejections.

The present amendments to independent Claims 1, 9, and 17 further distinguishes the claims over Prokoski and Wang. Both Prokoski and Wang are directed to systems that provide some form of "digital signature" (e.g., biometric code) to a third party system, which then uses the digital signature to authenticate that the user is associated with certain transaction information. In contrast, independent Claims 1, 9, and 17 each recite storing in memory biometric authentication information that is associated with transaction information, authenticating that the biometric information input by a user corresponds to the biometric authentication information associated with the transaction information, and providing the transaction information when the user upon successful authentication of the biometric information as required by claim. As such, independent Claims 1, 9, and 17 are believed to be allowable. The remaining claims depend, either directly or indirectly, from one of the aforementioned independent claims and are therefore believed to be allowable for the same reasons.

Additionally, as amended, Claims 25-27 each recite that "the transaction module configured to provide the transaction information ***but not the biometric information*** via the short range RF circuitry for use in the transaction" (***emphasis added***). These amendments clarify that since authentication may be completed on the device, the device would need to transmit only the transaction information to complete the transaction once the biometric information provided by

the user is determined to match the biometric authentication information associated with the transaction information. Notably, the biometric information provided by the user is ***not*** transmitted along with the transaction information, whereas both Prokoski and Wang require transmission of some form of personal identification information such as biometric data. Accordingly, since neither Prokoski nor Wang, whether considered independently or in combination, disclose or suggest all of the claimed features, Applicant respectfully submits that Claims 25-27 are patentable at least by virtue of their respective dependencies to independent Claims 1, 9, and 17, as well as for the recitations of their additional features.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-6, 8-12, 14, 16-22, and 24-27 is respectfully requested. If the Examiner believes that a telephone conversation may be useful in advancing prosecution, the Examiner is invited to contact the undersigned at the number listed below.

If necessary, applicant requests to extend the period for filing this reply pursuant to 37 C.F.R. 1.136(a) and authorizes the Director to charge any additional fee(s) or any underpayment of fee(s) or credit any overpayment(s) to Procopio Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: October 31, 2014

/ Li Zhang /
Li Zhang
Reg. No. 70902

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

Electronic Acknowledgement Receipt

EFS ID:	20580986
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	116546-6601UT
Receipt Date:	31-OCT-2014
Filing Date:	16-SEP-2013
Time Stamp:	18:11:43
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		116546_6601UT_Supplemental_Response_to_NFOA_08814.pdf	129256 ebd71e96706e8d46c4ef93b462af58607089d722	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	8
Warnings:			
Information:			
	Total Files Size (in bytes):	129256	

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

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

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

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

PTO/SB/06 (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 14/028,469	Filing Date 09/16/2013	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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	10/31/2014	(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))	* 23	Minus	** 24	= 0	X $80 =	0
	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	**0**

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
/TAMMY L. ACREE/

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/13	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

EXAMINER	
Van Thanh TRIEU	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
October 14, 2014	EFS WEB

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

Commissioner:

In response to the NON-Final Office Action dated August 8, 2014, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Response, where:

AMENDMENTS TO THE CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 6 of this paper.

Document Number: 2040298

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently amended) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

a memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in the memory; 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.

2. (Original) The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. (Currently amended) The mobile device of claim 1, wherein the transaction information is generated based at least in part on credit card ~~transaction~~ information.

4. (Currently amended) The mobile device of claim 1, wherein the transaction information is generated based at least in part on rewards card ~~awards~~ information.

5. (Original) The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. (Original) The mobile device of claim 5, wherein the security block is a cryptographic block.

7. (Cancelled)

8. (Currently amended) The mobile device of claim [[7]] 1, wherein the short range RF circuitry includes [[device is]] a radio frequency identification (RFID) device.

9. (Currently amended) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

a memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in the memory;

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 by the authentication module as being associated with the transaction information by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. (Original) The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. (Currently amended) The mobile device of claim 9, wherein the transaction information is generated based at least in part on credit card ~~transaction~~ information.

12. (Currently amended) The mobile device of claim 9, wherein the transaction information is generated based at least in part on rewards card ~~awards~~ information.

13. (Cancelled)

14. (Original) The mobile device of claim 9, wherein the security block is a cryptographic block.

15. (Cancelled)

16. (Currently amended) The mobile device of claim [[15]] 9, wherein the short range RF [[device]] circuitry includes [[is]] a radio frequency identification (RFID) device.

17. (Currently amended) A cellular telephone, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

a memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module.

18. (Previously presented) The cellular telephone of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. (Currently amended) The cellular telephone of claim 17, wherein the transaction information is generated based at least in part on credit card ~~transaction~~ information.

20. (Currently amended) The cellular telephone of claim 17, wherein the transaction information is generated based at least in part on rewards card ~~awards~~ information.

21. (Previously presented) The cellular telephone of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. (Previously presented) The cellular telephone of claim 21, wherein the security block is a cryptographic block.

23. (Cancelled)

24. (Currently amended) The cellular telephone of claim [[23]] 17, wherein the short range RF [[device]] circuitry includes [[is]] a radio frequency identification (RFID) device.

25. (New) The mobile device of claim 1, wherein the transaction module configured to provide only the transaction information via the short range RF circuitry for use in the transaction.

26. (New) The mobile device of claim 9, wherein the transaction module configured to provide only the transaction information via the short range RF circuitry for use in the transaction.

27. (New) The cellular phone of claim 17, wherein the transaction module configured to provide only the transaction information via the short range RF circuitry for use in the transaction.

REMARKS

Status of the Application

Claims 1-24 were pending in the application and stand rejected. Claims 1, 9, and 17 are the independent claims. Applicant has added claims 25-27. Claims 7, 13, 15, and 23 have been cancelled. Claims 1, 3, 4, 8, 9, 11, 12, 16, 17, 19, 20, and 24 have been amended to clarify the subject matter regarded as the invention. Accordingly, claims 1-6, 8-12, 14, 16-22, and 24-27 are now pending in the application.

Claim Rejections

Claims 1-3, 5-11, 13-19, and 21-24 — 35 U.S.C. § 103(a)

Claims 1-3, 5-11, 13-19, and 21-24 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,850,147 to Prokoski et al. ("Prokoski") in view of U.S. Patent No. 6,175,922 to Wang ("Wang"). Claims 7, 15, and 23 have been cancelled thereby rendering the rejection moot as to these claims. Applicant has essentially incorporated the limitation of these claims into the independent claims 1, 9, and 17, respectively, and will address those limitations as appropriate in the context of those independent claims. With respect to the rest of the claims, Applicant respectfully traverses this rejection.

Addressing the rejection of independent claim 1, Applicant respectfully submits that Prokoski and Wang, alone or in combination, do not disclose or suggest at least a "mobile device, comprising … a memory configured to store … ***biometric authentication information [that] has been previously associated with … transaction information***" (***emphasis added***), as recited in independent claim 1. Further, Applicant respectfully submits that Prokoski and Wang, alone or in combination, do not disclose or suggest "an authentication module configured to ***authenticate that the biometric information read by the biometric reading device is associated with the transaction information*** based at least in part on the biometric authentication information stored in the memory" (***emphasis added***), as recited in independent claim 1. Finally, neither Prokoski nor Wang disclose or suggest "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***" (***emphasis added***), as recited in independent claim 1.

Certain embodiments described and claimed in the present application are directed to a mobile device, such as a cellular telephone that includes both a biometric reading device, such as a fingerprint sensor, short range RF circuitry, such as RFID circuitry, and memory configured to store both biometric authentication information and the transaction information (e.g., credit card information) necessary to complete a pending transaction. See figures 12-14 and the accompanying description in the specification of the present application. The biometric authentication information has been previously associated with the transaction information. See specification, at para. [0062], [0068], and [0069].

As a result, the mobile device can be configured to authenticate that the user is associated with the transaction. Thus, the mobile device can be used, e.g., for a Point Of Sale (POS) transaction, wherein the transaction information is provided to the POS system via the short range RF circuitry when the biometric information read by the biometric reading device is determined to match the biometric authentication information already associated with the transaction information. See the description of figure 14 in the specification. The device can also be used to provide the transaction information over the cellular network. See specification, at para. [0062] and [0074]. Importantly, however, the biometric reading device can be used to verify that the user is authorized with respect to the transaction (e.g., use the stored transaction information to complete the pending transaction at the POS) by requiring the user to provide their biometric information so that it can be verified against biometric information stored in the device. Only when the biometric information is verified would the transaction information be released to the Internet or the POS. See specification, at para. [0067]-[0069].

In certain embodiments, the biometric authentication information stored in the device is transmitted to the POS. The user then inputs their biometric information into a biometric reading device included in the POS, and the POS verifies the identity of the user in possession of the device. See, e.g., specification, at para. [0072]-[0073]. However, in other embodiments, the biometric reading device is included in the mobile device, thus enabling the authentication process to be performed entirely on the device. See, e.g., specification, at para. [0067] and [0070]. The device can compare the biometric information input by the user with the stored biometric authentication information, which has already been associated with the transaction information. As such, verification of the user's identity allows the device to also authenticate the user's authorization with respect to the stored transaction information. Since authentication may

be completed on the device, in some instances, the device would need to transmit only the transaction information to complete the transaction once the biometric information provided by the user is determined to match the biometric authentication information associated with the transaction information.

Thus, e.g., claim 1 is directed to "A mobile device, comprising: Radio Frequency (RF) cellular circuitry; short range RF circuitry; a memory configured to store biometric authentication information and transaction information, wherein ***the biometric authentication information has been previously associated with the transaction information***; a biometric reading device configured to read biometric information; an authentication module configured to ***authenticate that the biometric information read by the biometric reading device is associated with the transaction information*** based at least in part on the biometric authentication information stored in the memory; 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 by the authentication module as being associated with the transaction information by the authentication module***" (***emphasis added***).

Contrastingly, both Prokoski and Wang are directed to systems that provide some form of "digital signature" to a third party system, which then authenticates that the user is associated with certain transaction information. For example, in Prokoski, the user selects the type of biometric sensor to be used and then generates a personal biometric code that is stored in a central repository so that is can be used by third parties for authentication. See Prokoski, at col. 9, lines 4-5 and lines 61-65; col. 11, lines 14-22. Thus, when a person is engaged in some form of transaction, a biometric sensor included in their device can be used to acquire biometric information from the user, which is then used to generate a biometric code that is transmitted to another party or third party system. The other party or third party system can then use the biometric code to authenticate the user with respect to the specific transaction.

Thus, in all embodiments of Prokoski, the biometric code is provided to a third party system. There are no embodiments where the verification or authentication of the user with respect to a pending transaction is performed on the device before transaction information is provided to, e.g., a POS system, to complete the transaction.

In the embodiments described in Wang, complex user identification data (e.g., social security number, user name, biometrics, etc.) can be stored in a portable electronic authorization device (PEAD). See Wang, col. 6, lines 42-48. However, the PEAD does not also store transaction information such as credit or rewards card information with an association to the user identification data. When the user uses the PEAD to engage in a transaction, the user is able to use the PEAD to indicate approval of a pending transaction. However, this approval merely causes the PEAD to send the stored user identification data to a third party system, and does not equate to authorizing the user with respect to the transaction. It is still incumbent upon the third party system to use the user identification data to authenticate the user with respect to the transaction. For example, the third party system must determine, based on the user identification data, whether the corresponding user is authorized to apply the transaction information in the pending transaction. This is first mentioned by Wang, at col. 5, lines 21-24; however, in all embodiments described, the user identification data is invariably sent to the third party system in order for the third party system to authenticate the user with respect to the transaction.

It should be noted that the user is not required to provide biometric information for verification, nor does the PEAD described in Wang necessarily include a biometric reading device. See Wang, at figure 2 for example. Although, as noted in the Action, in certain embodiments, the PEAD can include a, e.g., fingerprint scanner, whereby the user would approve the transaction by swiping their finger across the scanner to authenticate themselves and approve the transaction. However, obtaining this biometric information only authenticates the user with respect to the PEAD. That is, the user provides biometric information in order to verify that the user is authorized to use the device. The user is still required to indicate approval of one or more pending transactions. Wang does disclose that the provision of biometric information, e.g., swiping a finger, can also be used to indicate approval of the transaction). But such approval does not authenticate the user with respect to the transaction. Rather, as stated above, this approval merely triggers the release of user identification data to the third party system, which still must authenticate the user with respect to the transaction based on the user identification data.

Thus, neither Prokoski nor Wang, alone or in combination teach, suggest or disclose that storing in memory biometric authentication information that is associated with transaction information, authenticating that the biometric information input by a user corresponds to the

biometric authentication information associated with the transaction information, and providing the transaction information when the user upon successful authentication of the biometric information as required by claim 1. Therefore, claim 1 is patentable over the combined references.

Claims 9 and 17 include similar limitations as included in claim 1 and are patentable for similar reasons as discussed above. Claims 2, 3, 5, 6, 8, 10, 11, 14, 16, 18, 19, 21, 22, and 24 are patentable at least by virtue of their respective dependencies.

Claims 4, 12, and 20 - 35 U.S.C. § 103(a)

Claims 4, 12, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Prokoski in view of Wang in further view of U.S. Patent No. 7,980,378 to Jones et al. ("Jones"). Applicant respectfully traverses this rejection.

The combination of Prokoski and Jones does not disclose or suggest at least the above-noted features of claims 1, 9, and 17 incorporated into claims 4, 12, and 20 by virtue of their respective dependencies. As established above, Prokoski and Wang, alone or in combination, do not disclose or suggest at least these features. Jones does not cure the deficiencies of Prokoski and Wang.

The Examiner relies on Jones only to allegedly disclose the claimed features related to awards information as transaction information, as recited in the dependent claims. Without conceding the disclosure of Jones alleged by the Examiner, Applicant respectfully submits that Jones fails to disclose or suggest at least the features of a "mobile device, comprising … a memory configured to store … transaction information … and a transaction module configured to provide the transaction information … for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module," as incorporated into claims 4, 12, and 20 by virtue of their respective dependencies. Thus, Jones fails to cure the deficiencies of Prokoski and Wang.

Accordingly, since the combination of Prokoski, Wang, and Jones does not disclose or suggest all of the claimed features, Applicant respectfully submits that claims 4, 12, and 20 are patentable over the combined references.

New Claims 25-27

Applicant has added new claims 25-27 which depend from independent claims 1, 9, and 17.

Support for new claims 25-27 may be found throughout the specification and drawings, at least for example at paragraphs [0066], [0067], and [0070] of the specification. No new matter has been added.

New claims 25-27 each recite that "the transaction module [is] configured to provide ***only*** the transaction information via the short range RF circuitry for use in the transaction." Both Prokoski and Wang require transmission of some form of personal identification data in addition to the transaction information, and rely on third party systems to use the personal identification data to authenticate the user with respect to individual transactions. As discussed above, Prokoski transmits a personal biometric code while Wang transmits a selection of user identification data. Thus, neither Prokoski nor Wang, independently or in combination, disclose or suggest at least "provid[ing] only the transaction information… for use in the transaction," as recited in each of new claims 25-27.

Accordingly, since the combination of Prokoski and Wang does not disclose or suggest all of the claimed features, Applicant respectfully submits that new claims 25-27 are patentable at least by virtue of their respective dependencies as well as for the recitations of their additional features.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-6, 8-12, 14, 16-22, and 24 is respectfully requested. If the Examiner believes that a telephone conversation may be useful in advancing prosecution, the Examiner is invited to contact the undersigned at the number listed below.

If necessary, applicant requests to extend the period for filing this reply pursuant to 37 C.F.R. 1.136(a) and authorizes the Director to charge any additional fee(s) or any underpayment of fee(s) or credit any overpayment(s) to Procopio Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: October 14, 2014

/ /

Francis G. Plati, Sr.
Reg. No. 59,153

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

Electronic Acknowledgement Receipt

EFS ID:	20416132
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	116546-6601UT
Receipt Date:	14-OCT-2014
Filing Date:	16-SEP-2013
Time Stamp:	21:31:55
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		116546_6601UT_Response_to_NFOA81814.pdf	158223 2a4ba57354e1d9e7250a166e36e76a6ec8fbe3ad	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	12

Warnings:	
Information:	
Total Files Size (in bytes):	158223

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

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

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

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

PTO/SB/06 (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 14/028,469	Filing Date 09/16/2013	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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	10/14/2014	(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))	* 23	Minus	** 24	= 0	X $80 =	0
	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	0

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
/VERONICA DAY EVERETT/

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.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

27189 7590 08/18/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
08/18/2014	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

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner	Art Unit	
	VAN TRIEU	2685	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VAN TRIEU*. (3)_____.

(2) *FRANCIS G. PLATI, Reg. No. 59,153*. (4)_____.

Date of Interview: *08 August 2014*.

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: *None*.

Identification of prior art discussed: *None*.

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...)

Applicant requests to withdraw the Final Rejection filed on 07/09/2014 because there was no amendment in all claims 1-24 and a new reference of Wang was introduced into the Final Rejection. Examiner agrees and to introduce a new Non-Final Rejection.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the 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

	/Van T. Trieu/ Primary Examiner, AU 2685

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Office Action Summary	Application No. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	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 *06/13/2014*.

☐ 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) *1-24* 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) *1-24* 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 _____ 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. *8/8/2014* .

4) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1-3, 5-11, 13-19, 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Prokoski et al** [US 6,850,147] in view of **Wang** [US 6,175,922] Regarding claim 1, the claimed a mobile device, comprising Radio Frequency (RF) cellular circuitry (the user's cellular, PDA or portable device 104 embedded with a PBK 102, see Fig. 1, col. 10, lines 15-20); a memory configured to store biometric authentication information and transaction information (the user portable PBK 102

includes a memory 114 for storing biometric data, authorized information, templates and a database 114 with financial transactions data information, see Fig. 1, col. 7, lines 35-53, col. 9, lines 57-60, col. 10, lines 20-25, col. 11, lines 35-62); a biometric reading device configured to read biometric information (the biometric sensor 110, see Fig. 1); But **Prokoski et al** fails to disclose an authentication module to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory and a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module. However, **Prokoski et al** discloses that Wang presents a method and apparatus for approving a transaction request between an electronic transaction system and a portable electronic authorization device (PEAD) such as cellular phone, PDA carried by a user using an electronic service authorization token. Advantages of the invention include the ability to securely and conveniently perform transactions with a portable device. The PEAD shares some characteristics with the Personal Biometric Key (PBK) of the current invention (see col. 3, lines 62-67, col. 4, lines 1-4). The user portable PDA 104 embedded with PBK 102 serves/provides as a biometrically secure digital assistant to the user being authenticated or authorized by the remote analyzer 120, 220, 320,420, 520 for doing financial transactions, money, credit card and/or ATM transactions on the portable PDA 104 to withdraw up to $300.00 or more than $10,000.00 (see Figs. 1-6, col. 6, lines 17-37, col. 7, lines 26-59, col. 8, lines 55-61, col. 10, lines 30-41,54-67, col. 11, lines 1-22, 50-62). **Wang** discloses a

portable electronic authorization PEAD 200 such as a cellular, smartphone or PDA contained PBK, memories 504, 506, 656, 658, user authentication machine 612 to scan/read fingerprint from the fingerprint sensor, other biometrics and a logic circuitry 502 for authentic a user 160 to do credit card and/or financial transactions on the device 200 through an automated machine teller ATM 100, see Figs. 1-6, col. 5, lines 15-67, col. 6, lines 1-10, col. 9, lines 41-67, col. 10, lines 1-60, col. 11, lines 54-67, col. 12, lines 1-18). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the PEAD of Wang for the user portable cellular or PDA of Prokoski et al for preventing of losing/stolen user's identification data and for providing convenience and quickly authorization to a user operating a financial transactions without affecting the authentication functions since the both the portable cellular/PDA having similar circuitries as of the remote receiver/authentication device such as the analyzer 120, 220, memory 114, 232 in Figs. 1 and 2.

Regarding claim 2, wherein the biometric reading device is a fingerprint reading device (the fingerprint-based PBK or fingerprint scanner, see col. 8, lines 55-59, col. 13, lines 16-17).

Regarding claim 3, wherein the transaction information is credit card transaction information (the ATM and/or credit/smart card transaction, see col. 2, lines 50-61, col. 6, lines 33-39, col. 7, lines 9-14, 26-34).

Regarding claim 5, further comprising a security block configured to secure the transaction information before it is provided by the transaction module (the central authentication/repository includes encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 6, wherein the security block is a cryptographic block (the encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 7, further comprising an RF device configured to communicate the transaction information to an RF reader/writer (which reads upon the RF short range or Bluethooth for communicating ID tag or RFID tag, see col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 8, wherein the RF device is a radio frequency identification (RFID) device (the portable user device 104 is RFID tag, see Fig. 1, col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 9, all the claimed subject maters are cited in respect to claim 1 above.

Regarding claim 10, all the claimed subject matters are cited in respect to claims 2 and 9 above.

Regarding claim 11 all the claimed subject matters are cited ~n respect to claims 3 and 9 above.

Regarding claim 13, all the claimed subject matters are cited ~n respect to claims 5 and 9 above.

Regarding claim 14, all the claimed subject matters are cited ~n respect to claims 6 and 9 above.

Regarding claim 15, all the claimed subject matters are cited ~n respect to claims 7 and 9 above.

Regarding claim 16, all the claimed subject matters are cited ~n respect to claims 8 and 15 above.

Regarding claim 17, all the claimed subject matters are cited ~n respect to claim 1 above.

Regarding claim 18, all the claimed subject matters are cited ~n respect to claims 2 and 17 above.

Regarding claim 19, all the claimed subject matters are cited in respect to claims 3 and 17 above.

Regarding claim 21, all the claimed subject matters are cited in respect to claims 5 and 17 above.

Regarding claim 22, all the claimed subject matters are cited in respect to claims 6 and 17 above.

Regarding claim 23, all the claimed subject matters are cited in respect to claims 7 and 17 above.

Regarding claim 24, all the claimed subject matters are cited in respect to claims 8 and 23 above.

2. Claims 4, 12, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Prokoski et al** and **Wang** and further in view of **Jones et al** [US 7,980,378]

Regarding claim 4, **Prokoski et al** fails to disclose the transaction information is awards information. However, **Prokoski et al** discloses Convenience Users: currently, cell phone and PDAs and modem-equipped laptops are used to make mobile phone calls, access personal databases, calendars, address/phone books, voice mail/email, stock tracking, financial transactions, purchases, internet information access including travel

directions; with a PBK upgrade users are also able to deny use of device to unauthorized persons; and the devices are able to provide transaction security, legally accepted digital signatures, and elimination of passwords. Business and government users: currently, mobile cell phone and PDAs provide: voice mail, email, conference calling, paging, access to personal databases: calendar, address book, maps; access to company network and databases, order placement, report generation, authorizations verbal and written, financial transactions; with a PBK upgrade business users are able to deny use by unauthorized person, positive I D is tagged to each transaction, and Date/Time/Location is tagged to each transmission, and there is enabled legally accepted digital signatures, biometric control of other Bluetooth devices, and a portable personal biometric controller (col. 11, lines 35-62).

Jones et al suggests that the currency processing machines 10 is configured to communicate via an in-store computer system communication link 202,204 to an interface or receiving device 200 at any one of a plurality of destination locations. The destination locations include, but are not limited to, a service desk 210, a POS station 220a-n, a kiosk 230, and/or a portable electronic device 250. The portable electronic device 250 includes a display and a communication interface for enabling communications via the communication links 202, 204. The communication links 202,204 may utilize any convention wired or wireless protocol including, but not limited to, Ethernet, 802.11, Bluetooth.TM., USB, cellular (CDMA, GSM, and the like), and so forth. The associated communication interfaces may include wireless transceivers, USB controllers, Ethernet controllers, RFID transceivers, radio microchips, and/or

transponders, and the like. The portable electronic device 250 may, in different embodiments, be a digital wallet, a mobile a PDA, a smart card, a token, a fob, and the like. The portable electronic device 250 may comprise, for example, a Nokia 3220 telephone comprising a payment chip or a cellular telephone under development by Nokia and Cingular embedded with a "near field communication" ("NFC") chip. The store may, for example, give special promotions for those using credit balances off of their preferred accounts by using balances associated with the preferred card. These aspects enable the retailer to reward their most loyal customers and drive customer purchases into their stores (see Figs. 1-20, col. 15, lines 1-37, col. 41, lines 58-67, col. 60, lines 46-67, col. 61, lines 1-26). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the portable electronic device with the redemption of coupons, promotional or rewarding functions of **Jones et al** to the portable cellular/PDA use by personal/business users of **Prokoski et al** and **Wang** for advantages and conveniences to the business and financial companies to promote of advertisements, bonus, coupons, and/or awards and rewards to their goods and services and most loyal customers and drive/motivate customer purchases into their stores, which are available in the free markets.

Regarding claim 12, all the claimed subject matters are discussed between **Prokoski et al** and **Wang** and **Jones et al** in respect to claims 4 and 9 above.

Regarding claim 20, all the claimed subject matters are discussed between **Prokoski et al** and **Wang** and **Jones et al** in respect to claims 4 and 9 above.

Response to Arguments

3. Applicant's arguments filed on 06/13/2014 have been fully considered but they are not persuasive. Because,

Applicant's arguments:

(A) The mobile device memory 114 does not store transaction information, and the mobile device analyzer 120 does not provide transaction information based on successful authentication of the biometric information.

(B) The receiver subsystem transmits only a lock/unlock signal rather than transaction information as recited in the claim. Assuming arguendo that the lock/unlock signal could be construed as transaction information, the lock/unlock signal is transmitted by the remote receiver subsystem rather than by the mobile device, as recited in claim 1.

Response to the arguments:

(A) The mobile device memory 114 include a database that stores the financial transaction and the analyzer 120 functions to provide a user to do financial transaction after being authorized from the remote authentication.

(B) It is obvious to implement the portable electronic authorization device of **Wang** to the cellular/PDA financial transactions of **Prokoski et al** since the cellular/PDA portable authentication provides a greater convenience to a user with minimizing of losing or

stolen of his/her identification, biometric data from the medium transmissions or wireless data. Additionally, **Prokoski et al** discloses the **Wang**'s portable electronic authorization device PEAD shares some characteristics with the PBK cellular/PDA financial transactions.

Conclusion

4. In response to the interviewed on 08/08/2014, Applicant requests for withdrawing of the Final Rejection filed on 07/09/2014 that applicant do not amended of any claims 1-24 and a new reference of **Wang** was introduced in the Final Rejection. Therefore, a new Non-Office rejection is provided herewith.

5. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 08/08/2014

Applicant-Initiated Interview Summary	**Application No.** 14/028,469	**Applicant(s)** MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	**Art Unit** 2685	

All participants (applicant, applicant's representative, PTO personnel):

(1) *VAN TRIEU*. (3)_____.

(2) *FRANCIS G. PLATI, Reg. No. 59,153*. (4)_____.

Date of Interview: *08 August 2014*.

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: *None*.

Identification of prior art discussed: *None*.

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...)

Applicant requests to withdraw the Final Rejection filed on 07/09/2014 because there was no amendment in all claims 1-24 and a new reference of Wang was introduced into the Final Rejection. Examiner agrees and to introduce a new Non-Final Rejection.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the 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

	/Van T. Trieu/ Primary Examiner, AU 2685

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Notice of References Cited	Application/Control No. 14/028,469	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner VAN TRIEU	Art Unit 2685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,175,922	01-2001	Wang, Ynjiun P.	713/182
	B	US-			
	C	US-			
	D	US-			
	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	
	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.

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	8/8/14
	1	/
	2	/
	3	/
	4	/
	5	/
	6	/
	7	/
	8	/
	9	/
	10	/
	11	/
	12	/
	13	/
	14	/
	15	/
	16	/
	17	/
	18	/
	19	/
	20	/
	21	/
	22	/
	23	/
	24	/
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

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.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

27189 7590 07/09/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
07/09/2014	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. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	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 *06/13/2014*.

☐ 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) *1-24* 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) *1-24* 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 _____ 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

Claim Rejections - 35 USC § 103

The following is a quotation of 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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

1. Claims 1-3, 5-11, 13-19, 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Prokoski et al** [US 6,850,147] in view of **Wang** [US 6,175,922] Regarding claim 1, the claimed a mobile device, comprising Radio Frequency (RF) cellular circuitry (the user's cellular, PDA or portable device 104 embedded with a PBK 102, see Fig. 1, col. 10, lines 15-20); a memory configured to store biometric authentication information and transaction information (the user portable PBK 102

includes a memory 114 for storing biometric data, authorized information, templates and a database 114 with financial transactions data information, see Fig. 1, col. 7, lines 35-53, col. 9, lines 57-60, col. 10, lines 20-25, col. 11, lines 35-62); a biometric reading device configured to read biometric information (the biometric sensor 110, see Fig. 1); But **Prokoski et al** fails to disclose an authentication module to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory and a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module. However, **Prokoski et al** discloses that **Wang** presents a method and apparatus for approving a transaction request between an electronic transaction system and a portable electronic authorization device (PEAD) such as cellular phone, PDA carried by a user using an electronic service authorization token. Advantages of the invention include the ability to securely and conveniently perform transactions with a portable device. The PEAD shares some characteristics with the Personal Biometric Key (PBK) of the current invention (see col. 3, lines 62-67, col. 4, lines 1-4). The user portable PDA 104 embedded with PBK 102 serves/provides as a biometrically secure digital assistant to the user being authenticated or authorized by the remote analyzer 120, 220, 320, 420, 520 for doing financial transactions, money, credit card and/or ATM transactions on the portable PDA 104 to withdraw up to $300.00 or more than $10,000.00 (see Figs. 1-6, col. 6, lines 17-37, col. 7, lines 26-59, col. 8, lines 55-61, col. 10, lines 30-41, 54-67, col. 11, lines 1-22, 50-62). **Wang** discloses a

portable electronic authorization PEAD 200 such as a cellular, smartphone or PDA contained PBK, memories 504, 506, 656, 658, user authentication machine 612 to scan/read fingerprint from the fingerprint sensor, other biometrics and a logic circuitry 502 for authentic a user 160 to do credit card and/or financial transactions on the device 200 through an automated machine teller ATM 100, see Figs. 1-6, col. 5, lines 15-67, col. 6, lines 1-10, col. 9, lines 41-67, col. 10, lines 1-60, col. 11, lines 54-67, col. 12, lines 1-18). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the PEAD of **Wang** for the user portable cellular or PDA of **Prokoski et al** for preventing of losing/stolen user's identification data and for providing convenience and quickly authorization to a user operating a financial transactions without affecting the authentication functions since the both the portable cellular/PDA having similar circuitries as of the remote receiver/authentication device such as the analyzer 120, 220, memory 114, 232 in Figs. 1 and 2.

Regarding claim 2, wherein the biometric reading device is a fingerprint reading device (the fingerprint-based PBK or fingerprint scanner, see col. 8, lines 55-59, col. 13, lines 16-17).

Regarding claim 3, wherein the transaction information is credit card transaction information (the ATM and/or credit/smart card transaction, see col. 2, lines 50-61, col. 6, lines 33-39, col. 7, lines 9-14, 26-34).

Regarding claim 5, further comprising a security block configured to secure the transaction information before it is provided by the transaction module (the central authentication/repository includes encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 6, wherein the security block is a cryptographic block (the encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 7, further comprising an RF device configured to communicate the transaction information to an RF reader/writer (which reads upon the RF short range or Bluethooth for communicating ID tag or RFID tag, see col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 8, wherein the RF device is a radio frequency identification (RFID) device (the portable user device 104 is RFID tag, see Fig. 1, col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 9, all the claimed subject maters are cited in respect to claim 1 above.

Regarding claim 10, all the claimed subject matters are cited in respect to claims 2 and 9 above.

Regarding claim 11, all the claimed subject matters are cited in respect to claims 3 and 9 above.

Regarding claim 13, all the claimed subject matters are cited in respect to claims 5 and 9 above.

Regarding claim 14, all the claimed subject matters are cited in respect to claims 6 and 9 above.

Regarding claim 15, all the claimed subject matters are cited in respect to claims 7 and 9 above.

Regarding claim 16, all the claimed subject matters are cited in respect to claims 8 and 15 above.

Regarding claim 17, all the claimed subject matters are cited in respect to claim 1 above.

Regarding claim 18, all the claimed subject matters are cited in respect to claims 2 and 17 above.

Regarding claim 19, all the claimed subject matters are cited in respect to claims 3 and 17 above.

Regarding claim 21, all the claimed subject matters are cited in respect to claims 5 and 17 above.

Regarding claim 22, all the claimed subject matters are cited in respect to claims 6 and 17 above.

Regarding claim 23, all the claimed subject matters are cited in respect to claims 7 and 17 above.

Regarding claim 24, all the claimed subject matters are cited in respect to claims 8 and 23 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 4, 12, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Prokoski et al** and **Wang** and further in view of **Jones et al** [US 7,980,378]

Regarding claim 4, **Prokoski et al** fails to disclose the transaction information is awards information. However, **Prokoski et al** discloses Convenience Users: currently, cell phone and PDAs and modem-equipped laptops are used to make mobile phone calls, access personal databases, calendars, address/phone books, voice mail/email, stock tracking, financial transactions, purchases, internet information access including travel directions; with a PBK upgrade users are also able to deny use of device to unauthorized persons; and the devices are able to provide transaction security, legally accepted digital signatures, and elimination of passwords. Business and government users: currently, mobile cell phone and PDAs provide: voice mail, email, conference calling, paging, access to personal databases: calendar, address book, maps; access to company network and databases, order placement, report generation, authorizations verbal and written, financial transactions; with a PBK upgrade business users are able to deny use by unauthorized person, positive ID is tagged to each transaction, and Date/Time/Location is tagged to each transmission, and there is

enabled legally accepted digital signatures, biometric control of other Bluetooth devices, and a portable personal biometric controller (col. 11, lines 35-62).

Jones et al suggests that the currency processing machines 10 is configured to communicate via an in-store computer system communication link 202,204 to an interface or receiving device 200 at any one of a plurality of destination locations. The destination locations include, but are not limited to, a service desk 210, a POS station 220a-n, a kiosk 230, and/or a portable electronic device 250. The portable electronic device 250 includes a display and a communication interface for enabling communications via the communication links 202, 204. The communication links 202,204 may utilize any convention wired or wireless protocol including, but not limited to, Ethernet, 802.11, Bluetooth.TM., USB, cellular (CDMA, GSM, and the like), and so forth. The associated communication interfaces may include wireless transceivers, USB controllers, Ethernet controllers, RFID transceivers, radio microchips, and/or transponders, and the like. The portable electronic device 250 may, in different embodiments, be a digital wallet, a mobile a PDA, a smart card, a token, a fob, and the like. The portable electronic device 250 may comprise, for example, a Nokia 3220 telephone comprising a payment chip or a cellular telephone under development by Nokia and Cingular embedded with a "near field communication" ("NFC") chip. The store may, for example, give special promotions for those using credit balances off of their preferred accounts by using balances associated with the preferred card. These aspects enable the retailer to reward their most loyal customers and drive customer purchases into their stores (see Figs. 1-20, col. 15, lines 1-37, col. 41, lines 58-67, col.

60, lines 46-67, col. 61, lines 1-26). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the portable electronic device with the redemption of coupons, promotional or rewarding functions of **Jones et al** to the portable cellular/PDA use by personal/business users of **Prokoski et al** and **Wang** for advantages and conveniences to the business and financial companies to promote of advertisements, bonus, coupons, and/or awards and rewards to their goods and services and most loyal customers and drive/motivate customer purchases into their stores, which are available in the free markets.

Regarding claim 12, all the claimed subject matters are discussed between **Prokoski et al** and **Jones et al** in respect to claims 4 and 9 above.

Regarding claim 20, all the claimed subject matters are discussed between **Prokoski et al** and **Jones et al** in respect to claims 4 and 9 above.

Response to Arguments

3. Applicant's arguments filed on 06/13/2014 have been fully considered but they are not persuasive. Because,

Applicant's arguments:

(A) The mobile device memory 114 does not store transaction information, and the mobile device analyzer 120 does not provide transaction information based on successful authentication of the biometric information.

(B) The receiver subsystem transmits only a lock/unlock signal rather than transaction information as recited in the claim. Assuming arguendo that the lock/unlock signal could be construed as transaction information, the lock/unlock signal is transmitted by the remote receiver subsystem rather than by the mobile device, as recited in claim 1.

Response to the arguments:

(A) The mobile device memory 114 include a database that stores the financial transaction and the analyzer 120 functions to provide a user to do financial transaction after being authorized from the remote authentication.

(B) It is obvious to implement the portable electronic authorization device of **Wang** to the cellular/PDA financial transactions of **Prokoski et al** since the cellular/PDA portable authentication provides a greater convenience to a user with minimizing of losing or stolen of his/her identification, biometric data from the medium transmissions or wireless data. Additionally, **Prokoski et al** discloses the **Wang** portable electronic authorization device PEAD shares some characteristics with the PBK cellular/PDA financial transactions.

Conclusion

4. A 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).

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.

5. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 07/01/2014

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14028469	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
340	539.1, 539.11, 539.13, 568.1, 568.7, 572.1, 572.4, 572.7, 5.52, 5.53, 5.8, 5.82, 5.83, 5.86	12/2/13	vt
235	379, 380, 381	12/2/13	vt
455	419	12/2/13	vt
713	175, 176, 186, 189	12/2/13	vt
705	35, 44, 64	3/29/14	vt

SEARCH NOTES		
Search Notes	Date	Examiner
Update Search	2/27/14	vt
Update Search	7/1/14	vt

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	7/1/14
	1	/
	2	/
	3	/
	4	/
	5	/
	6	/
	7	/
	8	/
	9	/
	10	/
	11	/
	12	/
	13	/
	14	/
	15	/
	16	/
	17	/
	18	/
	19	/
	20	/
	21	/
	22	/
	23	/
	24	/
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(("6850147") or ("7980378") or ("7310734") or ("20020109580") or ("20030074317")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/07/01 11:22
L2	5	1 and transaction near9 (authentication or authoriz$5 or biometr$4 or fingerprint or eye or security)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 11:33
L3	4	1 and (handheld or mobile or cellular or PDA or portable) near9 (PBK or transaction)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 11:39
L4	1	2 and 3 and PBK near9 transaction near4 (data or information)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 11:42
L5	2	1 and (handheld or cellular or PDA or mobile or portable) near9 (authentication or authoriz$5)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 12:53
L6	1	("6175922").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/07/01 12:54
L7	1	6 and (handheld or cellular or PDA or mobile or portable) near9 (authentication or authoriz$5)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 12:55
L8	1	7 and (biometric or eye or face)	US-PGPUB; USPAT; USOCR	OR	ON	2014/07/01 12:57

EAST Search History (Interference)

< This search history is empty>

7/ 1/ 2014 1:00:36 PM
C:\ Users\ vtrieu\ Documents\ EAST\ \ default.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/13	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

EXAMINER	
Van Thanh TRIEU	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
June 13, 2014	EFS WEB

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

Commissioner:

In response to the NON-Final Office Action dated April 3, 2014, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Response, where:

LISTING OF THE CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 6 of this paper.

LISTING OF THE CLAIMS

No amendments are made to the claims in this Response.

LISTING OF CLAIMS:

1. (Previously presented) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

2. (Original) The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. (Original) The mobile device of claim 1, wherein the transaction information is credit card transaction information.

4. (Original) The mobile device of claim 1, wherein the transaction information is awards information.

5. (Original) The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. (Original) The mobile device of claim 5, wherein the security block is a cryptographic block.

7. (Previously presented) The mobile device of claim 1, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

8. (Previously presented) The mobile device of claim 7, wherein the RF device is a radio frequency identification (RFID) device.

9. (Original) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory;

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. (Original) The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. (Original) The mobile device of claim 9, wherein the transaction information is credit card transaction information.

12. (Original) The mobile device of claim 9, wherein the transaction information is awards information.

13. (Original) The mobile device of claim 9, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

14. (Original) The mobile device of claim 9, wherein the security block is a cryptographic block.

15. (Previously presented) The mobile device of claim 9, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

16. (Previously presented) The mobile device of claim 15, wherein the RF device is a radio frequency identification (RFID) device.

17. (Previously presented) A cellular telephone, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

18. (Previously presented) The cellular telephone of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. (Previously presented) The cellular telephone of claim 17, wherein the transaction information is credit card transaction information.

20. (Previously presented) The cellular telephone of claim 17, wherein the transaction information is awards information.

21. (Previously presented) The cellular telephone of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. (Previously presented) The cellular telephone of claim 21, wherein the security block is a cryptographic block.

23. (Previously presented) The cellular telephone of claim 17, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

24. (Previously presented) The cellular telephone of claim 23, wherein the RF device is a radio frequency identification (RFID) device.

REMARKS

Status of the Application

Claims 1-24 are pending in the application and stand rejected. Claims 1, 9, and 17 are the independent claims.

Formal Matters

Applicant thanks the Examiner for considering the references submitted with the Information Disclosure Statement filed on February 28, 2014.

Claim Rejections

Claims 1-3, 5-11, 13-19, and 21-24 — 35 U.S.C. § 102(e)

Claims 1-3, 5-11, 13-19, and 21-24 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,850,147 to Prokoski et al. ("Prokoski"). Applicant respectfully traverses this rejection.

Addressing the rejection of independent claim 1, Applicant respectfully submits that Prokoski does not disclose or suggest at least a "mobile device, comprising … a memory configured to store … transaction information … and a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module," as recited in independent claim 1.

As disclosed by Prokoski, the mobile device memory 114 ***stores only biometric features*** obtained from the biometric sensor 110. The analyzer 120 compares the stored biometric features with currently obtained biometric features from the biometric sensor and ***generates a personal biometric code*** corresponding to the user. ***Only the personal biometric code*** that is based on the sensor input and the stored biometric information ***is encoded and transmitted*** to a receiver 210 in a receiver subsystem (col. 10, ll. 17-28). On the other hand, as recited in claim 1, the ***transaction module in the mobile device*** is configured to ***provide the transaction information for use in a transaction***.

The remote, i.e., not part of the mobile device, receiver 210 disclosed by Prokoski receives the encoded transmission, and a decoder/analyzer 220 ***extracts the personal biometric code***. A comparator 230 ***in the remote receiver subsystem*** compares the personal biometric code

with a stored reference, and ***sends a lock or unlock signal***, depending on the comparison results, to a controlled mechanism (col. 10, ll. 30-40).

Thus, the mobile device ***memory 114 does not store transaction information***, and the ***mobile device analyzer 120 does notprovide transaction information*** based on successful authentication of the biometric information, as alleged by the Examiner. Therefore, Prokoski does not disclose or suggest at least the claimed memory and transaction module.

Further, the receiver subsystem ***transmits only a lock/unlock signal*** rather than transaction information as recited in the claim. Assuming *arguendo* that the lock/unlock signal could be construed as transaction information, the lock/unlock signal is ***transmitted by the remote receiver subsystem rather than by the mobile device***, as recited in claim 1.

Accordingly, since Prokoski does not disclose or suggest all of the claimed features, Applicant respectfully submits that independent claim 1 is patentable over Prokoski.

Independent claims 9 and 17 contain features similar to the features recited in claim 1 and are therefore patentable for similar reasons.

Claims 2, 3, 5-8, 10, 11, 13-16, 18, 19, and 21-24 are patentable at least by virtue of their respective dependencies.

Claims 4, 12, and 20 - 35 U.S.C. § 103(a)

Claims 4, 12, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Prokoski in view of U.S. Patent No. 7,980,378 to Jones et al. ("Jones"). Applicant respectfully traverses this rejection.

The combination of Prokoski and Jones does not disclose or suggest at least The above-noted features of claims 1, 9, and 17 incorporated into claims 4, 12, and 20 by virtue of their respective dependencies. As established above, Prokoski does not disclose or suggest at least these features. Jones does not cure the deficiencies of Prokoski.

The Examiner relies on Jones only to allegedly disclose the claimed features related to awards information as transaction information, as recited in the dependent claims. Without conceding the disclosure of Jones alleged by the Examiner, Applicant respectfully submits that Jones fails to disclose or suggest at least the features of a "mobile device, comprising … a memory configured to store … transaction information … and a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module,"

as incorporated into claims 4, 12, and 20 by virtue of their respective dependencies. Thus, Jones fails to cure the deficiencies of Prokoski.

Accordingly, since the combination of Prokoski and Jones does not disclose or suggest all of the claimed features, Applicant respectfully submits that claims 4, 12, and 20 are patentable over the combined references.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-24 is respectfully requested. If the Examiner believes that a telephone conversation may be useful in advancing prosecution, the Examiner is invited to contact the undersigned at the number listed below.

If necessary, applicant requests to extend the period for filing this reply pursuant to 37 CFR 1.136(a) and authorizes the Director to charge any additional fee(s) or any underpayment of fee(s) or credit any overpayment(s) to Procopio Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: June 13, 2014

/ /
Francis G. Plati
Reg. No. 59,153

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

Electronic Acknowledgement Receipt

EFS ID:	19307034
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	Francis G. Plati Sr./angelica zepeda
Filer Authorized By:	Francis G. Plati Sr.
Attorney Docket Number:	116546-6601UT
Receipt Date:	13-JUN-2014
Filing Date:	16-SEP-2013
Time Stamp:	22:35:21
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		116546-6601UT_Response.pdf	152967 de07ec70153713250f6b48640faccfac3946ae50	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Abstract	6	8
Warnings:			
Information:			
	Total Files Size (in bytes):	152967	

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

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

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

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

PTO/SB/06 (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 14/028,469	Filing Date 09/16/2013	☐ 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	06/13/2014	(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))	* 24	Minus	** 24	= 0	X $80 =	0
	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	0

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
/CORALIA BETANCOURT/

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.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

27189 7590 04/03/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
04/03/2014	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. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	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 *03/14/2014*.

☐ 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) *1-24* 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) *1-24* 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 _____ 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 *2/28/2014*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

1. Claim 1-3, 5-11, 13-19, 21-24 are rejected under 35 U.S.C. 102(e) as being anticipated by **Prokoski et al** [US 6,850,147].

Regarding claim 1, the claimed a mobile device, comprising Radio Frequency (RF) cellular circuitry (the user portable device 102 embedded a Cellular/PDA 104, see Fig. 1, col. 10, lines 15-20); a memory configured to store biometric authentication information and transaction information (the database 114 for storing biometric PBK information and transaction data, see Fig. 1, col. 9, lines 57-60, col. 10, lines 20-25, col. 11, lines 35-44); a biometric reading device configured to read biometric information (the biometric sensor 110, see Fig. 1); an authentication module to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory (the analyzer 220, 420, 520 and comparator 230, 530 and the database 232, 414, 514 to send authorized signal to unlock mechanism 240, 540 or to access to any device such as personal database, company computer networks and databases, and/or authorizations ATM transactions, financial transactions or send to the central authentication subsystem 650 for

authorizations, see Figs. 2, 4, 5, 6, col. 6, lines 17-24, col. 7, lines 26-32, col. 10, lines 30-41, 54-67, col. 11, lines 1-22, 50-62); and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module (the PBK serves as a biometrically secure digital assistant in documenting legal, ATM transactions and financial transactions, transmitted over the internet, phone system, personal exchanges, or stored in a database (see Figs. 2, 4, 5, 6, col. 6, lines 17-24, col. 7, lines 26-32, col. 10, lines 30-41, 54-67, col. 11, lines 1-22, 50-62).

Regarding claim 2, wherein the biometric reading device is a fingerprint reading device (the fingerprint-based PBK or fingerprint scanner, see col. 8, lines 55-59, col. 13, lines 16-17).

Regarding claim 3, wherein the transaction information is credit card transaction information (the ATM and/or credit/smart card transaction, see col. 2, lines 50-61, col. 6, lines 33-39, col. 7, lines 9-14, 26-34).

Regarding claim 5, further comprising a security block configured to secure the transaction information before it is provided by the transaction module (the central authentication/repository includes encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 6, wherein the security block is a cryptographic block (the encryption techniques, see Fig. 6, col. 9, lines 61-67, col. 10, line 1, col. 12, lines 40-41).

Regarding claim 7, further comprising an RF device configured to communicate the transaction information to an RF reader/writer (which reads upon the RF short range or Bluethooth for communicating ID tag or RFID tag, see col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 8, wherein the RF device is a radio frequency identification (RFID) device (the portable user device 104 is RFID tag, see Fig. 1, col. 3, lines 59-61, col. 7, lines 49-57, col. 11, lines 50-67, col. 12, lines 1-41).

Regarding claim 9, all the claimed subject maters are cited in respect to claim 1 above.

Regarding claim 10, all the claimed subject matters are cited in respect to claims 2 and 9 above.

Regarding claim 11, all the claimed subject matters are cited in respect to claims 3 and 9 above.

Regarding claim 13, all the claimed subject matters are cited in respect to claims 5 and 9 above.

Regarding claim 14, all the claimed subject matters are cited in respect to claims 6 and 9 above.

Regarding claim 15, all the claimed subject matters are cited in respect to claims 7 and 9 above.

Regarding claim 16, all the claimed subject matters are cited in respect to claims 8 and 15 above.

Regarding claim 17, all the claimed subject matters are cited in respect to claim 1 above.

Regarding claim 18, all the claimed subject matters are cited in respect to claims 2 and 17 above.

Regarding claim 19, all the claimed subject matters are cited in respect to claims 3 and 17 above.

Regarding claim 21, all the claimed subject matters are cited in respect to claims 5 and 17 above.

Regarding claim 22, all the claimed subject matters are cited in respect to claims 6 and 17 above.

Regarding claim 23, all the claimed subject matters are cited in respect to claims 7 and 17 above.

Regarding claim 24, all the claimed subject matters are cited in respect to claims 8 and 23 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 4, 12, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Prokoski et al** [US 6,850,147] in view of **Jones et al** [US 7,980,378]

Regarding claim 4, **Prokoski et al** fails to disclose the transaction information is awards information. However, **Prokoski et al** discloses Convenience Users: currently, cell phone and PDAs and modem-equipped laptops are used to make mobile phone calls, access personal databases, calendars, address/phone books, voice mail/email, stock tracking, financial transactions, purchases, internet information access including travel directions; with a PBK upgrade users are also able to deny use of device to unauthorized persons; and the devices are able to provide transaction security, legally accepted digital signatures, and elimination of passwords.

Business and government users: currently, mobile cell phone and PDAs provide: voice mail, email, conference calling, paging, access to personal databases: calendar, address book, maps; access to company network and databases, order placement, report generation, authorizations verbal and written, financial transactions; with a PBK upgrade business users are able to deny use by unauthorized person, positive ID is tagged to each transaction, and Date/Time/Location is tagged to each transmission, and there is enabled legally accepted digital signatures, biometric control of other Bluetooth devices, and a portable personal biometric controller (col. 11, lines 35-62). Jones et al suggests that the currency processing machines 10 is configured to communicate via

an in-store computer system communication link 202,204 to an interface or receiving device 200 at any one of a plurality of destination locations. The destination locations include, but are not limited to, a service desk 210, a POS station 220a-n, a kiosk 230, and/or a portable electronic device 250. The portable electronic device 250 includes a display and a communication interface for enabling communications via the communication links 202, 204. The communication links 202,204 may utilize any convention wired or wireless protocol including, but not limited to, Ethernet, 802.11, Bluetooth.TM., USB, cellular (CDMA, GSM, and the like), and so forth. The associated communication interfaces may include wireless transceivers, USB controllers, Ethernet controllers, RFID transceivers, radio microchips, and/or transponders, and the like. The portable electronic device 250 may, in different embodiments, be a digital wallet, a mobile a PDA, a smart card, a token, a fob, and the like. The portable electronic device 250 may comprise, for example, a Nokia 3220 telephone comprising a payment chip or a cellular telephone under development by Nokia and Cingular embedded with a "near field communication" ("NFC") chip. The store may, for example, give special promotions for those using credit balances off of their preferred accounts by using balances associated with the preferred card. These aspects enable the retailer to reward their most loyal customers and drive customer purchases into their stores (see Figs. 1-20, col. 15, lines 1-37, col. 41, lines 58-67, col. 60, lines 46-67, col. 61, lines 1-26). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the portable electronic device with the redemption of coupons, promotional or rewarding functions of **Jones et al** to the portable

cellular/PDA use by personal/business users of **Prokoski et al** for advantages and conveniences to the business and financial companies to promote of advertisements, bonus, coupons, and/or awards and rewards to their goods and services and most loyal customers and drive/motivate customer purchases into their stores, which are available in the free markets.

Regarding claim 12, all the claimed subject matters are discussed between **Prokoski et al** and **Jones et al** in respect to claims 4 and 9 above.

Regarding claim 20, all the claimed subject matters are discussed between **Prokoski et al** and **Jones et al** in respect to claims 4 and 9 above.

Response to Arguments

3. Applicant's arguments, see the response, filed 03/14/2014, with respect to the rejection(s) of claim(s) 1-23 under **Beenau** have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Prokoski et al** to make the rejection smoother as above.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Boate et al discloses the improved computer network security system and a personal identifier device used for controlling network with real time authentication of both a person's identity and presence at a computer workstation is provided. A new user is registered to a portable personal digital identifier device and, within the portable personal digital identifier device, an input biometric of the user is received and a master template is derived therefrom and securely maintained in storage. A private key and public key encryption system is utilized to authenticate a user registered to the portable personal digital identifier device. The personal digital identifier device verifies the origin of a digitally signed challenge message from the network security manager component. A digitally and biometrically signed challenge response message is produced and transmitted by the personal digital identifier device in response to the verified challenge message. [US 7,310,734]

Shreve et al discloses the two-way bi-directional wireless-based access communication system that allows a user to access any one of multiple independent secured domain systems from a single handheld remote keyless entry device, whereupon activation of the remote keyless device by the user, an encoded request signal containing a predetermined access code is generated and transmitted by the remote keyless entry device to one of the multiple secure domain systems. And, based on the access code contained within the encoded request signal, the domain system determines the validity of the access code and transmits a corresponding encoded authorization signal to user at the transceiver device. [US 2002/0109580]

Hofi discloses the user portable device, system and method for authorizing a transaction requested by an authorized user while preventing authorization of a transaction requested by an unauthorized user. The system comprises a user device and a server device. The user portable device comprises (a) an identity verification unit operable to receive current biometric input from a current user and to utilize that biometric input to determine if the current user is an authorized user of the device; (b) a transaction code provider operable to provide a transaction code if, and only if, the identity verification unit determines that a current user is an authorized user; and (c) a first communication device operable to communicate the provided transaction code. The server device comprises (a) a second communication device operable to receive a communicated code; (b) a transaction code verifier operable to determine if a received communicated code is a transaction code provided by the transaction code provider; and (c) an authorizer operable to authorize a transaction if and only if said transaction code verifier determines that a received communicated code is a verified transaction code. [US 2003/0074317]

5. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 03/29/2014

Notice of References Cited	Application/Control No. 14/028,469	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner VAN TRIEU	Art Unit 2685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,850,147	02-2005	Prokoski et al.	340/5.53
*	B	US-7,310,734	12-2007	Boate et al.	713/186
*	C	US-2002/0109580	08-2002	Shreve et al.	340/5.61
*	D	US-2003/0074317	04-2003	Hofi, Eyal	705/44
	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	
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	11	(("8126449") or ("6182894") or ("7225337") or ("4529870") or ("6793134") or ("7671746") or ("8004410") or ("7980378") or ("8126449") or ("8401539") or ("20100094754") or ("20100095130")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 07:59
L2	13184	(biometric or fingerprint or eye) near9 (cellular or handheld or mobile or PDA or portable)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:01
L3	101015	(inquir$3 or requir$3 or request$3) near9 (financial or transaction)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:02
L4	303368	(compar$5 or match$3) near9 (code or ID or key or security)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:03
L5	124761	(authenti$5 or authoriz$5) near9 (code or ID or key or security)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:04
L6	665	2 and 3 and 4 and 5	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:04
L7	135	(1 or 6) not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:05
L8	87	7 and (RFID or radio or RF or antenna or dipole)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:06
L10	1	("6016476").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 08:52
L11	1	10 and 2	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:53
L12	4626	(compar$5 or match$3) near9 ((code or ID or key) near4 security)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:56
L13	10	(8 or 10) and 12	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 08:57
L14	7	13 and (biometric or eye)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:02
L15	4	14 and (inquir$3 or request$3) near4 access$3	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:11
L16	6	14 and (inquir$3 or request$3) and access$3	US-PGPUB; USPAT;	OR	ON	2014/03/28 09:12

			USOCR			
L17	6	14 and (inquir$3 or request$3) same access$3	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:13
L18	6	14 and (inquir$3 or request$3) with access$3	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:13
L19	137	(("8041815") or ("7844505") or ("7533809") or ("7487538") or ("7080819") or ("7031946") or ("6975834") or ("6950013") or ("6894615") or ("6758405") or ("6753759") or ("6698653") or ("6617961") or ("6427504") or ("6388579") or ("6360208") or ("6340116") or ("6334059") or ("6570487") or ("6276607") or ("6275157") or ("6269292") or ("6268796") or ("6211790") or ("6203952") or ("6175922") or ("6167333") or ("6157333") or ("6140941") or ("6111506") or ("6104281") or ("6098879") or ("6073840") or ("6052068") or ("6025784") or ("6025780") or ("5974500") or ("5874896") or ("5864580") or ("5787174") or ("5742618") or ("5657008") or ("5552789") or ("20050149764") or ("20030200227") or ("20020089434") or ("2004006165") or ("2002042076") or ("9843104") or ("0993999") or ("0977145")).PN. or ((19/608757) or (10/042805)).APP.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/03/28 09:23
L20	1	19 and 8	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:24
L21	0	20 and 12	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:25
L22	10245	(G06F1/00, G06F19/00, G06F19/10, G06F21/31, G06F21/32, G06F21/34).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:40
L24	17230	(G06Q20/10, G06Q20/105, G06Q20/32, G06Q20/322, G06Q20/3278).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:44
L25	10753	(H04W12/06, H04W12/08).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:45
L26	21	22 and 24 and 25	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:45
L27	4	26 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:46
L28	1	27 and (inquir$3 or request$3) with access$3	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 09:47

EAST Search History (Interference)

<This search history is empty>

3/28/2014 9:48:43 AM
C:\Users\vtrieu\Documents\EAST\\default.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. 3712

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/028,469	09/16/2013 RULE	705	2685	116546-6601UT

APPLICANTS

INVENTORS

Francisco Martinez de Velasco Cortina, La Jolla, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

**** CONTINUING DATA **************************** /vt/

This application 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 **************************** /vt/

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
10/08/2013

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged _____ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	24	24	3

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		
2220	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).

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	14028469
Filing Date	2013-09-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	2685
Examiner Name	TRIEU, VAN THANH
Attorney Docket Number	116546-66001UT

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	8041815	B2	2011-10-18	Bahl et al.	
	2	7844505	B1	2010-11-30	Arneson et al.	
	3	7533809	B1	2009-05-19	Robinson et al.	
	4	7487538	B2	2009-02-03	Mok	
	5	7080819	B2	2006-07-25	Tojo	
	6	7031946	B1	2006-04-18	Tamai et al.	
	7	6975834	B1	2005-12-13	Forster	
	8	6950013	B2	2005-09-27	Scaman et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	9	6894615	B2	2005-05-17	Look	
	10	6758405	B2	2004-07-06	Look	
	11	6753759	B2	2004-06-22	Stegmaier et al.	
	12	6698653	B1	2004-03-02	Diamond et al.	
	13	6617961	B1	2003-09-09	Janssen et al.	
	14	6570487	B1	2003-05-27	Steeves	
	15	6427504	B1	2002-08-06	Janssen et al.	
	16	6388579	B1	2002-05-14	Adcox et al.	
	17	6360208	B1	2002-03-19	Ohanian et al.	
	18	6340116	B1	2002-01-22	Cecil et al.	
	19	6334059	B1	2001-12-25	Stilp et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	20	6276607	B1	2001-08-21	Sato	
	21	6275157	B1	2001-08-14	Mays et al.	
	22	6269292	B1	2001-07-31	Kokubu et al.	
	23	6268796	B1	2001-07-31	Gnadinger et al.	
	24	6211790	B1	2001-04-03	Radomsky et al.	
	25	6203952	B1	2001-03-20	O'Brien et al.	
	26	6175922	B1	2001-01-16	Wang	
	27	6167333	A	2000-12-26	GEHLOT; NARAYAN L. et al.	
	28	6157333	A	2000-12-05	Louagie et al.	
	29	6140941	A	2000-10-31	Dwyer et al.	
	30	6111506	A	2000-08-29	YAP; CHAS HOCK ENG et al.	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	31	6104281	A	2000-08-15	HEINRICH; HARLEY KENT et al.	
	32	6098879	A	2000-08-08	TERRANOVA; STEVEN N. et al.	
	33	6073840	A	2000-06-13	MARION; KENNETH O. et al.	
	34	6052068	A	2000-04-18	PRICE R et al.	
	35	6025784	A	2000-02-15	Mish	
	36	6025780	A	2000-02-15	BOWERS; JOHN H. et al.	
	37	5974500	A	1999-10-26	MALETSKY; KERRY D. et al.	
	38	5874896	A	1999-02-23	SMALL et al.	
	39	5864580	A	1999-01-26	Lowe et al.	
	40	5787174	A	1998-07-28	TUTTLE JOHN R	
	41	5742618	A	1998-04-21	Lowe	

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	42	5657008	A	1997-08-12	Bantli	
	43	5552789	A	1996-09-03	Schuermann	
	44					

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	20050149764	A1	2005-07-07	Bahl et al.	
	2	20030200227	A1	2003-10-23	Ressler	
	3	20020089434	A1	2002-07-11	Ghazarian	
	4					

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]

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	1	2004006165	WO	A1	2004-01-15	CORTINA		☐
	2	2002042076	JP	A	2002-02-08	NISHIKAWA SEIICHI		☐
	3	19608757	DE	A1	1997-09-11	NICHTNENNUNG		☐
	4	10042805	DE	A1	2002-03-14	LANGENSTUECK HOLGER		☐
	5	9843104	WO	A2	1998-10-01	PRICE FREDERICK J R-W		☐
	6	993999	EP	A2	2000-04-19	Gilmore		☐
	7	977145	EP	A2	2000-02-02	Karasawa		☐
	8							☐

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, Solution Making Smart Cards Smarter, 2000, 12 pages.	☐

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	2	Extended European Search Report issued by the European Patent Office in related European Application No. 10182033.0 dated Jan. 13, 2012 (7 pages).	☐
	3	FANCHER, Carol Hovenga, In Your Pocket Smartcards, IEEE Spectrum, February 2007, 7 pages.	☐
	4	RAKERS, Patrick, et al., Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal Of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	☐
	5	Official Action in Japanese Patent Application No. 2004-519130 dated May 12, 2009, 10 pages.	☐
	6	Anonymous, Read Write RFID Offers Standalone Advantages, Security, August 1996, 1 page.	☐
	7	21 C.C.R. §1700	☐
	8	21 C.C.R. § 1701(r)	☐
	9	21 C.C.R. § 1702.1	☐
	10	21 C.C.R. § 1703(c)	☐
	11	21 C.C.R. § 1703(e-i)	☐
	12	21 C.C.R. § 1704.1	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	13	21 C.C.R. § 1704.2	☐
	14	21 C.C.R. § 1704.3	☐
	15	21 C.C.R. § 1704.5(e)(1)	☐
	16	21 C.C.R. § 1704.6	☐
	17	21 C.C.R. § 1705.1	☐
	18	21 C.C.R. § 1705.2	☐
	19	21 C.C.R. § 1705.3	☐
	20	21 C.C.R. § 1705.4	☐
	21	21 C.C.R. § 1705.5	☐
	22	21 C.C.R. § 1705.5(d) and (e)(1)	☐
	23	21 C.C.R. 1705.8	☐

EFS Web 2.1.17 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

If you wish to add additional non-patent literature document citation information please click the Add button			Add
EXAMINER SIGNATURE			
Examiner Signature	/Van Trieu/ (03/29/2014)	Date Considered	03/29/2014

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /VT/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

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	/ F.G. Plati /	Date (YYYY-MM-DD)	2014-02-28
Name/Print	Francis G. Plati, Sr.	Registration Number	59153

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. /VT/

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. /VT/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(("6016476") or ("6850147") or ("7310734") or ("20020104006") or ("20030074317")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 12:40
L2	3	1 and (inquir$3 or request$3) with access$3	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:42
L3	5	1 and (compar$5 or different or match$3) near9 ((code or ID or key) near4 (user or password or transaction or security))	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:44
L4	5	1 and (biometric or eye)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:45
L5	3	2 and 3 and 4	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:45
L6	5	1 and (financial$2 or transaction)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:49
L7	1	1 and RFID	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:51
L8	4	1 and (RF or antenna or PDA)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:52
L9	4	1 and (RF or antenna or PDA or transponder)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:52
L10	5	1 and radio	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 12:53
L11	4	1 and access$4 near9 (memory or database or storage)	US-PGPUB; USPAT; USOCR	OR	ON	2014/03/28 14:16
L25	4	(("8237568") or ("8004410") or ("7671746") or ("7081819")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/03/28 14:55

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L12	13193	(biometric or fingerprint or eye) near9 (cellular or handheld or mobile or PDA or portable)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:18
L13	102928	(inquir$3 or requir$3 or request$3) near9 (financial or transaction)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:19
L14	515886	(compar$5 or different or match$3) near9 (code or ID or key or security)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:19
L15	125221	(authenti$5 or authoriz$5) near9 (code or ID or key or security)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:19
L16	813	12 and 13 and 14 and 15	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:20
L18	147	16 not @AY > "2003"	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:20
L19	1245168	access$4 near9 (memory or database or storage)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:21
L20	122	18 and 19	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:21
L21	3666	19 near9 (receiv$3 or obtain$3) near9 (antenna or RF or radio or wireless or transceiv$3 or transponder)	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:22
L22	1	20 and 21	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:23
L23	28	(compar$5 or different or match$3) near9 (code or ID or key or security) near9 21	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:26
L24	0	22 and 23	US-PGPUB; USPAT; UPAD	OR	ON	2014/03/28 14:26

3/28/2014 3:16:57 PM
C:\Users\vtrieu\Documents\EAST\\default.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14028469	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
340	539.1, 539.11, 539.13, 568.1, 568.7, 572.1, 572.4, 572.7, 5.52, 5.53, 5.8, 5.82, 5.83, 5.86	12/2/13	vt
235	379, 380, 381	12/2/13	vt
455	419	12/2/13	vt
713	175, 176, 186, 189	12/2/13	vt
705	35, 44, 64	3/29/14	vt

SEARCH NOTES		
Search Notes	Date	Examiner
Update Search	2/27/14	vt

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	12/6/13	2/27/14	3/29/14						
	1	/	/	/						
	2	/	/	/						
	3	/	/	/						
	4	/	/	/						
	5	/	/	/						
	6	/	/	/						
	7	/	/	/						
	8	/	/	/						
	9	/	/	/						
	10	/	/	/						
	11	/	/	/						
	12	/	/	/						
	13	/	/	/						
	14	/	/	/						
	15	/	/	/						
	16	/	/	/						
	17	/	/	/						
	18	/	/	/						
	19	/	/	/						
	20	/	/	/						
	21	/	/	/						
	22	/	/	/						
	23	/	/	/						
	24	/	/	/						
	25									
	26									
	27									
	28									
	29									
	30									
	31									
	32									
	33									
	34									
	35									
	36									
	37									
	38									
	39									
	40									
	41									
	42									
	43									
	44									
	45									
	46									
	47									
	48									
	49									
	50									

Claim		Date								
Final	Original									
	51									
	52									
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/13	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

EXAMINER	
Van Thanh TRIEU	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
March 14, 2014	EFS WEB

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

Commissioner:

In response to the NON-Final Office Action dated March 6, 2014, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Response, where:

AMENDMENTS TO THE CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 6 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently amended) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module ~~configure~~ configured to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

2. (Original) The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. (Original) The mobile device of claim 1, wherein the transaction information is credit card transaction information.

4. (Original) The mobile device of claim 1, wherein the transaction information is awards information.

5. (Original) The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. (Original) The mobile device of claim 5, wherein the security block is a cryptographic block.

7. (Previously presented) The mobile device of claim 1, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

8. (Previously presented) The mobile device of claim 7, wherein the RF device is a radio frequency identification (RFID) device.

9. (Original) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory;

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. (Original) The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. (Original) The mobile device of claim 9, wherein the transaction information is credit card transaction information.

12. (Original) The mobile device of claim 9, wherein the transaction information is awards information.

13. (Original) The mobile device of claim 9, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

14. (Original) The mobile device of claim 9, wherein the security block is a cryptographic block.

15. (Previously presented) The mobile device of claim 9, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

16. (Previously presented) The mobile device of claim 15, wherein the RF device is a radio frequency identification (RFID) device.

17. (Currently amended) A ~~mobile device~~cellular telephone, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module ~~configure~~ configured to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

18. (Currently amended) The ~~mobile device~~cellular telephone of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. (Currently amended) The ~~mobile device~~cellular telephone of claim 17, wherein the transaction information is credit card transaction information.

20. (Currently amended) The ~~mobile device~~cellular telephone of claim 17, wherein the transaction information is awards information.

21. (Currently amended) The ~~mobile device~~cellular telephone of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. (Currently amended) The ~~mobile device~~cellular telephone of claim 21, wherein the security block is a cryptographic block.

23. (Currently amended) The ~~mobile device~~cellular telephone of claim 17, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

24. (Currently amended) The ~~mobile device~~cellular telephone of claim 23, wherein the RF device is a radio frequency identification (RFID) device.

REMARKS

Status of the Application

Claims 1-24 are pending in the application and stand rejected. Claims 1, 9, and 17 are the independent claims.

Claim Rejections

Claims 1-24 — 35 U.S.C. § 102(b)

Claims 1-24 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 8,126,449 to Beenau et al. ("Beenau"). Applicant respectfully traverses this rejection.

Applicant respectfully submits that Beenau is not prior art with respect to the present application. The filing date of Beenau is November 13, 2008, which is after the instant application's provisional priority date of July 9, 2002, based on U.S. Provisional Application No. 60/394,241. The provisional application is believed to fully support the claimed inventions. By way of example, pages 34 to 39 of the drawings and the accompanying description support the claims of the present application.

Accordingly, Applicant respectfully submits that the rejection of claims 1-24 based on Beenau is in error and should be withdrawn.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-24 is respectfully requested. If the Examiner believes that a telephone conversation may be useful in advancing prosecution, the Examiner is invited to contact the undersigned at the number listed below.

If necessary, applicant requests to extend the period for filing this reply pursuant to 37 CFR 1.136(a) and authorizes the Director to charge any additional fee(s) or any underpayment of fee(s) or credit any overpayment(s) to Procopio Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: March 14, 2014

/ /

Francis G. Plati, Sr.
Reg. No. 59,153

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

Electronic Acknowledgement Receipt

EFS ID:	18485756
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	Francis G. Plati Sr./angelica zepeda
Filer Authorized By:	Francis G. Plati Sr.
Attorney Docket Number:	116546-6601UT
Receipt Date:	14-MAR-2014
Filing Date:	16-SEP-2013
Time Stamp:	20:40:45
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		116546-6601UT_amendment.pdf	116703 e108a953f28fc97533c9056e93eb80ed5d0249ad	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	7

Warnings:	
Information:	
Total Files Size (in bytes):	116703

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

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

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

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

PTO/SB/06 (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 14/028,469	Filing Date 09/16/2013	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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	03/14/2014	(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))	* 24	Minus	** 24	= 0	X $80 =	0
	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	0

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
/HALLEY MASSEY/

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.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

27189 7590 03/06/2014

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
03/06/2014	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. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	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 *03 February 2014*.

☐ 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) *1-24* 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) *1-24* 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 _____ 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

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-24 are rejected under 35 U.S.C. 102(b) as being anticipated by **Beenau et al** [US 8,126,449].

Regarding claim 1, the claimed a mobile device, comprising Radio Frequency (RF) cellular circuitry (the system 100 includes a mobile device 110 such as mobile phone or cellular phone including RF communications circuitry, see Fig. 1, col. 3, lines 47-48, col. 5, lines 2-11);

a memory configured to store biometric authentication information and transaction information (the mobile device 110 is configured with a biometric security system with a computer-readable storage medium and memory for storing the TXA-ID includes data such as account number, biometric data, identification and related information for authentication, verifying authorized user and/or authorizing a transaction, see Fig. 1, col. 4, lines 10-67, col. 5, lines 24-46, col. 7, lines 3-35, col. 11, lines 8-27);

a biometric reading device configured to read biometric information (the biometric scanner, see col. 5, lines 34-39);

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory (the mobile phone 110 is used to provide authorization or authentication to a user and/or financial transaction based on the scanned biometric and stored biometric data, see Figs. 1-3, col. 4, lines 10-67, col. 5, lines 24-60, col. 7, lines 3-35, col. 11, lines 8-27); and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module (the TXA payment or transaction processes based on the scanned consumer/customer/user's biometric information, see Figs. 1-4, col. 2, lines 52-65, col. 3, lines 20-56, col. 4, lines 10-67, col. 5, lines 1-46, col. 13, lines 4-63).

Regarding claim 2, wherein the biometric reading device is a fingerprint reading device (the scanning of fingerprint, facial, ear, signature, hand geometry, iris, retinal or any other biometrics, see col. 5, lines 33-46).

Regarding claim 3, wherein the transaction information is credit card transaction information (the credit card, American express card, Visa card, and etc. see col. 6, lines 24-43).

Regarding claim 4, wherein the transaction information is awards information (the reward card or reward program, see col. 3, lines 33-34, col. 4, lines 10-12).

Regarding claim 5, further comprising a security block configured to secure the transaction information before it is provided by the transaction module (the system 100 could be used to detect or prevent security issues with a client-side scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography and network security, see any of the following references: (1) "Applied Cryptography: Protocols, Algorithms, And Source Code In C", by Bruce Schneier, published by John Wiley & Sons (second edition, 1995); (2) "Java Cryptography" by Jonathan Knudson, published by O'Reilly & Associates (1998); (3) "Cryptography & Network Security: Principles & Practice" by William Stallings, published by Prentice Hall; all of which are hereby incorporated by reference (see col. 11, lines 30-41).

Regarding claim 6, wherein the security block is a cryptographic block (the cryptography, see co. 11, lines 30-41).

Regarding claim 7, further comprising an RF device configured to communicate the transaction information to an RF reader/writer (the RFID or RF communications, RF transponder and/or RF interrogator, see col. 3, lines 39-49, 58).

Regarding claim 8, wherein the RF device is a radio frequency identification (RFID) device (the RFID, see col. 3, lines 39-47).

Regarding claim 9, all the claimed subject matters are cited in respect to claims 1 and 5 above.

Regarding claim 10, all the claimed subject matters are cited in respect to claims 2 and 9 above.

Regarding claim 11, all the claimed subject matters are cited in respect to claims 3 and 9 above.

Regarding claim 12, all the claimed subject matters are cited in respect to claims 4 and 9 above.

Regarding claim 13, all the claimed subject matters are cited in respect to claims 5 and 9 above.

Regarding claim 14, all the claimed subject matters are cited in respect to claims 6 and 9 above.

Regarding claim 15, all the claimed subject matters are cited in respect to claims 7 and 9 above.

Regarding claim 16, all the claimed subject matters are cited in respect to claims 8 and 15 above.

Regarding claim 17, all the claimed subject matters are cited in respect to claim 1 above.

Regarding claim 18, all the claimed subject matters are cited in respect to claims 2 and 17 above.

Regarding claim 19, all the claimed subject matters are cited in respect to claims 3 and 17 above.

Regarding claim 20, all the claimed subject matters are cited in respect to claims 4 and 17 above.

Regarding claim 21, all the claimed subject matters are cited in respect to claims 5 and 18 above.

Regarding claim 22, all the claimed subject matters are cited in respect to claims 6 and 21 above.

Regarding claim 23, all the claimed subject matters are cited in respect to claims 7 and 17 above.

Regarding claim 24, all the claimed subject matters are cited in respect to claims 8 and 23 above.

Response to Arguments

2. Applicant's arguments, see the response, filed 03 February 2014, with respect to the arguments have been fully considered and are persuasive. The previous Office Rejection of 06 December 2013 has been withdrawn. A new Office Rejection is based on the previous cited reference of **Beenau et al** to make the rejection smoother regarding to the mobile device including a biometric reader/scanner.

Conclusion

3. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 02/27/2014

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	12/6/13	2/27/14							
	1	/	/							
	2	/	/							
	3	/	/							
	4	/	/							
	5	/	/							
	6	/	/							
	7	/	/							
	8	/	/							
	9	/	/							
	10	/	/							
	11	/	/							
	12	/	/							
	13	/	/							
	14	/	/							
	15	/	/							
	16	/	/							
	17	/	/							
	18	/	/							
	19	/	/							
	20	/	/							
	21	/	/							
	22	/	/							
	23	/	/							
	24	/	/							
	25									
	26									
	27									
	28									
	29									
	30									
	31									
	32									
	33									
	34									
	35									
	36									
	37									
	38									
	39									
	40									
	41									
	42									
	43									
	44									
	45									
	46									
	47									
	48									
	49									
	50									

Claim		Date								
Final	Original									
	51									
	52									
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14028469	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
340	539.1, 539.11, 539.13, 568.1, 568.7, 572.1, 572.4, 572.7	12/2/13	vt
235	379, 380, 381	12/2/13	vt
455	419	12/2/13	vt
713	175, 189	12/2/13	vt

SEARCH NOTES		
Search Notes	Date	Examiner
Update Search	2/27/14	vt

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10	(("7225337") or ("7980378") or ("4529870") or ("6793134") or ("7671746") or ("8004410") or ("8126449") or ("8401539") or ("20100094754") or ("20100095130")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/02/27 09:46
L2	6	1 and biometric near9 (read$3 or scan$4)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:47
L3	8	1 and biometric and (read$3 or scan$4)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:47
L4	5	1 and fingerprint near9 (read$3 or scan$4)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:47
L5	9	1 and fingerprint and (read$3 or scan$4)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:48
L6	10	1 and fingerprint	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:48
L7	2	1 and biometric near9 (read$3 or scan$4) same (handheld or carrying or cellular or mobile or portable)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:53
L8	2	7 and (certificat$3 or money or transaction or exchang$3) same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:55
L9	2	7 and (award$3 or reward$3)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:57
L10	0	7 and cryptographic$4	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:58
L11	6	1 and cryptographic$4	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:58
L12	2	2 and 11	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:58

L13	2	12 and (certificat$3 or money or transaction or exchang$3) same biometric	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:59
L14	0	12 and (read$3 or scan$4) same (handheld or carrying or cellular or mobile or portable)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 09:59
L15	2	12 and (handheld or carrying or cellular or mobile or portable)	US-PGPUB; USPAT; USOCR	OR	ON	2014/02/27 10:00

EAST Search History (Interference)

<This search history is empty>

2/27/2014 10:05:44 AM
C:\Users\vtrieu\Documents\EAST\\default.wsp

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	14028469
Filing Date	2013-09-16
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	2685
Examiner Name	TRIEU, VAN THANH
Attorney Docket Number	116546-66001UT

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	8041815	B2	2011-10-18	Bahl et al.	
	2	7844505	B1	2010-11-30	Arneson et al.	
	3	7533809	B1	2009-05-19	Robinson et al.	
	4	7487538	B2	2009-02-03	Mok	
	5	7080819	B2	2006-07-25	Tojo	
	6	7031946	B1	2006-04-18	Tamai et al.	
	7	6975834	B1	2005-12-13	Forster	
	8	6950013	B2	2005-09-27	Scaman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	9	6894615	B2	2005-05-17	Look	
	10	6758405	B2	2004-07-06	Look	
	11	6753759	B2	2004-06-22	Stegmaier et al.	
	12	6698653	B1	2004-03-02	Diamond et al.	
	13	6617961	B1	2003-09-09	Janssen et al.	
	14	6570487	B1	2003-05-27	Steeves	
	15	6427504	B1	2002-08-06	Janssen et al.	
	16	6388579	B1	2002-05-14	Adcox et al.	
	17	6360208	B1	2002-03-19	Ohanian et al.	
	18	6340116	B1	2002-01-22	Cecil et al.	
	19	6334059	B1	2001-12-25	Stilp et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	20	6276607	B1	2001-08-21	Sato	
	21	6275157	B1	2001-08-14	Mays et al.	
	22	6269292	B1	2001-07-31	Kokubu et al.	
	23	6268796	B1	2001-07-31	Gnadinger et al.	
	24	6211790	B1	2001-04-03	Radomsky et al.	
	25	6203952	B1	2001-03-20	O'Brien et al.	
	26	6175922	B1	2001-01-16	Wang	
	27	6167333	A	2000-12-26	GEHLOT; NARAYAN L. et al.	
	28	6157333	A	2000-12-05	Louagie et al.	
	29	6140941	A	2000-10-31	Dwyer et al.	
	30	6111506	A	2000-08-29	YAP; CHAS HOCK ENG et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	31	6104281	A	2000-08-15	HEINRICH; HARLEY KENT et al.	
	32	6098879	A	2000-08-08	TERRANOVA; STEVEN N. et al.	
	33	6073840	A	2000-06-13	MARION; KENNETH O. et al.	
	34	6052068	A	2000-04-18	PRICE R et al.	
	35	6025784	A	2000-02-15	Mish	
	36	6025780	A	2000-02-15	BOWERS; JOHN H. et al.	
	37	5974500	A	1999-10-26	MALETSKY; KERRY D. et al.	
	38	5874896	A	1999-02-23	SMALL et al.	
	39	5864580	A	1999-01-26	Lowe et al.	
	40	5787174	A	1998-07-28	TUTTLE JOHN R	
	41	5742618	A	1998-04-21	Lowe	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	42	5657008	A	1997-08-12	Bantli	
	43	5552789	A	1996-09-03	Schuermann	
	44					

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	20050149764	A1	2005-07-07	Bahl et al.	
	2	20030200227	A1	2003-10-23	Ressler	
	3	20020089434	A1	2002-07-11	Ghazarian	
	4					

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	1	2004006165	WO	A1	2004-01-15	CORTINA		☐
	2	2002042076	JP	A	2002-02-08	NISHIKAWA SEIICHI		☐
	3	19608757	DE	A1	1997-09-11	NICHTNENNUNG		☐
	4	10042805	DE	A1	2002-03-14	LANGENSTUECK HOLGER		☐
	5	9843104	WO	A2	1998-10-01	PRICE FREDERICK J R-W		☐
	6	993999	EP	A2	2000-04-19	Gilmore		☐
	7	977145	EP	A2	2000-02-02	Karasawa		☐
	8							☐

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, Solution Making Smart Cards Smarter, 2000, 12 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	2	Extended European Search Report issued by the European Patent Office in related European Application No. 10182033.0 dated Jan. 13, 2012 (7 pages).	☐
	3	FANCHER, Carol Hovenga, In Your Pocket Smartcards, IEEE Spectrum, February 2007, 7 pages.	☐
	4	RAKERS, Patrick, et al., Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal Of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	☐
	5	Official Action in Japanese Patent Application No. 2004-519130 dated May 12, 2009, 10 pages.	☐
	6	Anonymous, Read Write RFID Offers Standalone Advantages, Security, August 1996, 1 page.	☐
	7	21 C.C.R. §1700	☐
	8	21 C.C.R. § 1701(r)	☐
	9	21 C.C.R. § 1702.1	☐
	10	21 C.C.R. § 1703(c)	☐
	11	21 C.C.R. § 1703(e-i)	☐
	12	21 C.C.R. § 1704.1	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

	13	21 C.C.R. § 1704.2	☐
	14	21 C.C.R. § 1704.3	☐
	15	21 C.C.R. § 1704.5(e)(1)	☐
	16	21 C.C.R. § 1704.6	☐
	17	21 C.C.R. § 1705.1	☐
	18	21 C.C.R. § 1705.2	☐
	19	21 C.C.R. § 1705.3	☐
	20	21 C.C.R. § 1705.4	☐
	21	21 C.C.R. § 1705.5	☐
	22	21 C.C.R. § 1705.5(d) and (e)(1)	☐
	23	21 C.C.R. 1705.8	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

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	14028469
	Filing Date	2013-09-16
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-66001UT

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	/ F.G. Plati /	Date (YYYY-MM-DD)	2014-02-28
Name/Print	Francis G. Plati, Sr.	Registration Number	59153

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 Alsterberg 10, 87616 Marktoberdorf (DE).

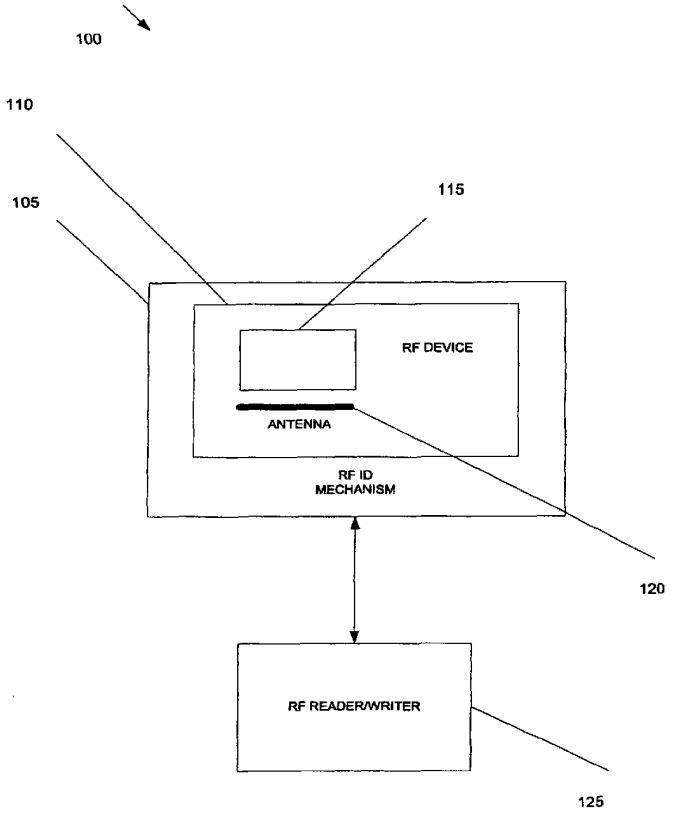
(74) Agent: **MIDGLEY, Jonathan, Lee**; Marks & Clerk, 57-60 Lincolns Inn Fields, London, WC2A 3LS (GB).

(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).

D. 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:

$$L_1 = 2.931 \times 10^{8} H$$
$$L_2 = 6.437 \times 10^{12} H$$

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

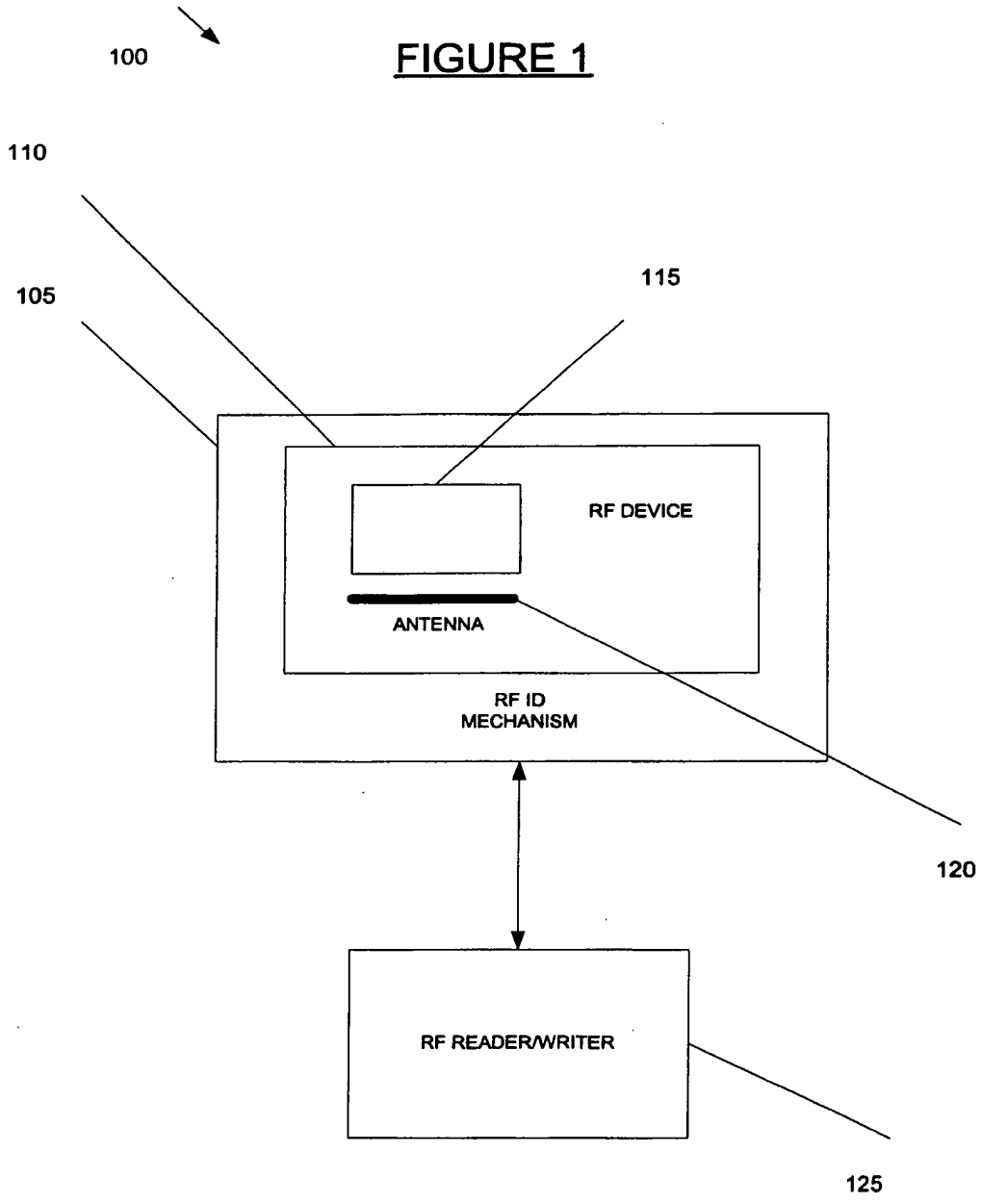

100
110
105
115
RF DEVICE
ANTENNA
RF ID
MECHANISM
120
RF READER/WRITER
125

FIGURE 2

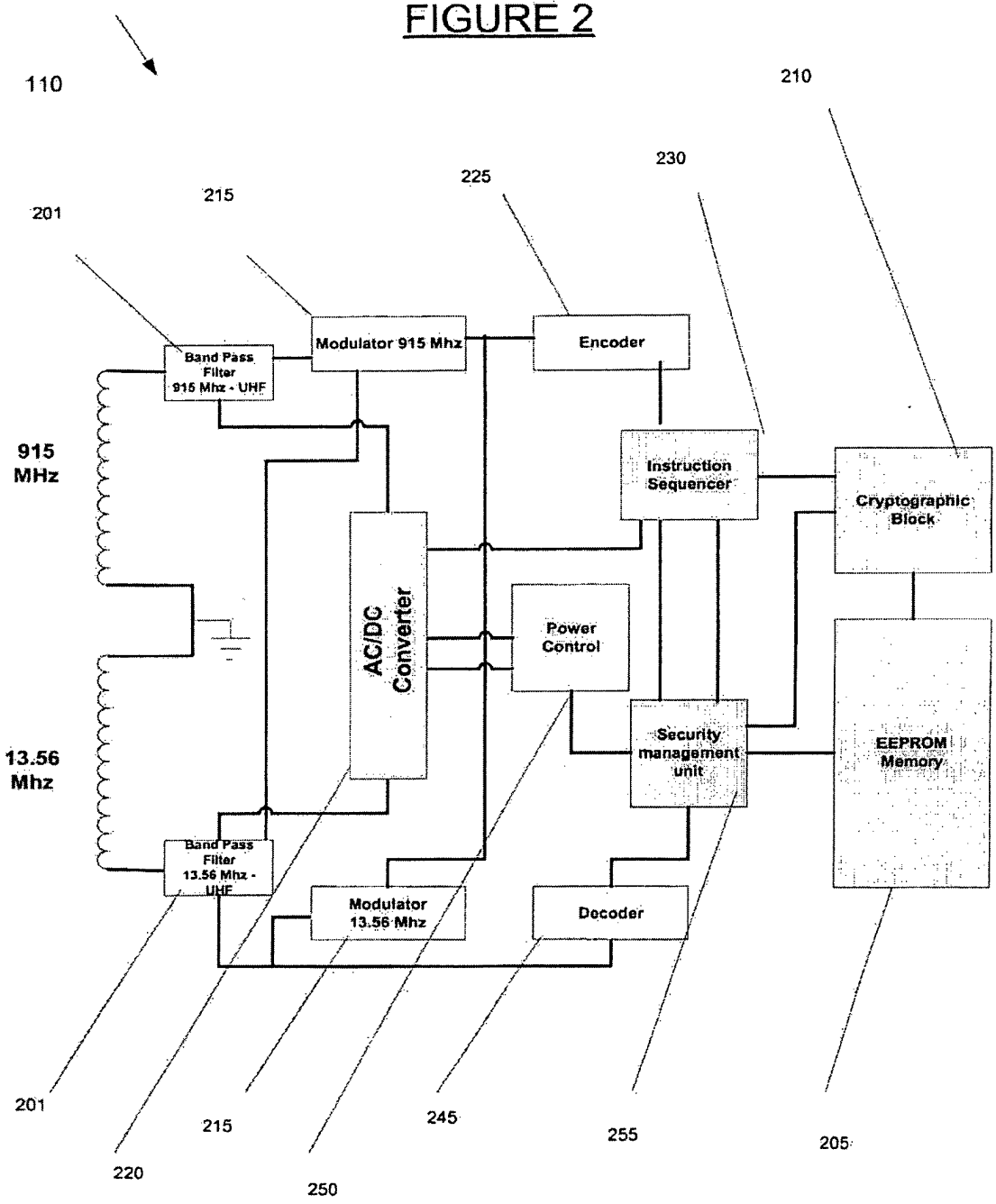

110
210
230
225
215
201
Band Pass Filter 915 Mhz - UHF
Modulator 915 Mhz
Encoder
915 MHz
Instruction Sequencer
Cryptographic Block
AC/DC Converter
Power Control
13.56 Mhz
Security management unit
EEPROM Memory
Band Pass Filter 13.56 Mhz - UHF
Modulator 13.56 Mhz
Decoder
201
215
245
255
205
220
250

FIGURE 3A

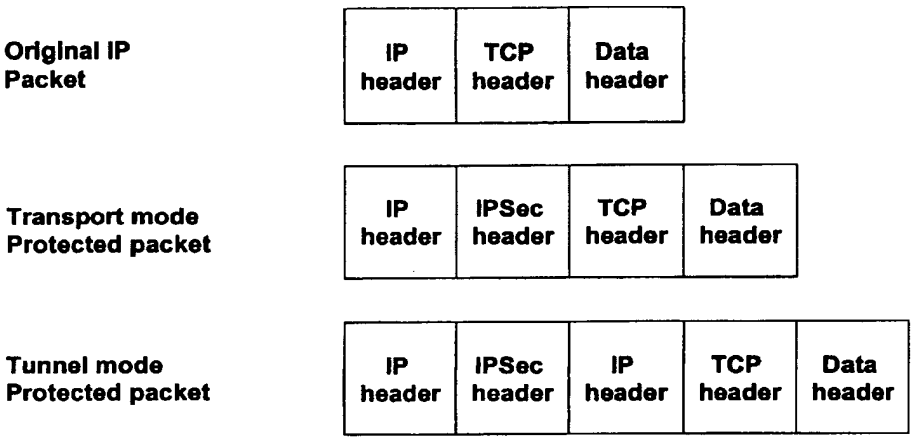
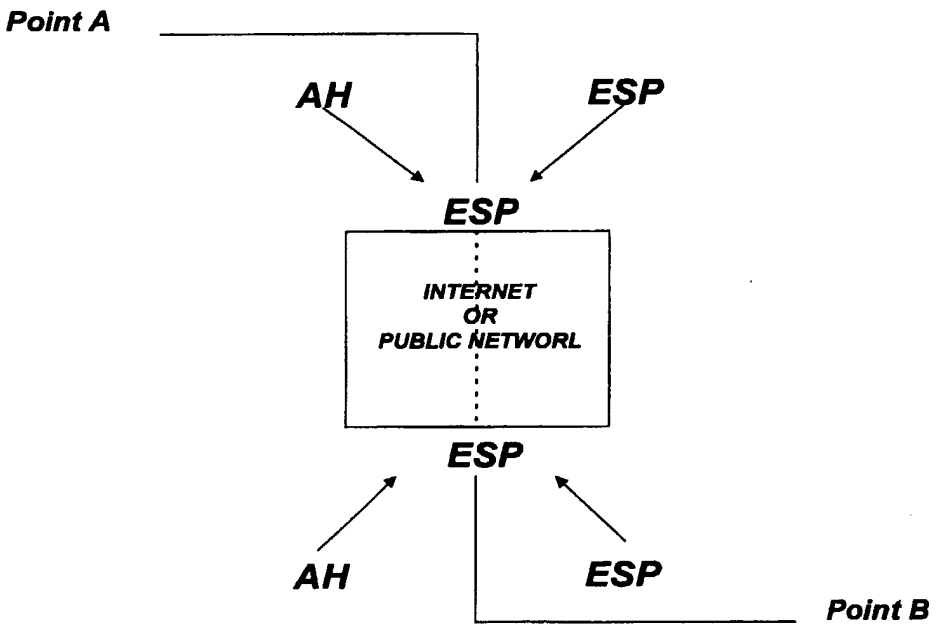

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIGURE 3B


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

400

FIGURE 4

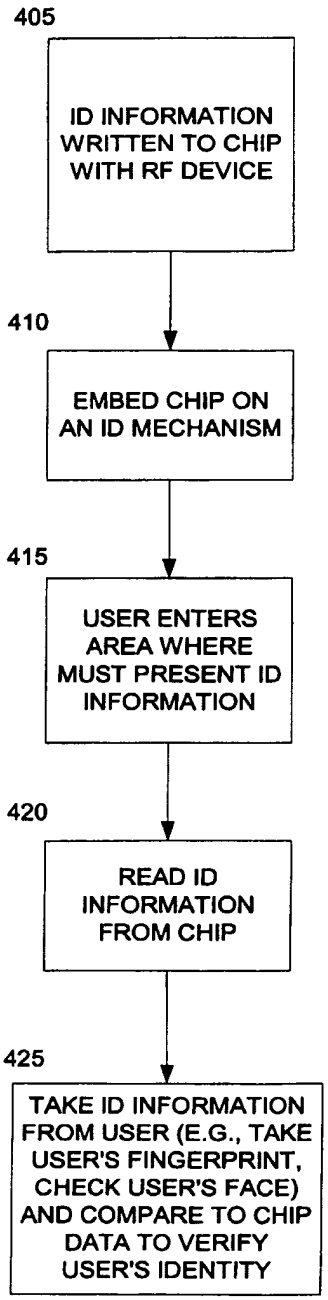

405
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
410
EMBED CHIP ON AN ID MECHANISM
415
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
420
READ ID INFORMATION FROM CHIP
425
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 5

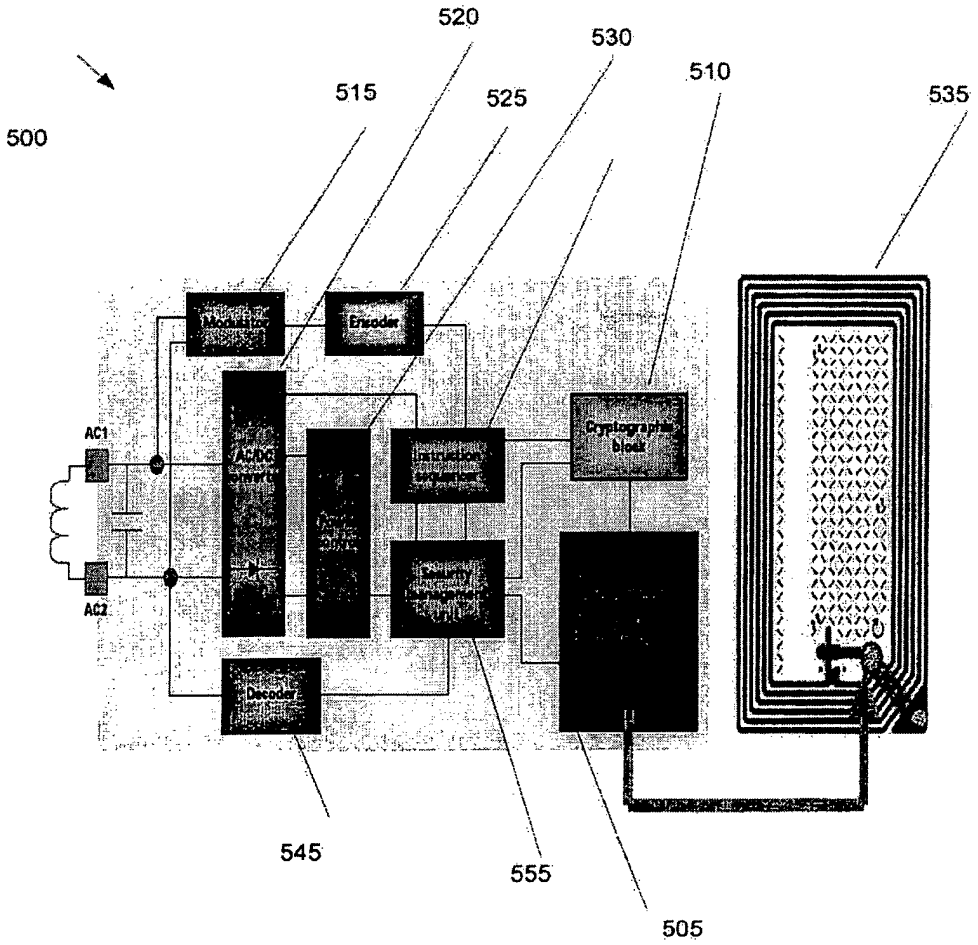

500
520
530
510
515
525
535
Encoder
AC1
AC2
Cryptographic block
Decoder
545
555
505

FIGURE 6

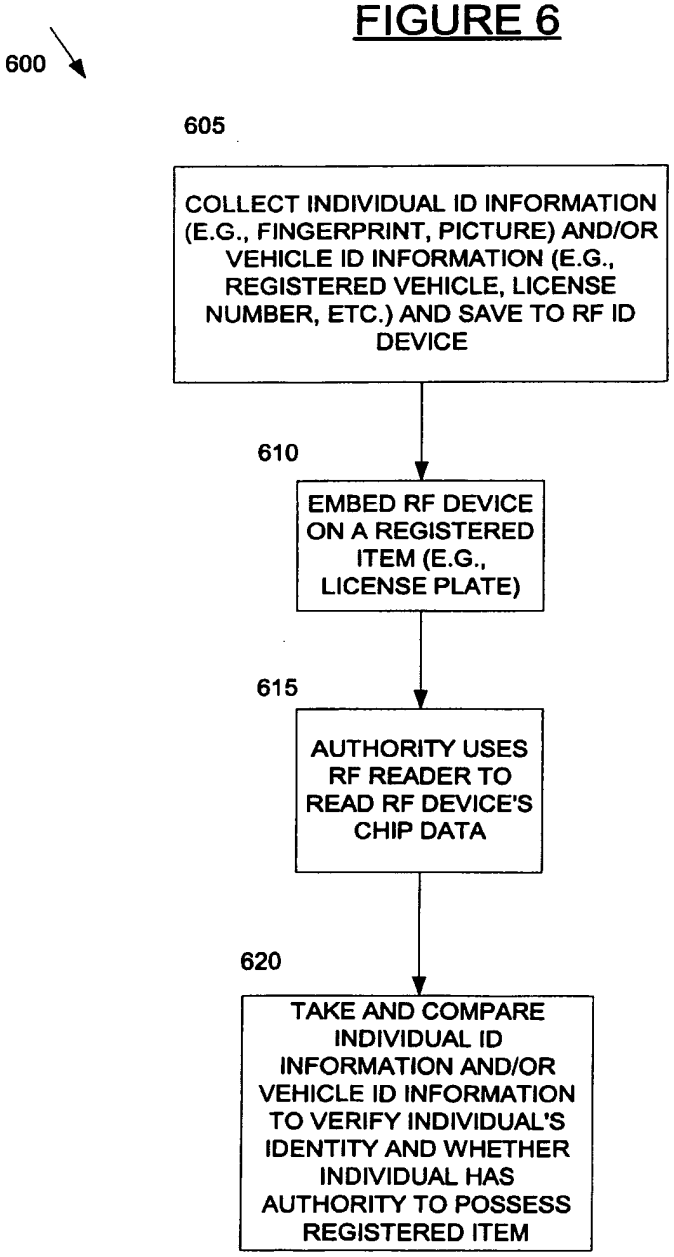

600
605
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
610
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
615
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
620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

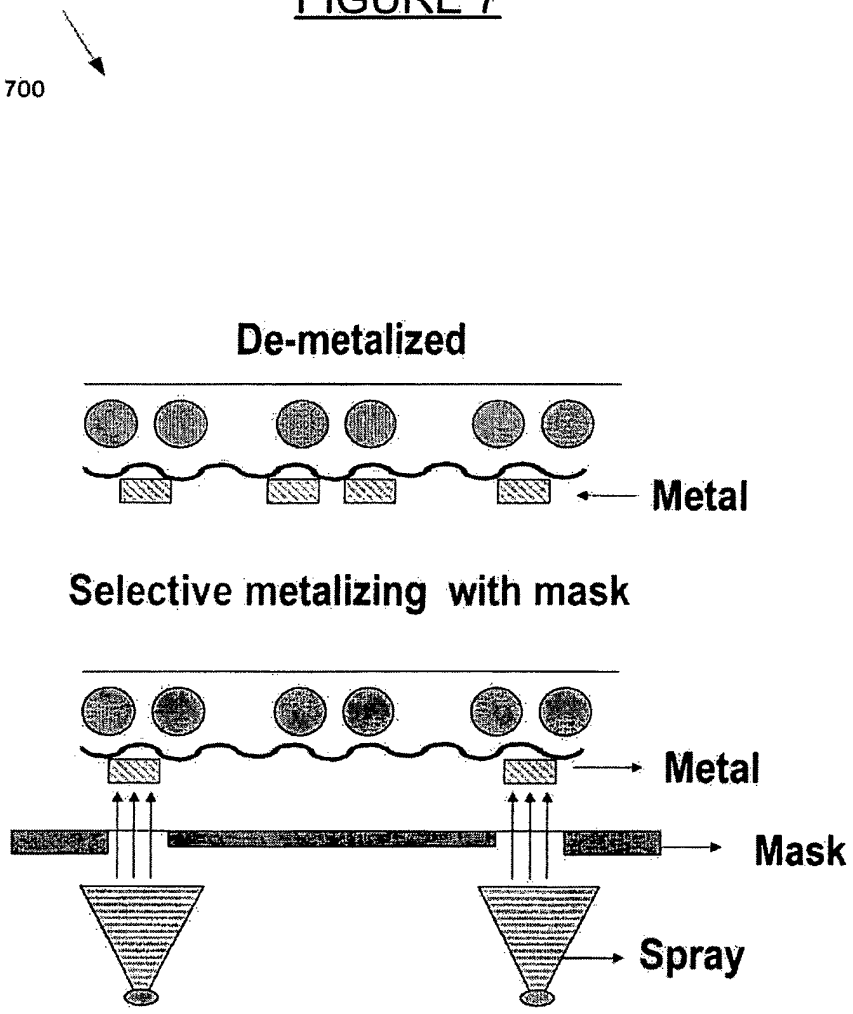

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIGURE 8

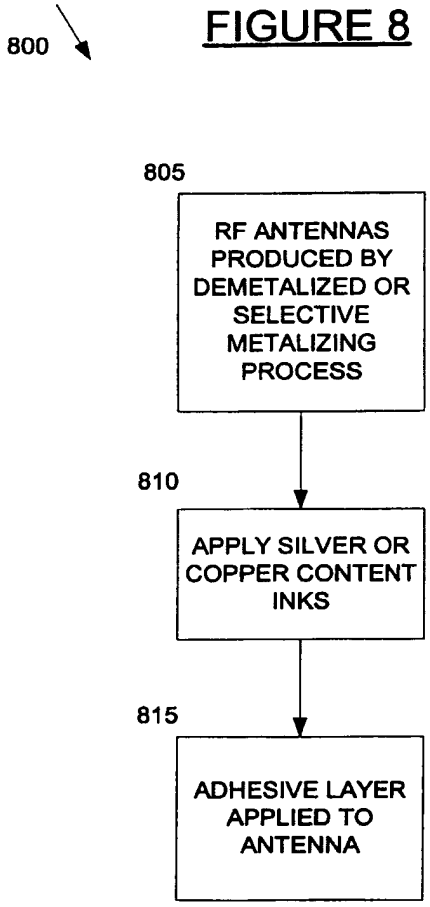

800
805
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
810
APPLY SILVER OR COPPER CONTENT INKS
815
ADHESIVE LAYER APPLIED TO ANTENNA

FIGURE 9

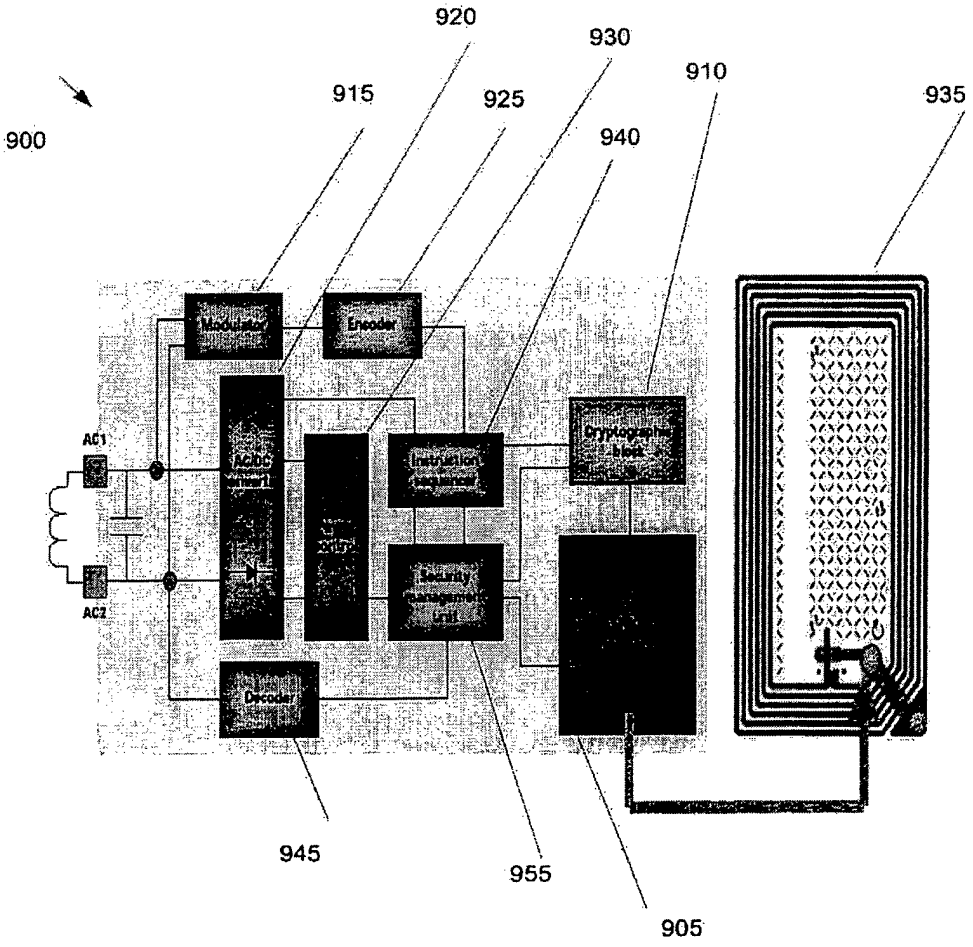


FIGURE 10

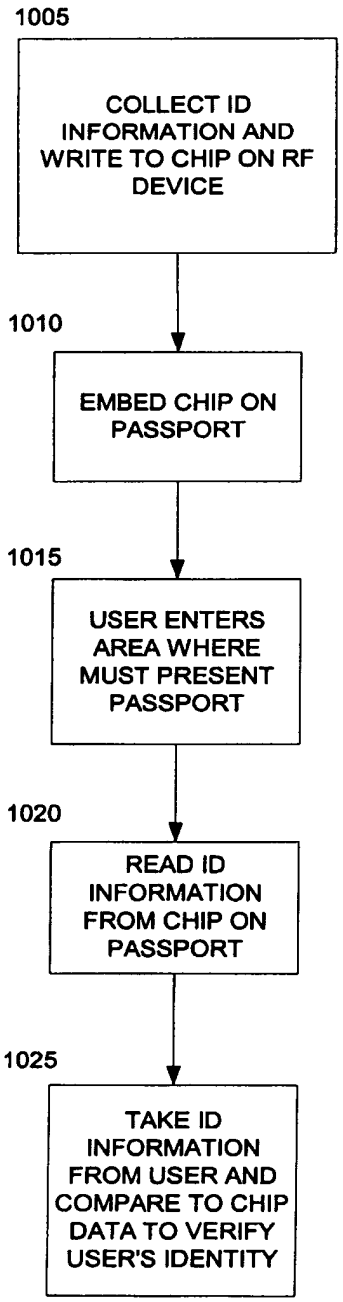

1005
COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1010
EMBED CHIP ON PASSPORT
1015
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1020
READ ID INFORMATION FROM CHIP ON PASSPORT
1025
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 11

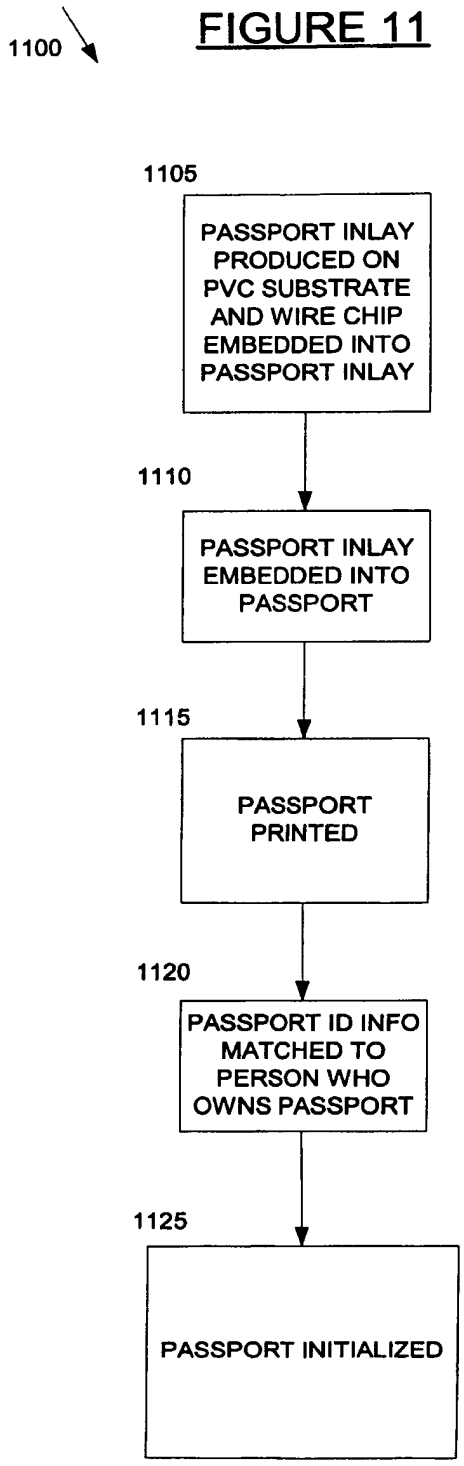

1100
1105
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1110
PASSPORT INLAY EMBEDDED INTO PASSPORT
1115
PASSPORT PRINTED
1120
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1125
PASSPORT INITIALIZED

FIGURE 12

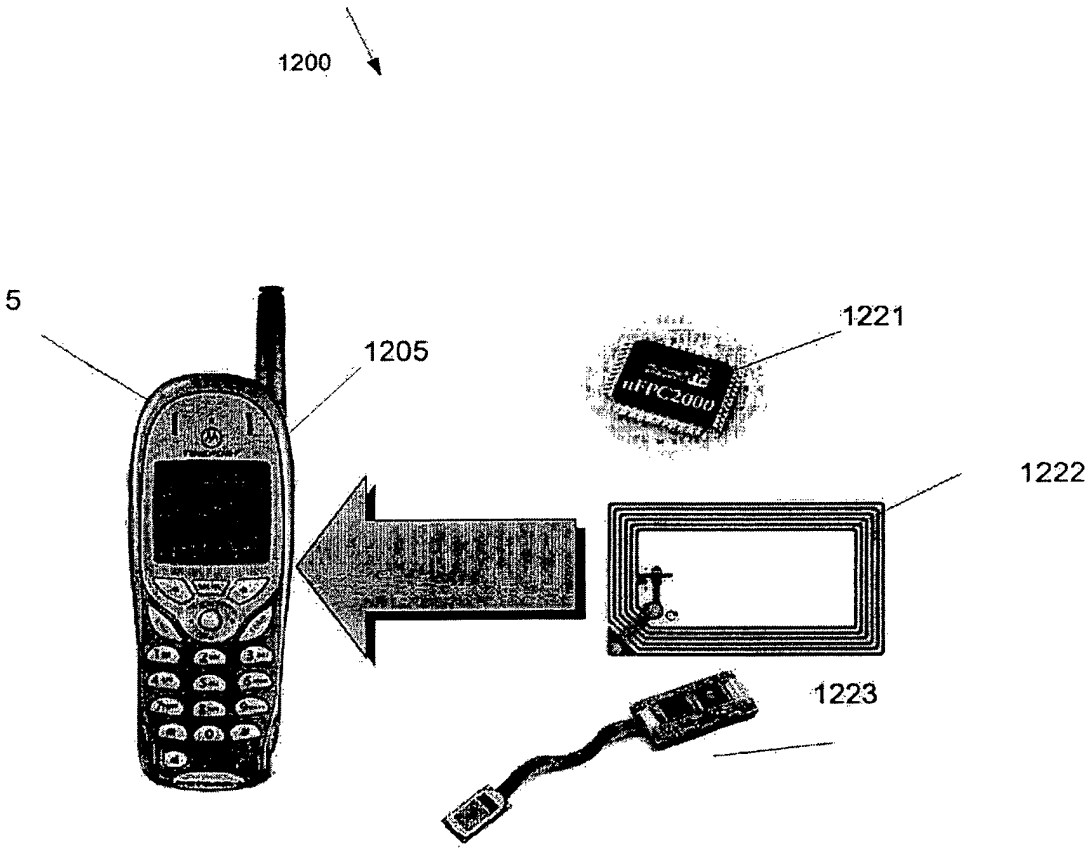


FIGURE 13

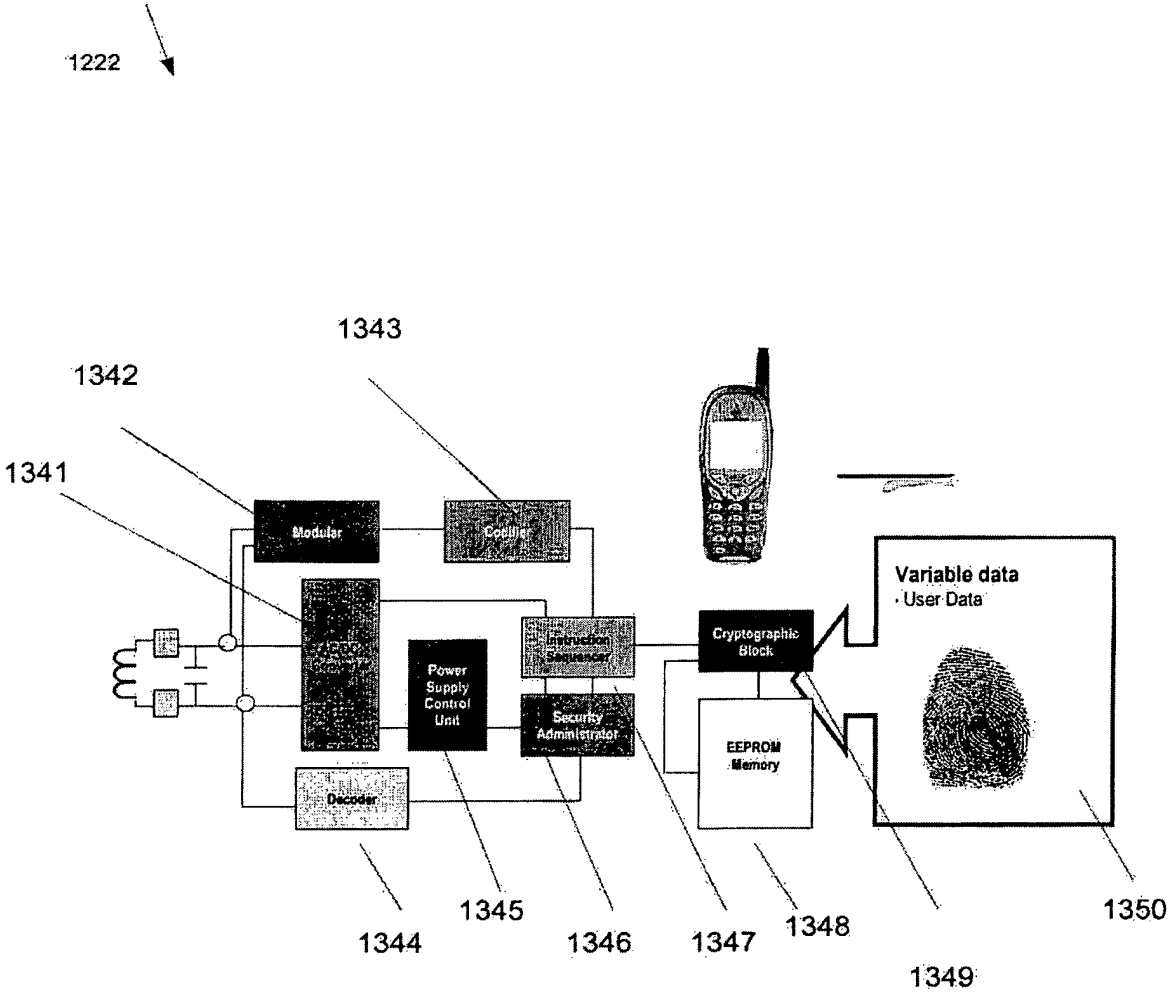

1222
1343
1342
1341
Modular
Coding
Variable data
User Data
Power Supply Control Unit
Instruction Sequencer
Cryptographic Block
Security Administrator
EEPROM Memory
Decoder
1344
1345
1346
1347
1348
1349
1350

FIGURE 14

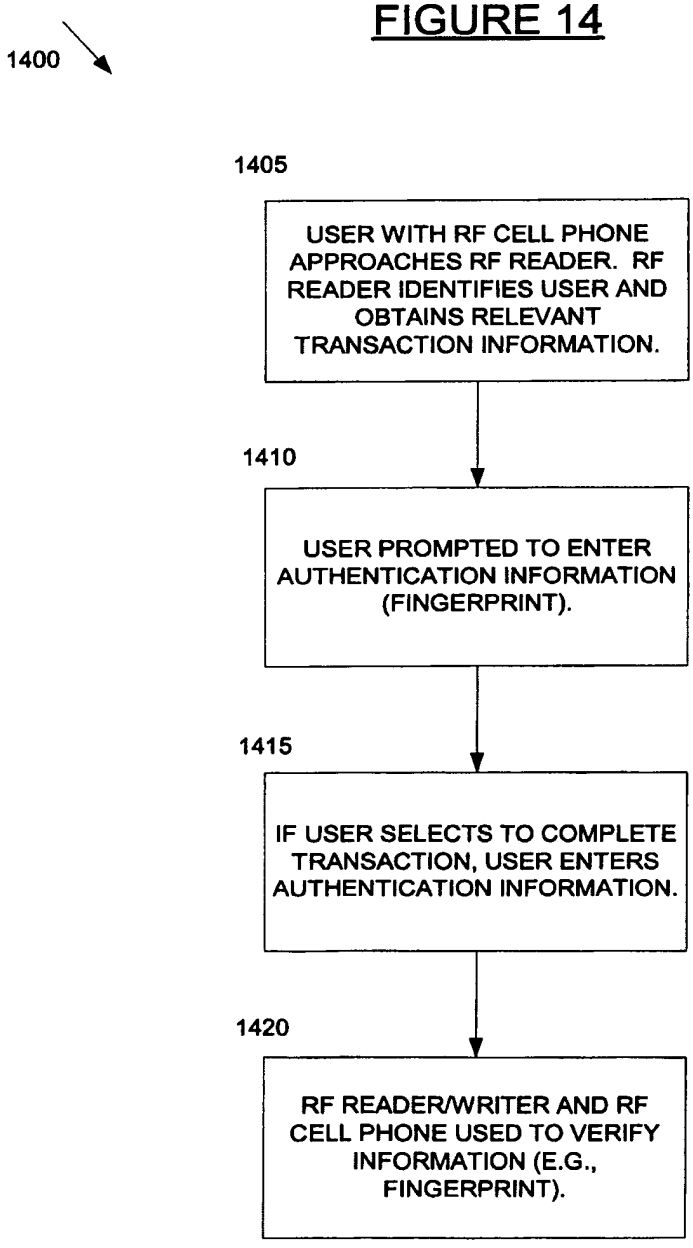

1400
1405
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION.
1410
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT).
1415
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION.
1420
RF READER/WRITER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

FIGURE 15

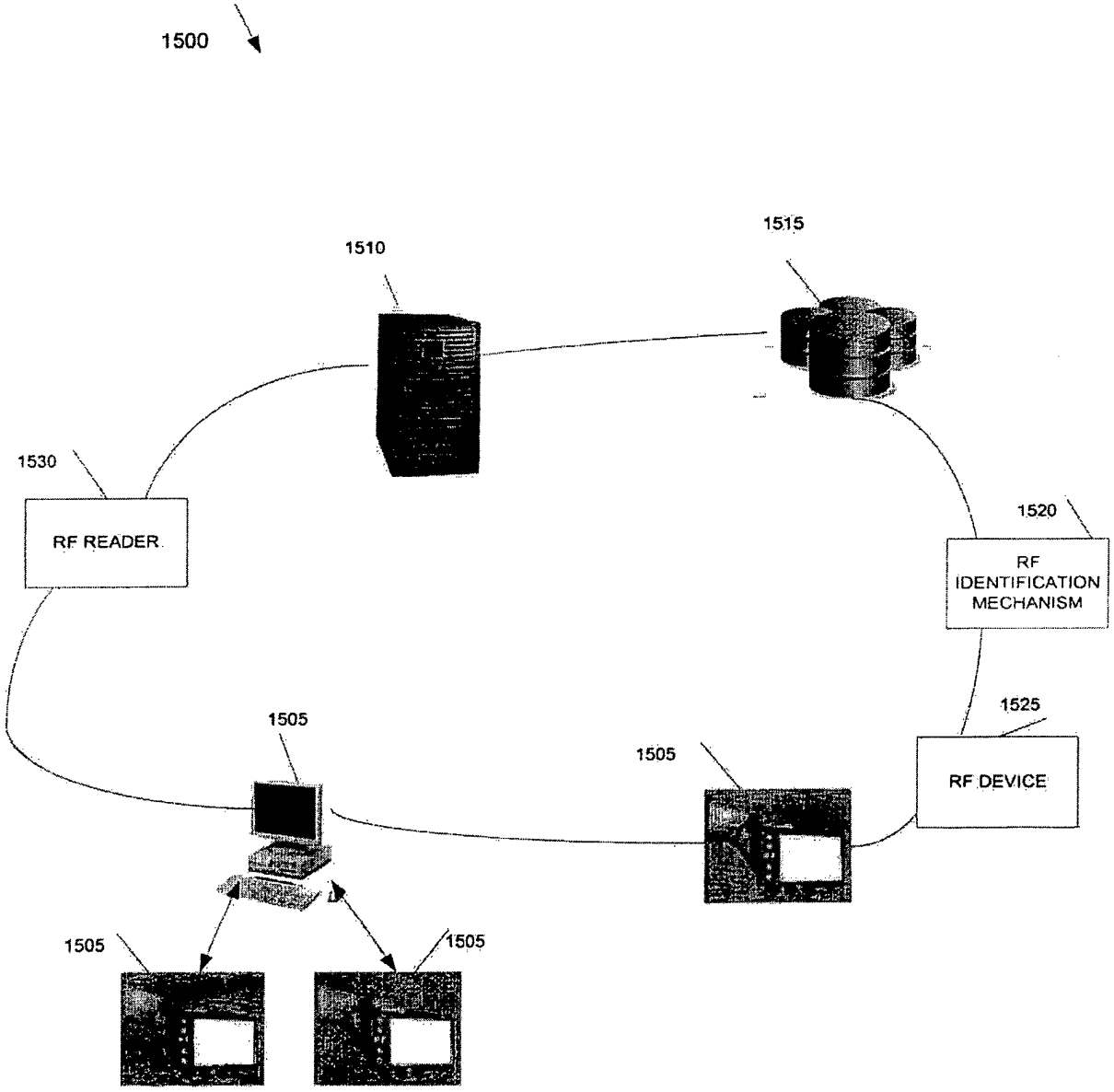

1500
1510
1515
1530
RF READER
1520
RF IDENTIFICATION MECHANISM
1525
RF DEVICE
1505
1505
1505
1505

FIGURE 16

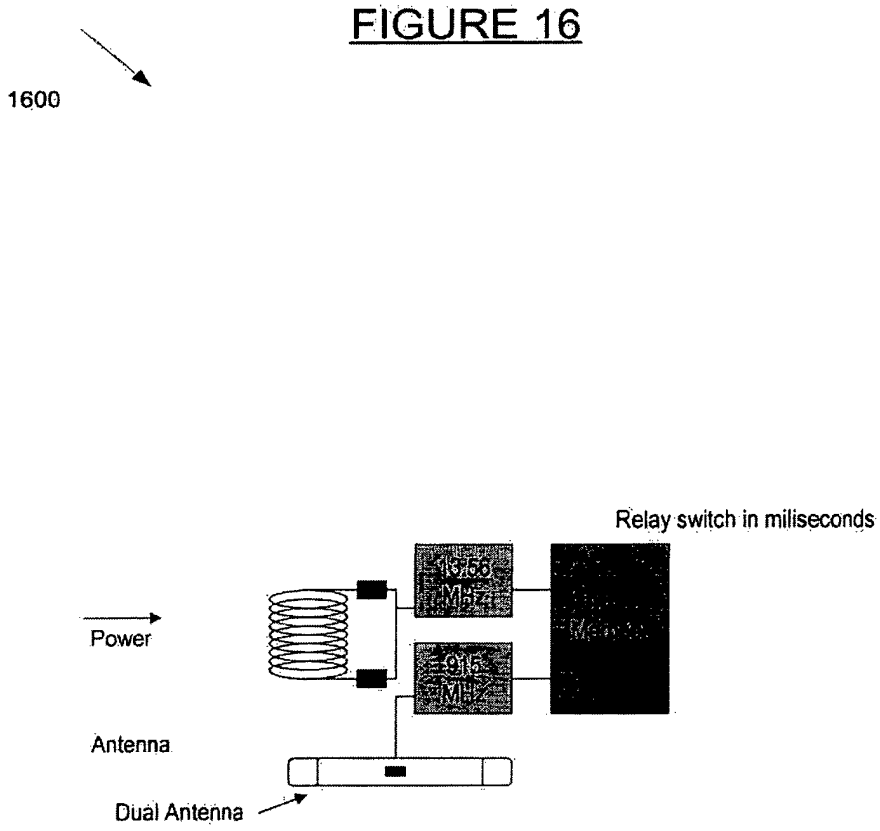

1600
Relay switch in miliseconds
Power
Antenna
Dual Antenna

FIGURE 17

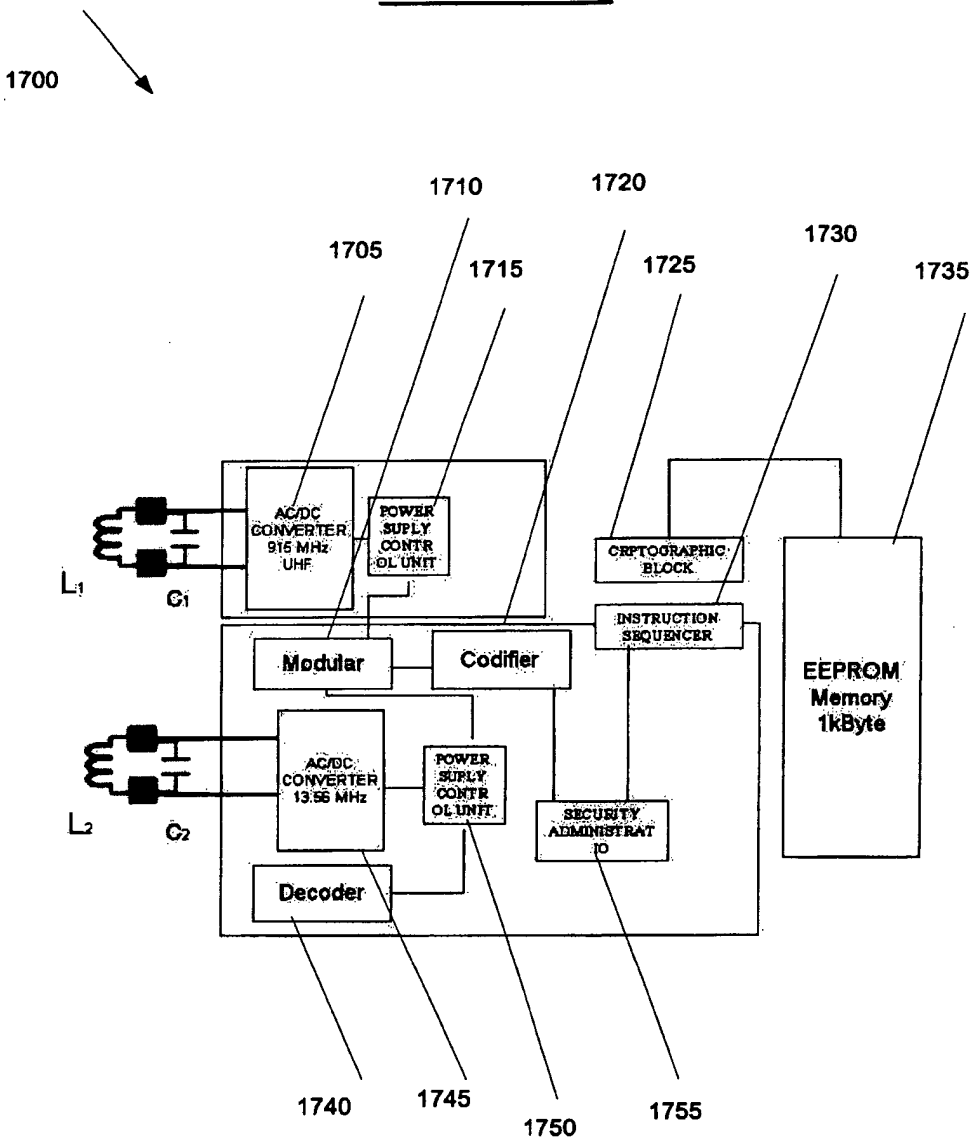

1700
1710
1720
1705
1715
1725
1730
1735
AC/DC CONVERTER 915 MHz UHF
POWER SUPLY CONTR OL UNIT
CRPTOGRAPHIC BLOCK
INSTRUCTION SEQUENCER
L1
C1
Modular
Codifier
EEPROM Memory 1kByte
AC/DC CONVERTER 13.56 MHz
POWER SUPLY CONTR OL UNIT
SECURITY ADMINISTRAT IO
L2
C2
Decoder
1740
1745
1750
1755

FIGURE 18

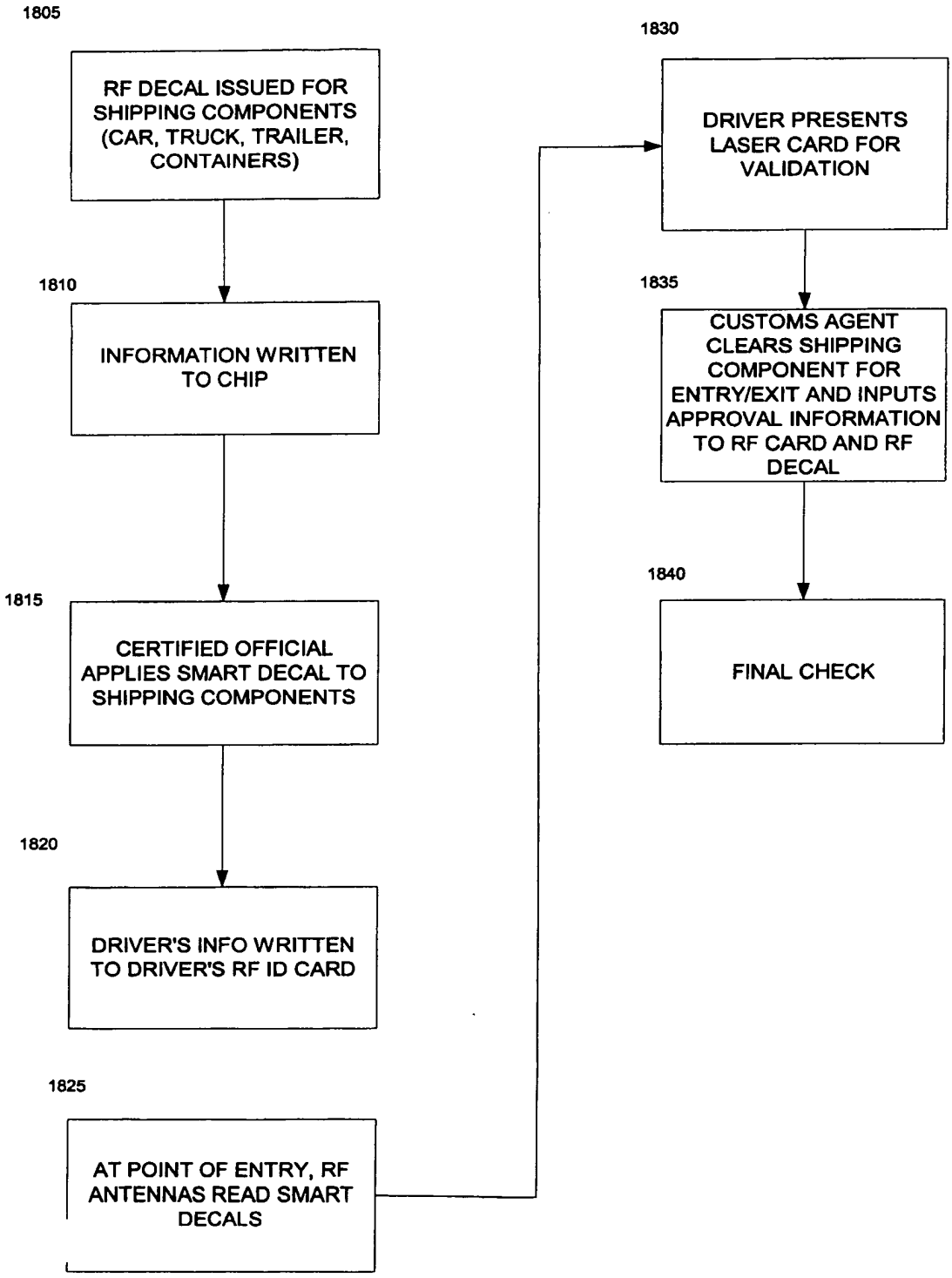

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS 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

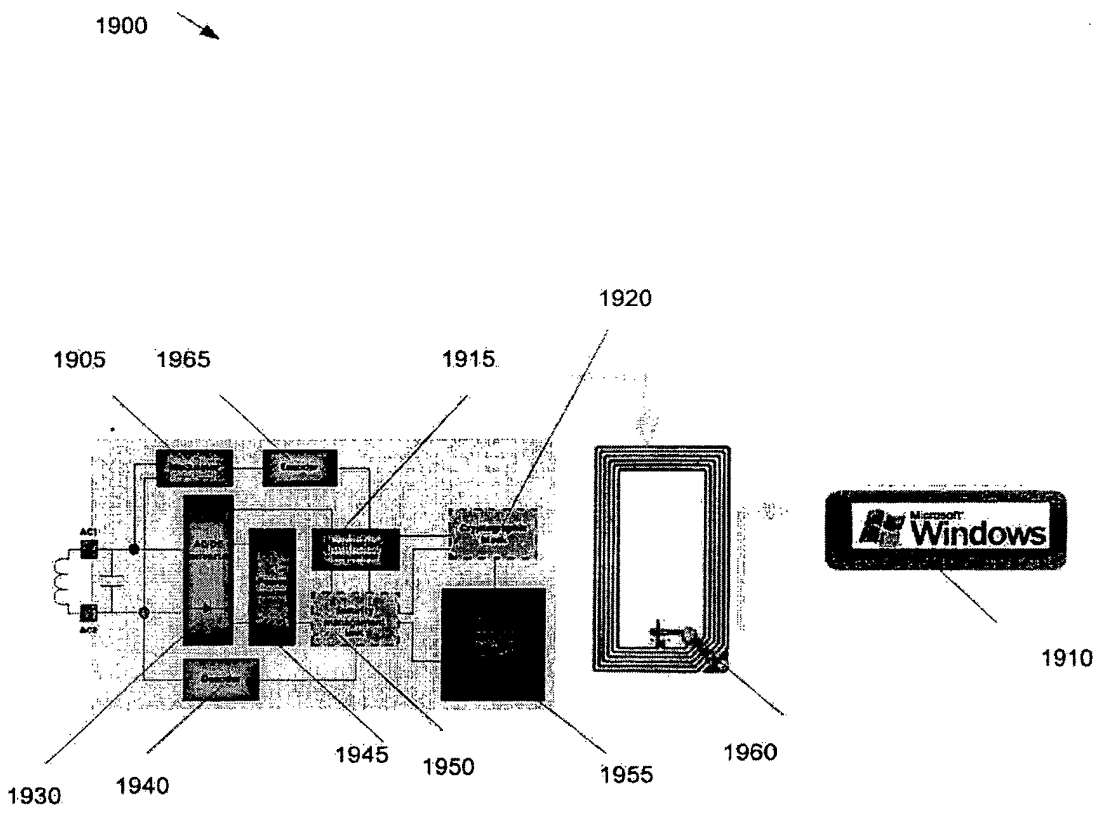
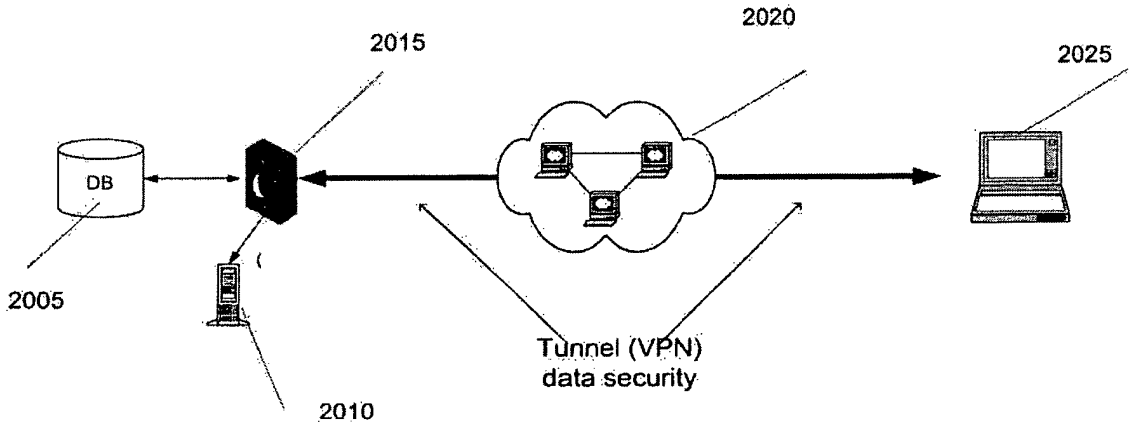


FIGURE 20



2100

FIGURE 21

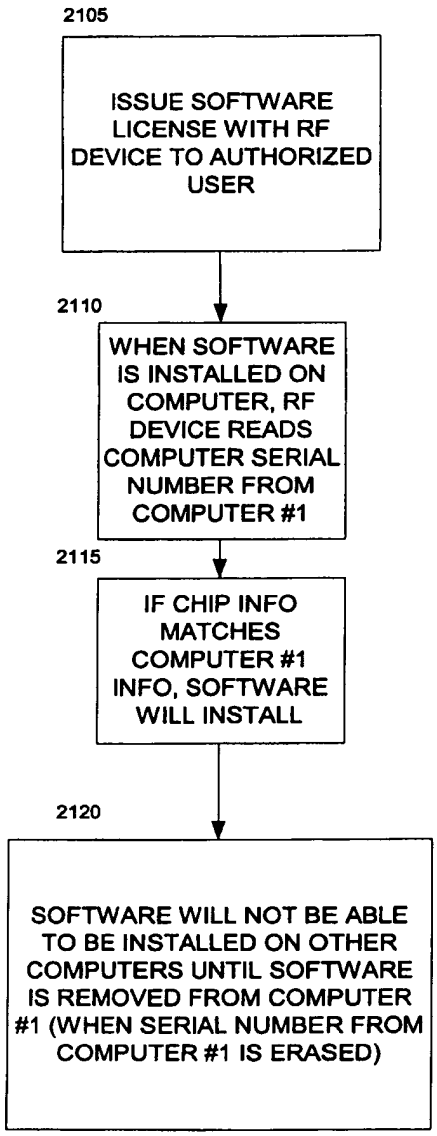


FIGURE 22

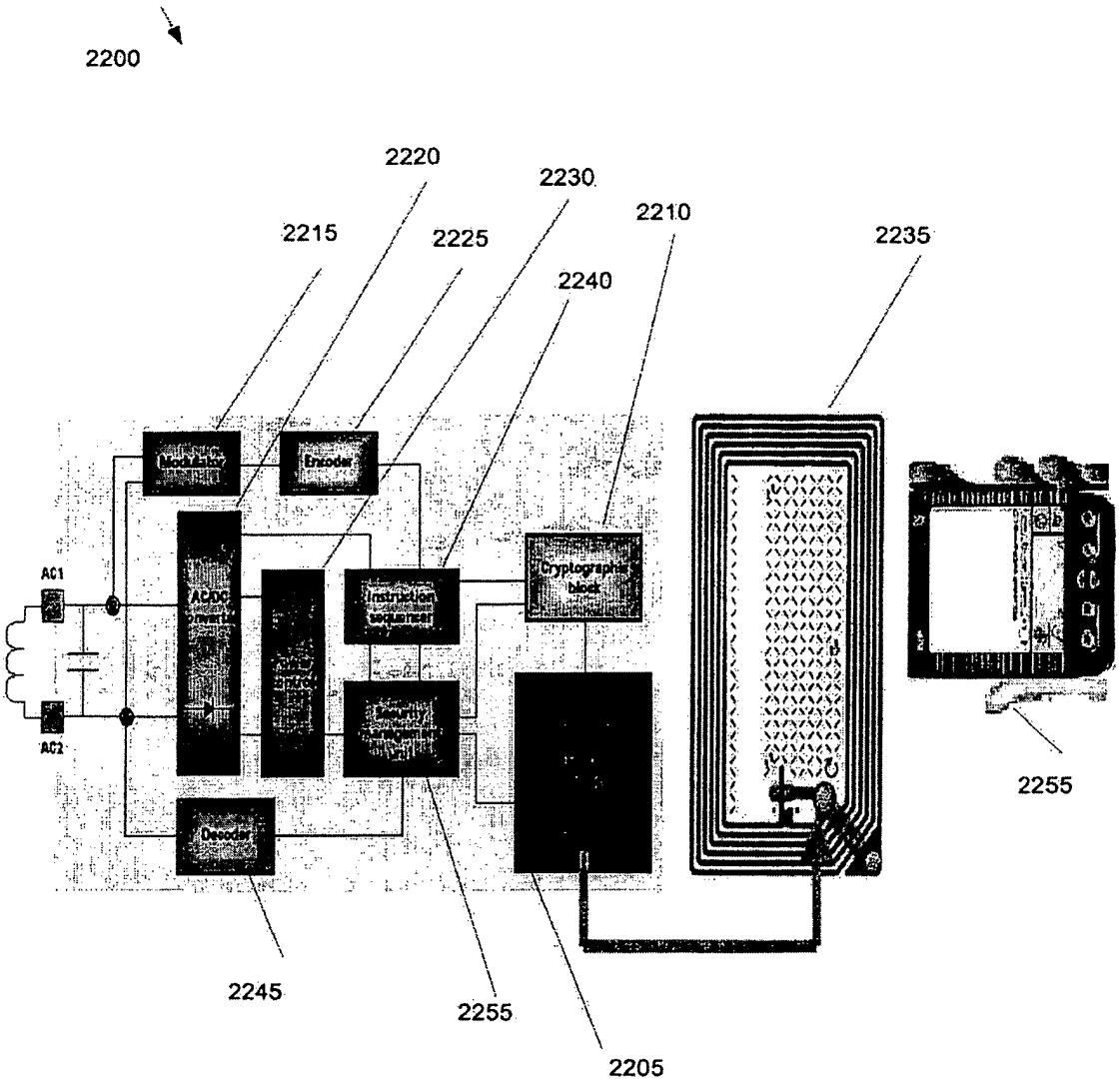
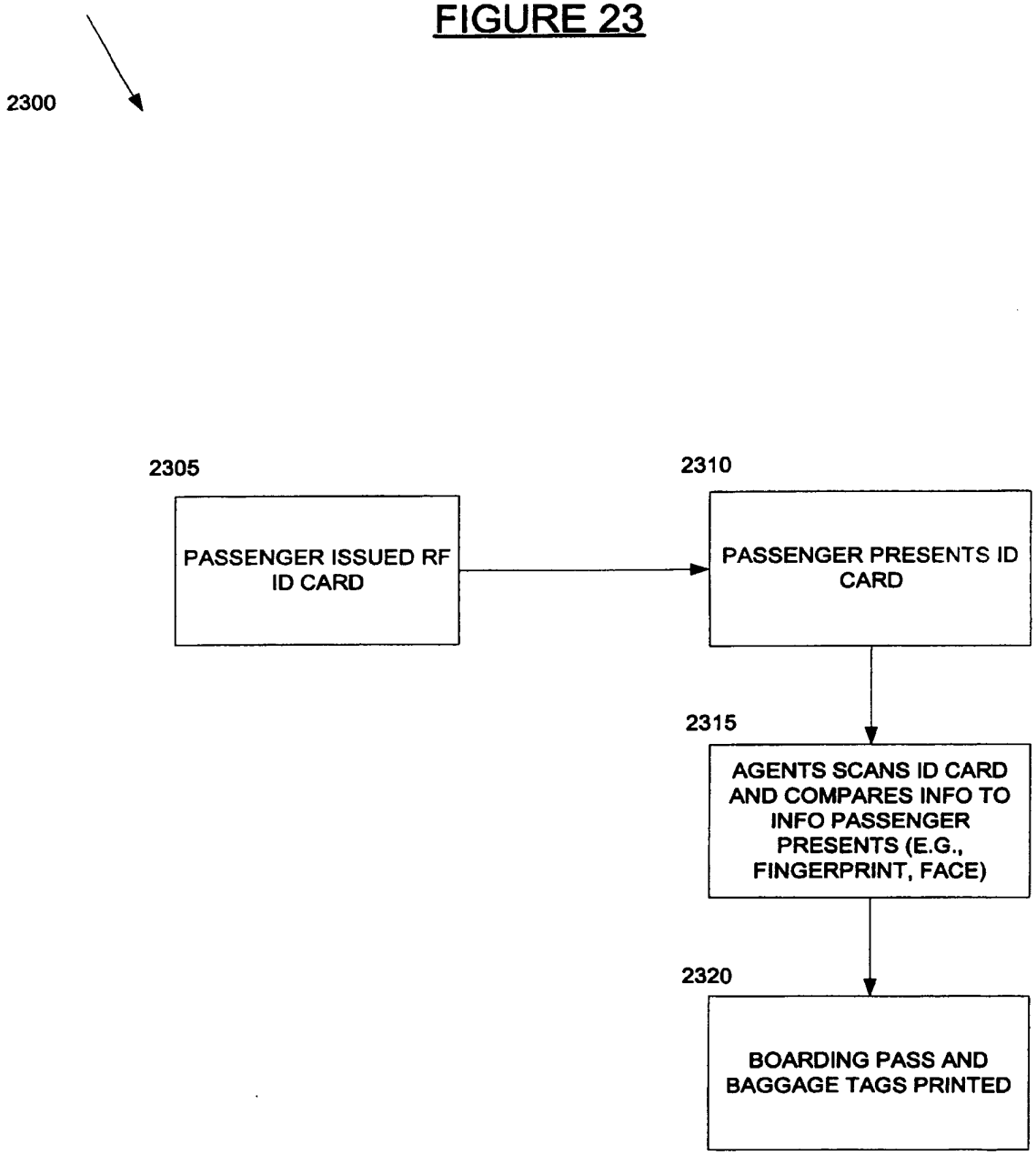

2200
2220
2230
2210
2215
2225
2235
2240
Encoder
Instruction sequencer
Cryptographic block
AC1
AC2
Decoder
2255
2245
2255
2205

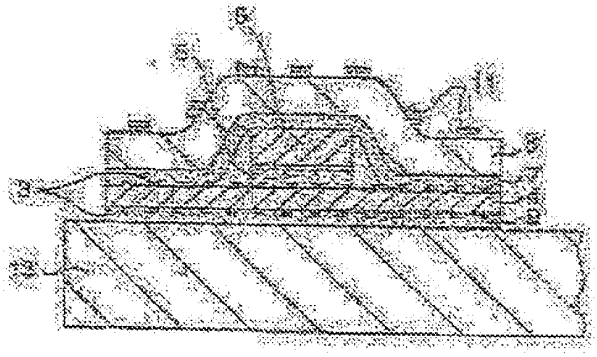
FIGURE 23


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

NON-CONTACT DATA CARRIER AND BOOKLET THEREWITH

Publication number: JP2002042076 (A)
Publication date: 2002-02-08
Inventor(s): NISHIKAWA SEIICHI
Applicant(s): DAINIPPON PRINTING CO LTD
Classification:
- international: *B42D15/10; B42D11/00; G06K19/00; G06K19/07; G06K19/077; G07D9/00;* B42D15/10; B42D11/00; G06K19/00; G06K19/07; G06K19/077; G07D9/00; (IPC1-7): G06K19/07; B42D11/00; B42D15/10; G06K19/00; G06K19/077; G07D9/00
- European:
Application number: JP20000220336 20000721
Priority number(s): JP20000220336 20000721

Abstract of JP 2002042076 (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.



Data supplied from the *esp@cenet* database — Worldwide

DE19608757

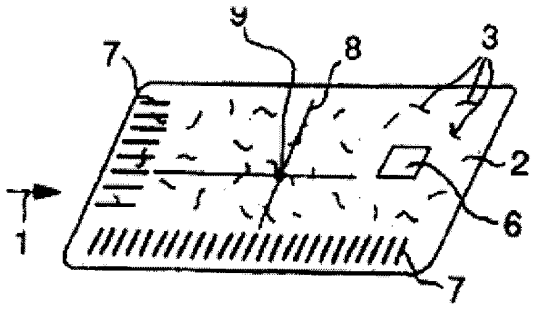
Patent number: DE19608757
Publication date: 1997-09-11
Inventor:
Applicant: BROSOW JOERGEN (AT)
Classification:
- international: ***G06K19/10;*** **G06K19/10;** (IPC1-7): G07D7/00; G07F7/12
- european: G06K19/10
Application number: DE19961008757 19960306
Priority number(s): DE19961008757 19960306; DE19961008233 19960304

Also published as:
WO9733252 (A1)

Report a data error here

Abstract of **DE19608757**

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.



Data supplied from the ***esp@cenet*** database - Worldwide

(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

INTELLECTUAL PROPERTY OFFICE

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] ±	
Applicant(s):	BUNDESDRUCKEREI GMBH [DE] ±	
Classification:	**- international:**	***B60R25/00; B60R25/10; B63J99/00; B64D45/00; G08B13/24;*** (IPC1-7): B60R25/00; B63B45/00; B64D45/00; G08B13/00
	- european:	B60R25/00; B60R25/10D2; B63J5/00; B64D45/00H; G08B13/24B
Application number:	DE20001042805 20000830	
Priority number (s):	DE20001042805 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.

Last updated: 5.12.2011 Worldwide Database 5.7.31; 92p

(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 **6a** und **7a** eine elektrisch leitende Verbindung zwischen dem einen Ende der Antenne **3** und dem einen Ende des Mikrochips **2** und bewirkt in den Bereichen **6b** und **7b** 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 (Ex), 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 Satellit (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

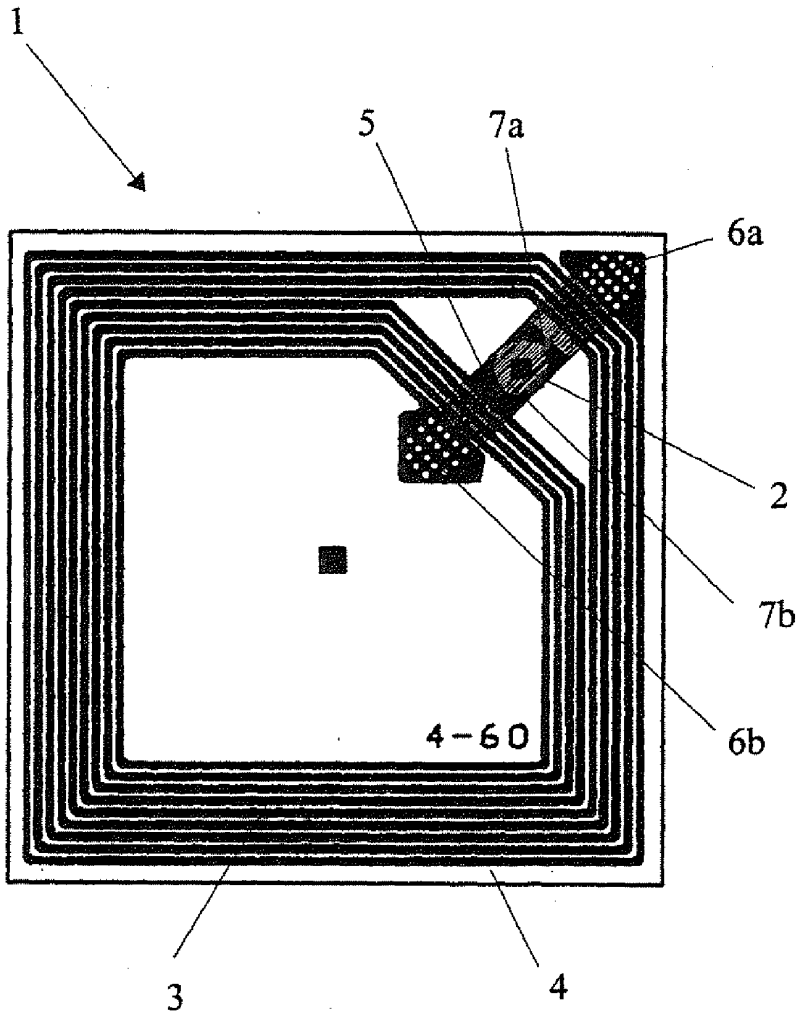


FIG. 1

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

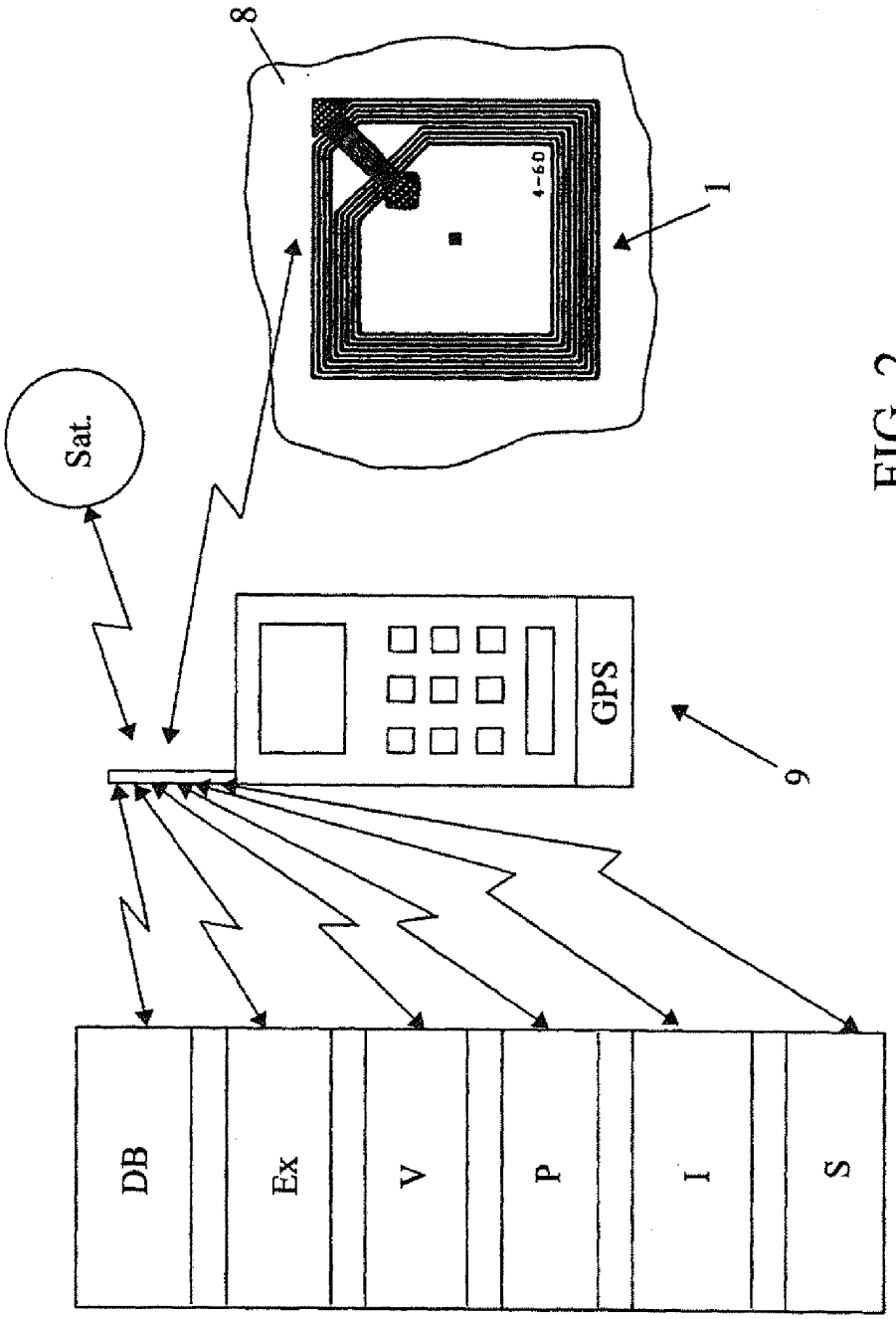


FIG. 2

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

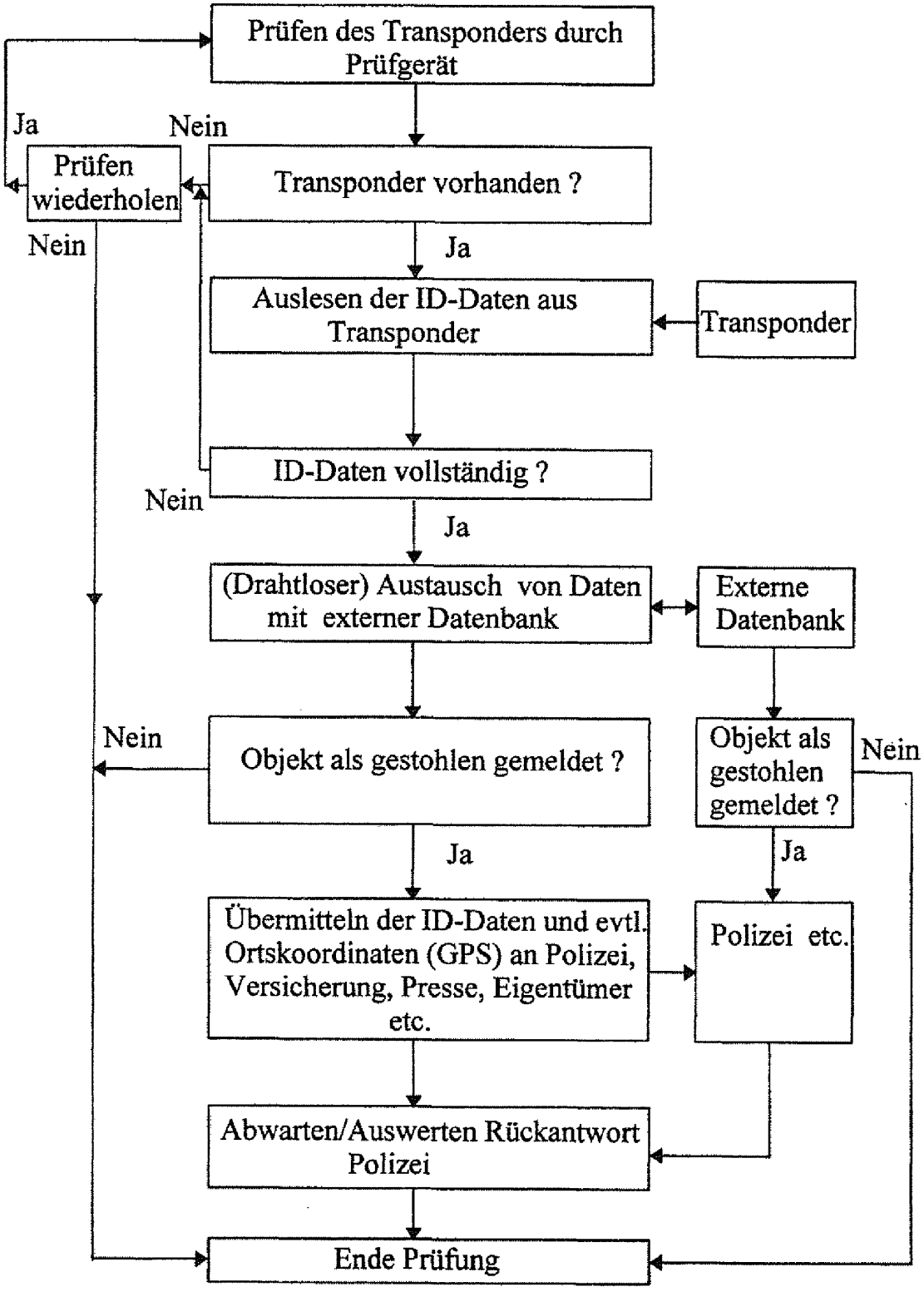


FIG. 3

101 710/436

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **G08G 1/01**	**A3**	**(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).

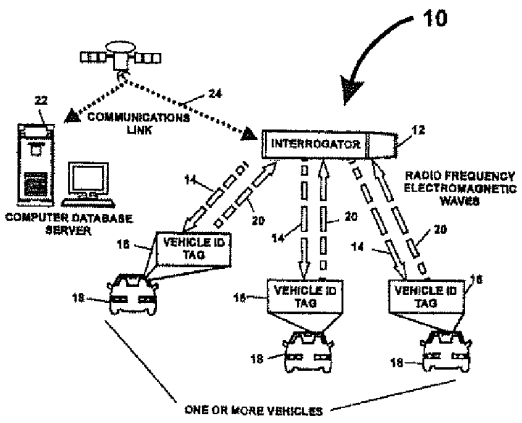
(74) Agents: CAYWOOD, Michael et al.; Locke Purnell Rain Harrell, Suite 300, 100 Congress Avenue, Austin, TX 78701 (US).

(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
With international search report.

(88) Date of publication of the international search report:
30 December 1998 (30.12.98)

(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 (10) includes an interrogator (12) for directionally broadcasting an interrogation signal toward a vehicle (18) of interest and a set of vehicle identification tags (16) 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 (16) which allows the interrogator (12) to identify the ownership or registration of the vehicle (18). Each tag (16) on the vehicle also communicates with the other tags (16) in the tag set on a vehicle (18), 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 (12).

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		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/05686

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G08G 1/01
US CL :340/933

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/933

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

Please See Extra Sheet.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X __,P Y	US 5,686,902 A (REIS ET AL.) 11 November 1997, SEE ABSTRACT, FIGS. 2,4, COL.1 LINES 25-45;	1,19-24, 2-12,32-37,
Y	US 5,459,304 A (EISENMASNN) 17 October 1995, SEE ABSTRACT	2-12

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 JUNE 1998	Date of mailing of the international search report 13 OCT 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Nina Tong Telephone No. (703) 305-4831

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

BNSDOCID: <WO_____9843104A3_I_>

B. FIELDS SEARCHED
Documentation other than minimum documentation that are included in the fields searched:

340/932.2, 988, 928, 901-905, 934-936, 991, 825.54, 825.49;
364/436; 342/457; 235/380, 384.

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).

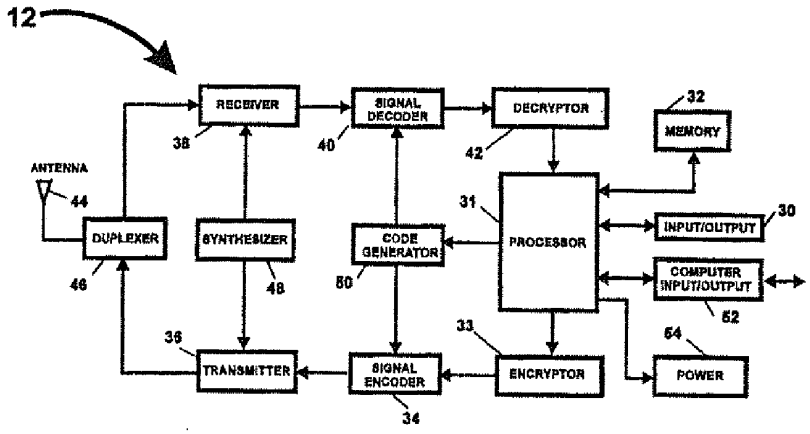
(72) Inventor: CLEVELAND, Joseph, Robert; 911 Grinnell Drive, Richardson, TX 75081 (US).

(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.

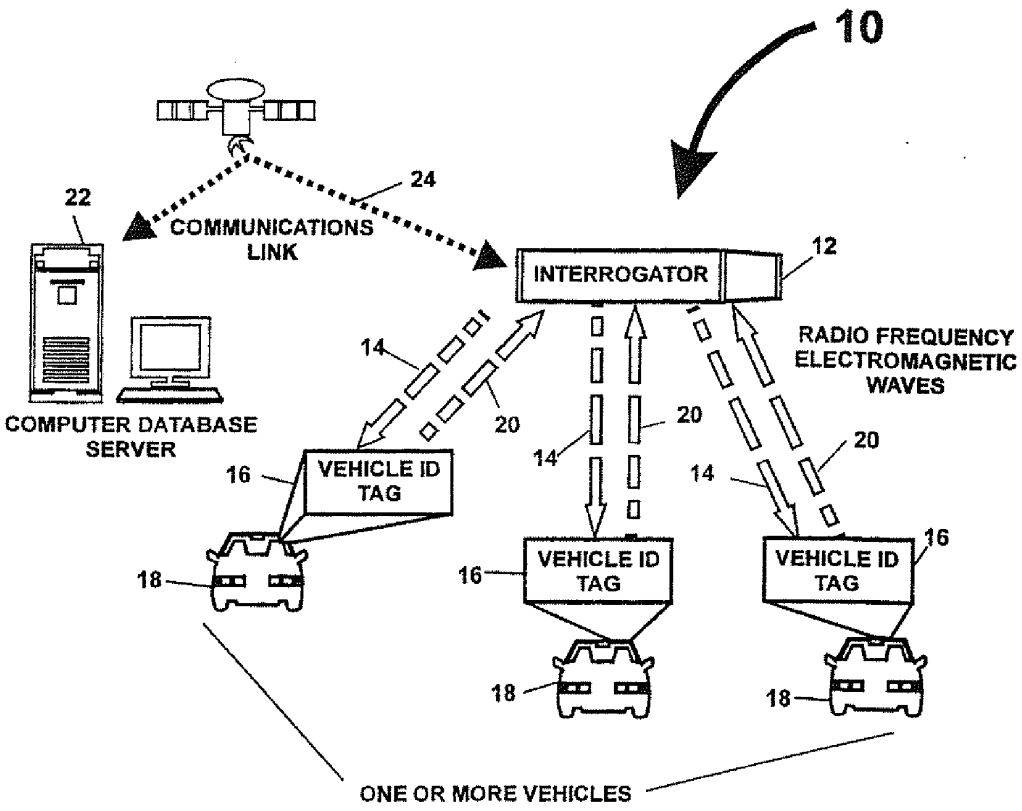


Figure 1

BNSDOCID: <WO_____9843104A2_I_>

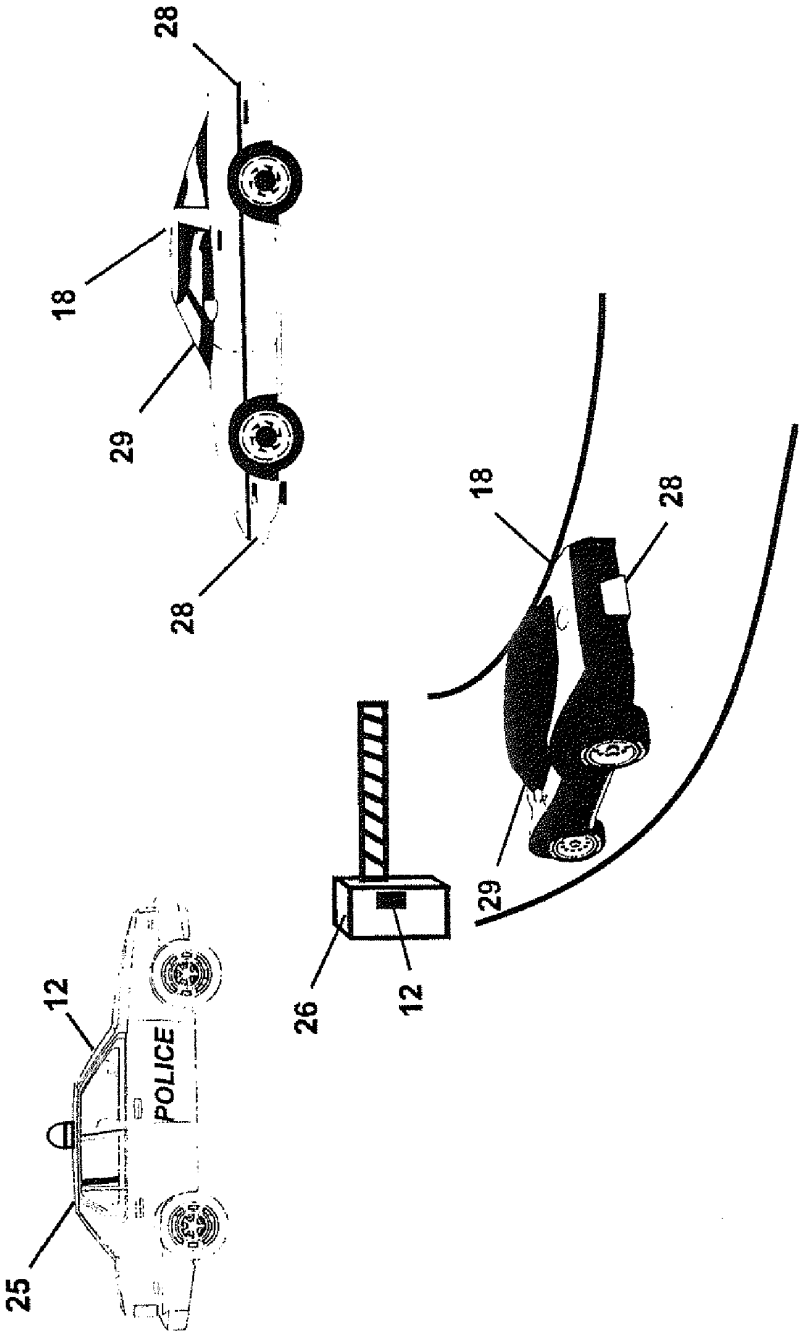


Figure 2

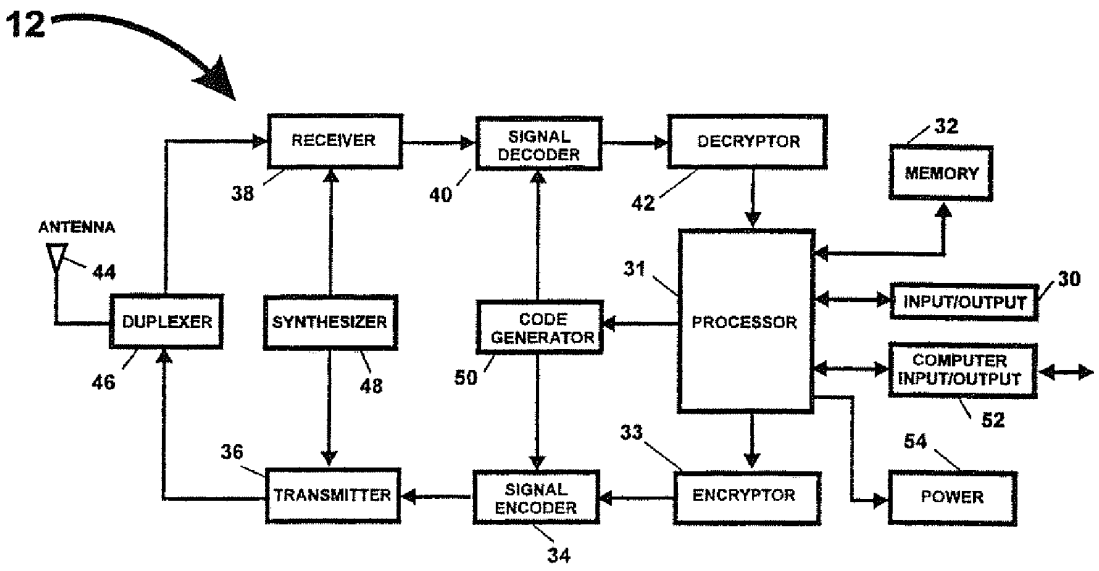


Figure 3

BNSDOCID: <WO_____9843104A2_i_>

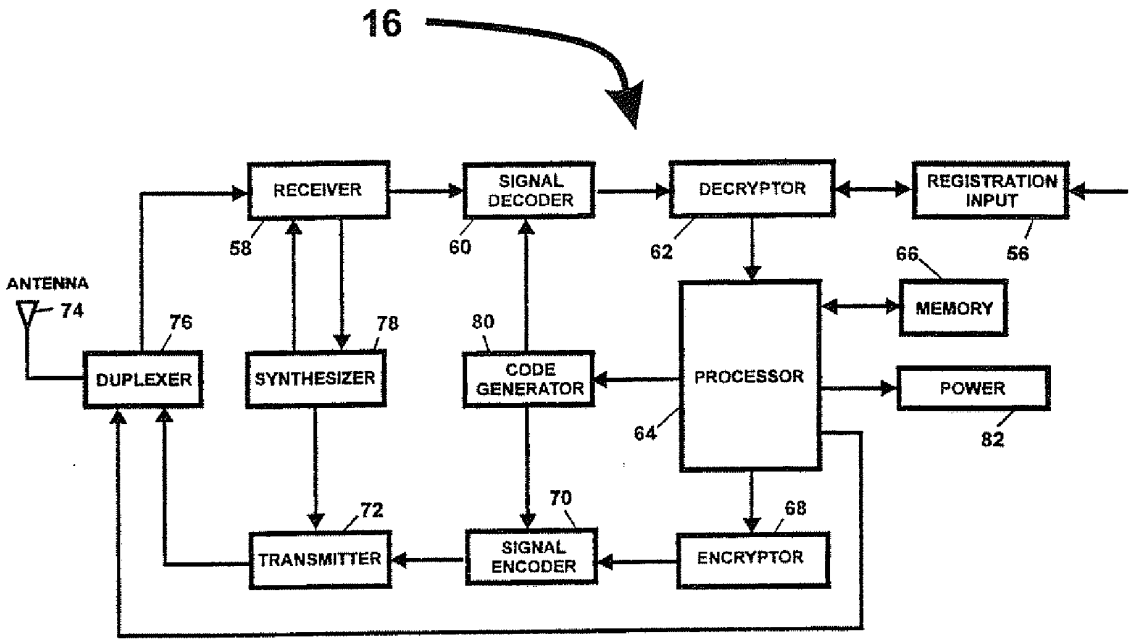

16
RECEIVER
SIGNAL DECODER
DECRYPTOR
REGISTRATION INPUT
58
60
62
66
56
ANTENNA
74
MEMORY
76
78
80
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
POWER
64
82
72
70
68
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR

Figure 4

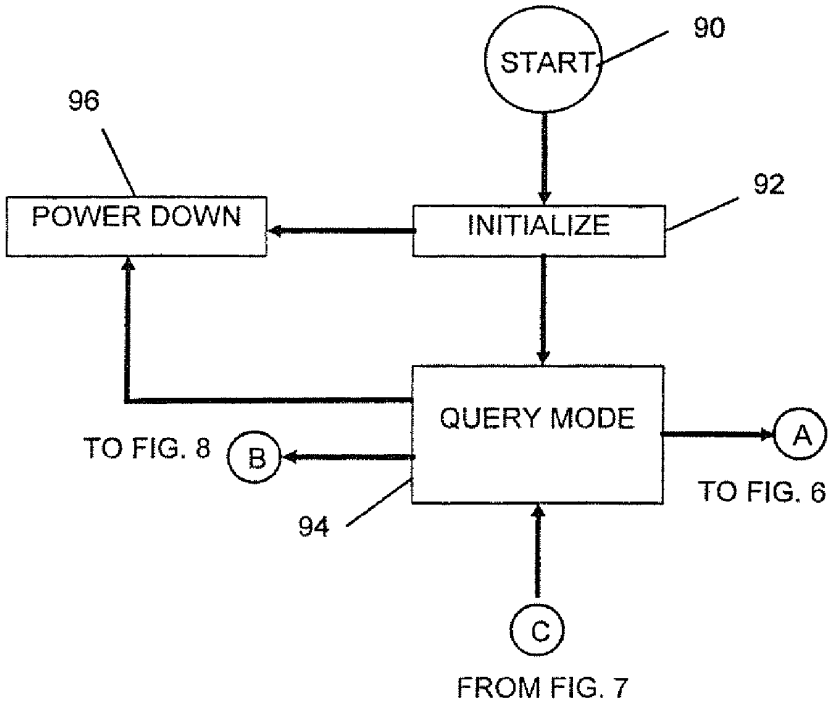


Figure 5

BNSDOCID: <WO_____9843104A2_I_>

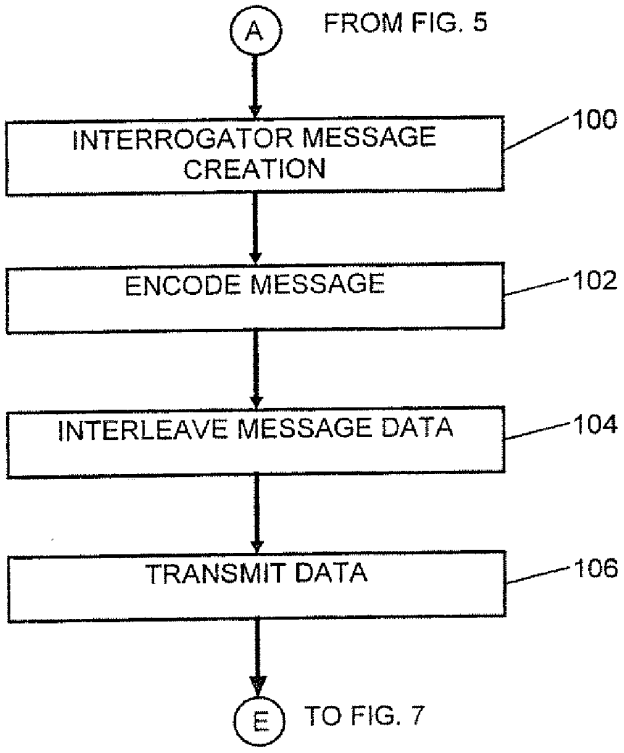

A
FROM FIG. 5
INTERROGATOR MESSAGE CREATION
100
ENCODE MESSAGE
102
INTERLEAVE MESSAGE DATA
104
TRANSMIT DATA
106
E
TO FIG. 7

Figure 6

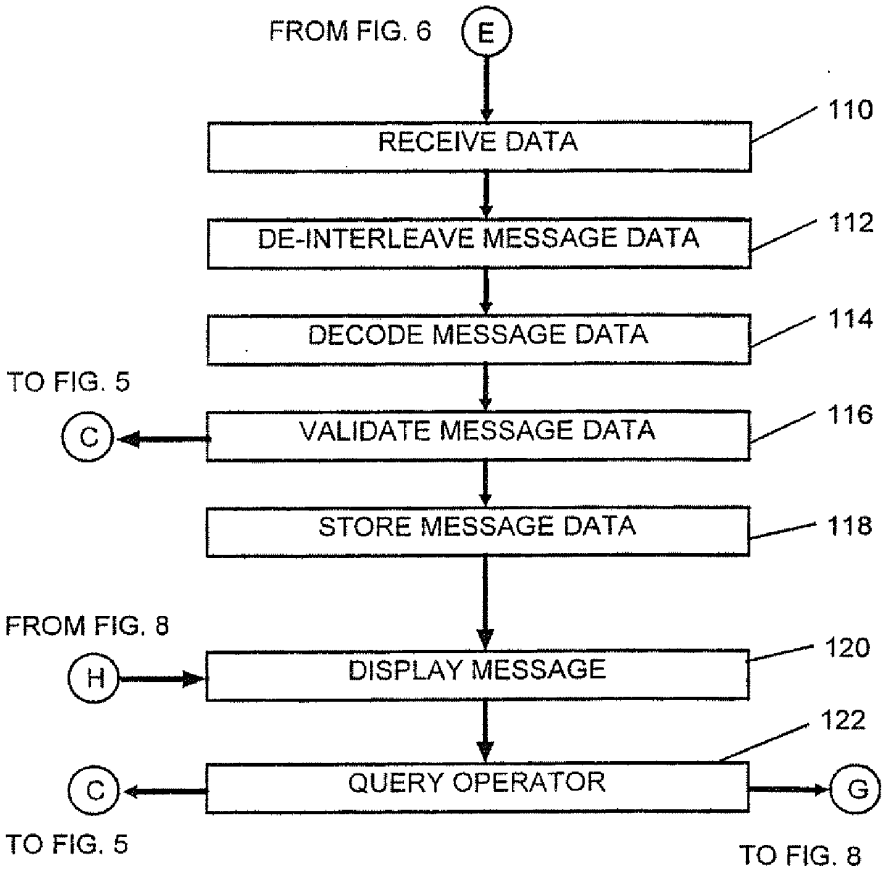


Figure 7

BNSDOCID: <WO_____9843104A2_I_>

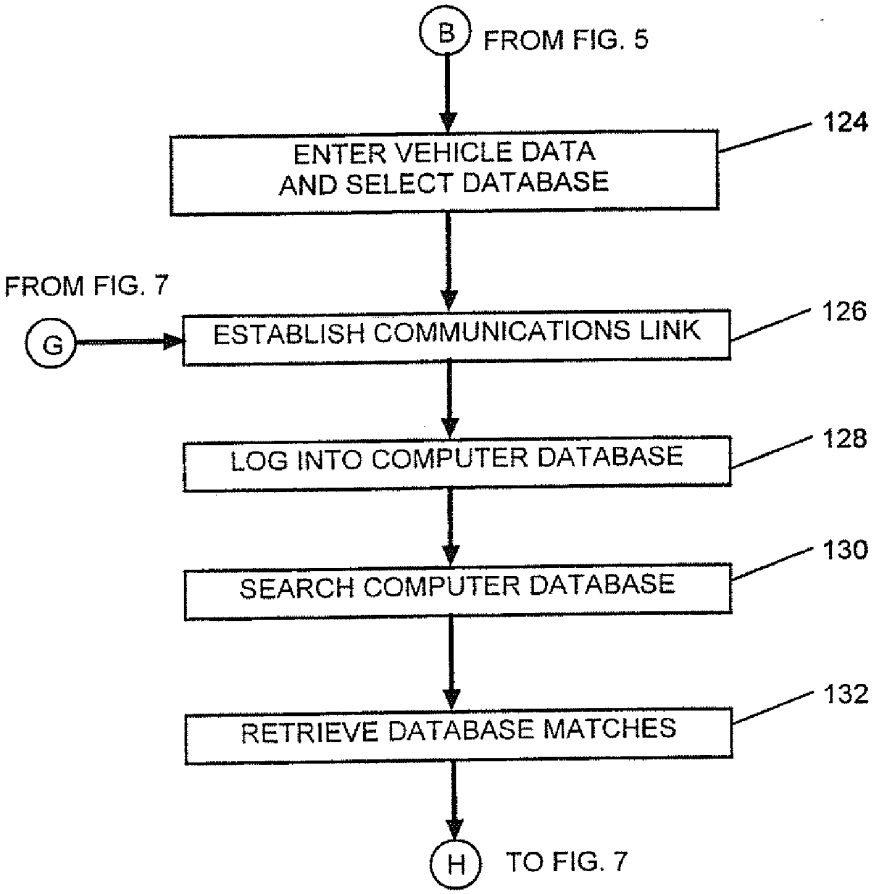

B
FROM FIG. 5
ENTER VEHICLE DATA AND SELECT DATABASE
124
FROM FIG. 7
G
ESTABLISH COMMUNICATIONS LINK
126
LOG INTO COMPUTER DATABASE
128
SEARCH COMPUTER DATABASE
130
RETRIEVE DATABASE MATCHES
132
H
TO FIG. 7

Figure 8

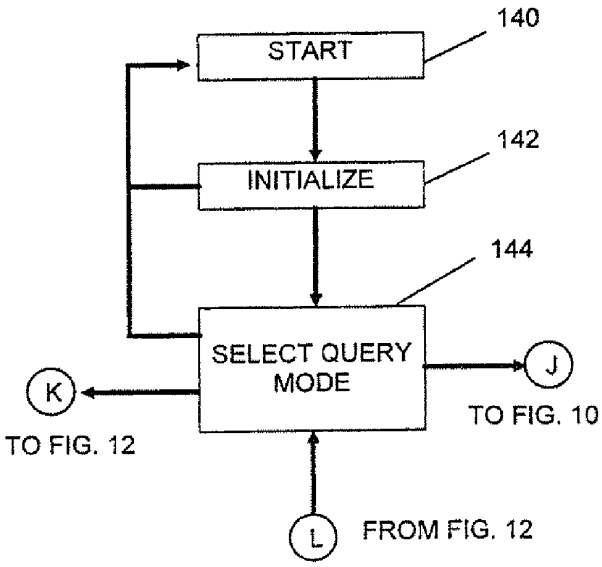

140
START
142
INITIALIZE
144
SELECT QUERY MODE
J
TO FIG. 10
K
TO FIG. 12
L
FROM FIG. 12

Figure 9

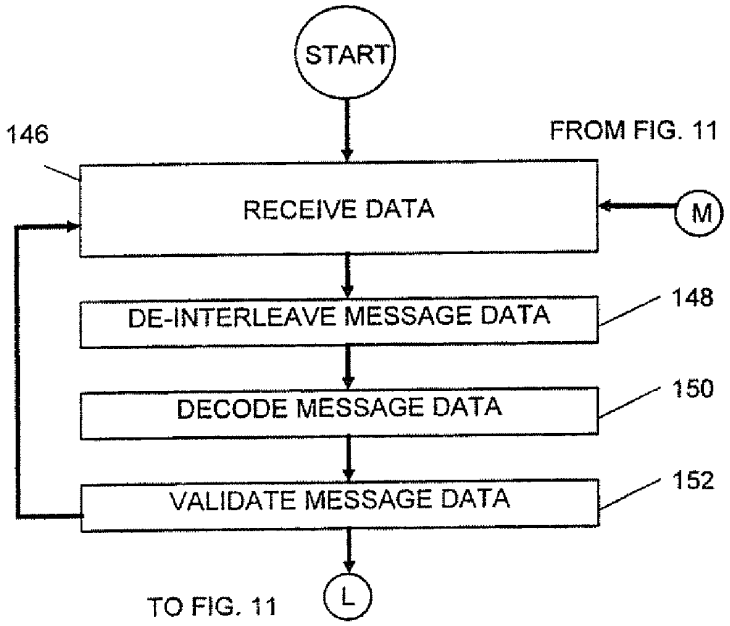

START
146
FROM FIG. 11
RECEIVE DATA
M
DE-INTERLEAVE MESSAGE DATA
148
DECODE MESSAGE DATA
150
VALIDATE MESSAGE DATA
152
TO FIG. 11
L

Figure 10

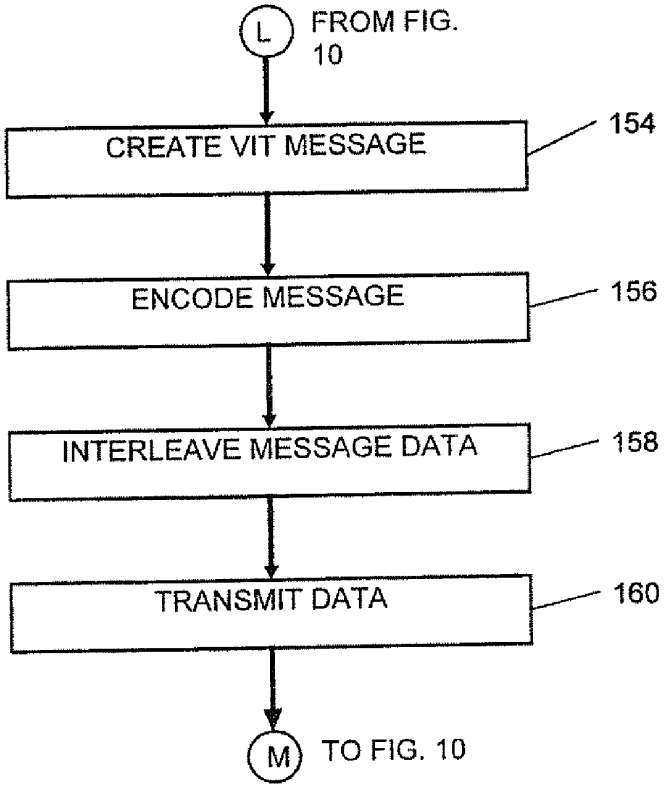

L
FROM FIG. 10
CREATE VIT MESSAGE
154
ENCODE MESSAGE
156
INTERLEAVE MESSAGE DATA
158
TRANSMIT DATA
160
M
TO FIG. 10

Figure 11

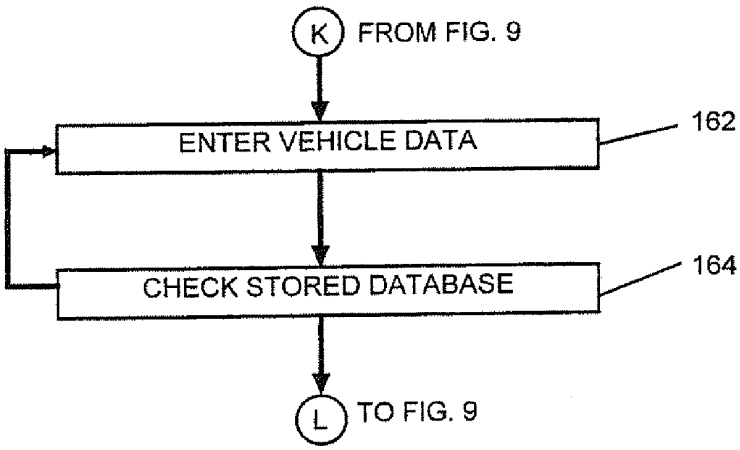

K
FROM FIG. 9
ENTER VEHICLE DATA
162
CHECK STORED DATABASE
164
L
TO FIG. 9

Figure 12

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

(11) EP 0 977 145 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: **99114633.3**

(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 33893498
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).

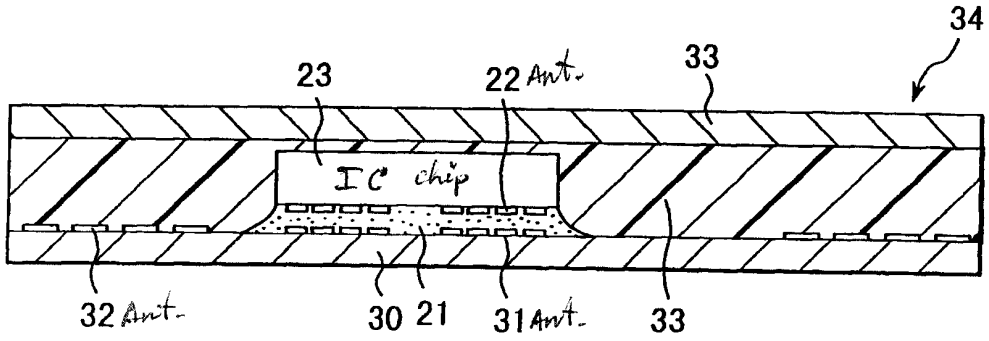


FIG. 14

EP 0 977 145 A2

Printed by Jouve, 75001 PARIS (FR)

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 Cunife. 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 O 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 sl 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

$$v = -d\Phi/dt \tag{6}$$

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,

$$\begin{aligned} \Phi &= B \cdot S \\ &= \mu \cdot H \cdot S \end{aligned} \qquad \ldots(7)$$

[0198] The induction electromotive force v is expressed by

$$v = \mu \cdot S \cdot dH/dt \tag{8}$$

[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:

$$\mu = 1.25 \times 10^{6}\ [H/m] \tag{9}$$

[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

$$\begin{aligned} H &= 2.87 \times 10^{4}\ [Oe] \\ &= 2.28 \times 10^{6}\ [A/m] \end{aligned} \qquad \ldots(10)$$

[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

$$v = 500\mu \cdot S \cdot 2H/10^{-1}$$
$$= 1.14 \ [V] \qquad \ldots(11)$$

[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 61. 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 83 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 80 is constituted.

[0258] In step #15, printing is effected on the surface of the carrier body 80, and at last the manufactured radio IC card is inspected.

[0259] The size of the manufactured radio IC card is 86 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 (91) 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 (l10b) 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).

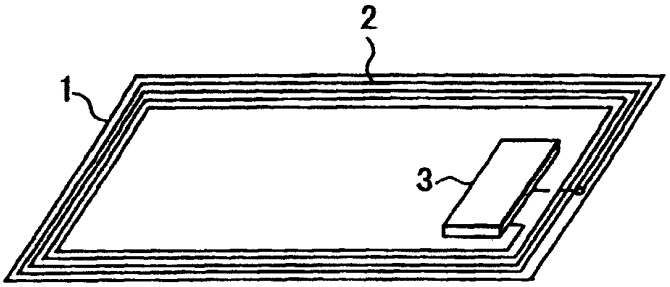


FIG. 1

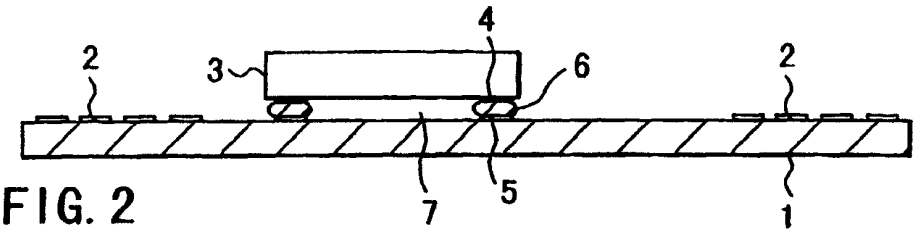


FIG. 2

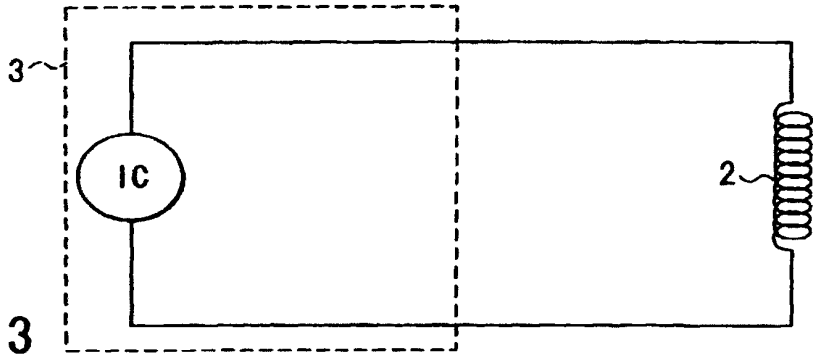


FIG. 3

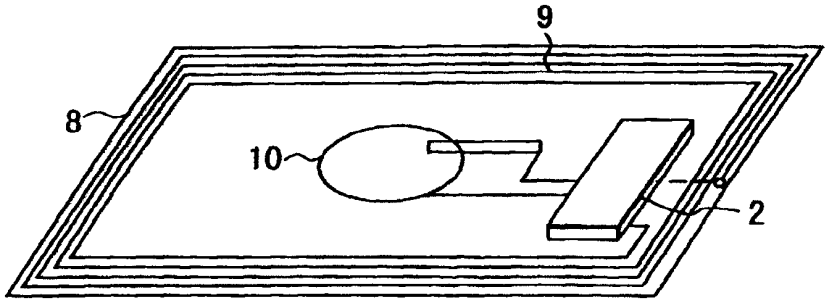


FIG. 4

FIG. 5

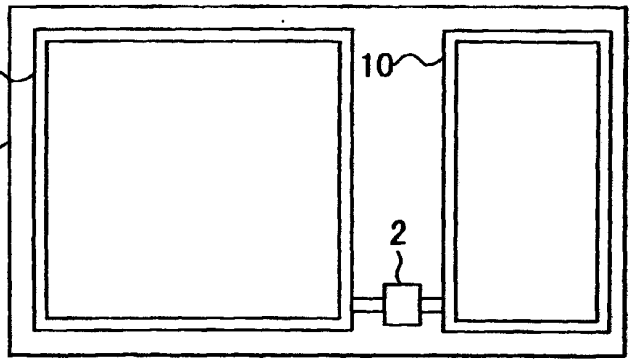


FIG. 6

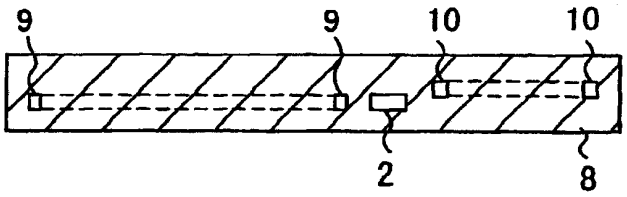


FIG. 7A

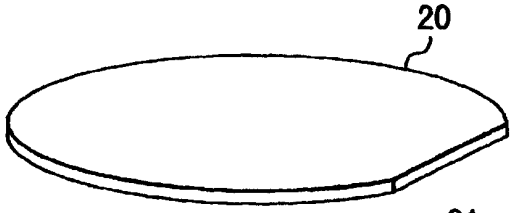


FIG. 7B

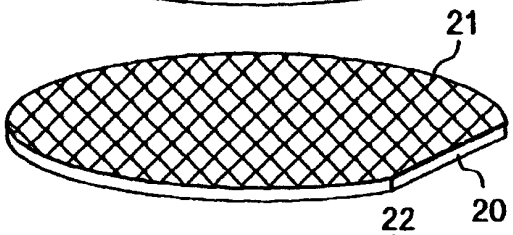


FIG. 7C

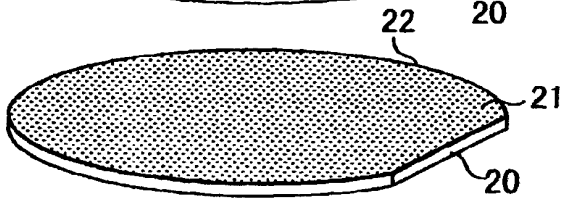
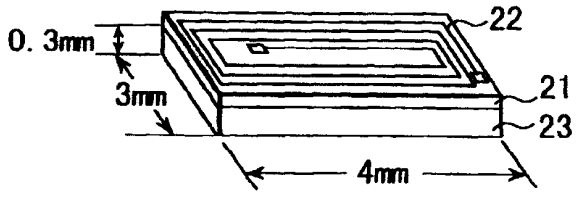


FIG. 7D



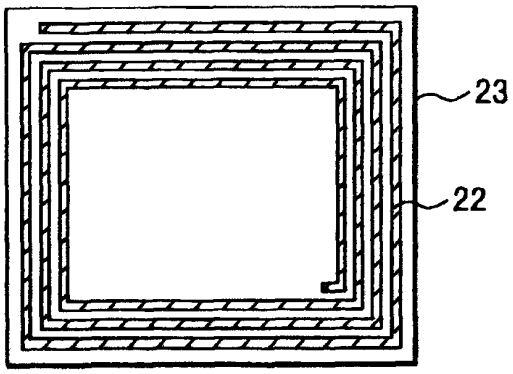


FIG. 8A

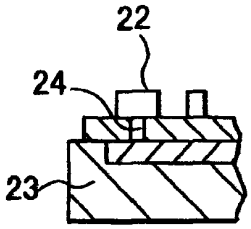


FIG. 8C

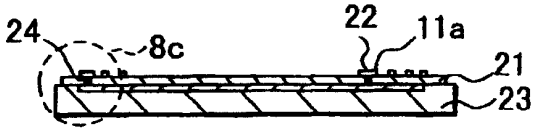


FIG. 8B

FIG. 8D

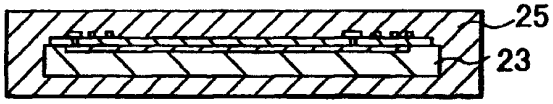


FIG. 9A

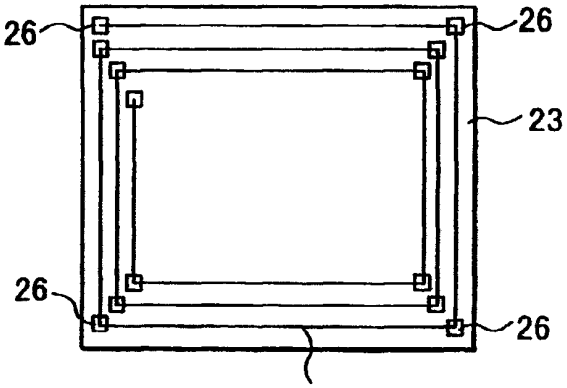


FIG. 9B

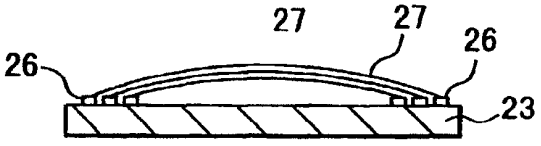


FIG. 10

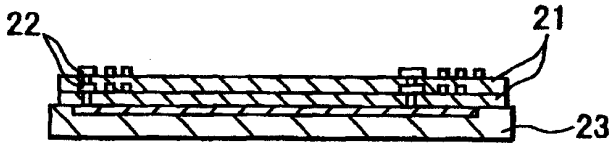


FIG. 11

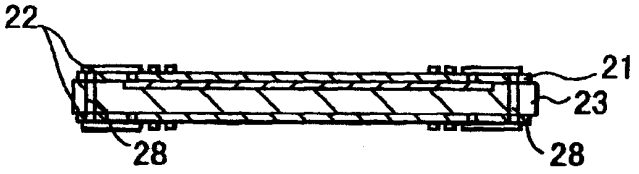


FIG. 12

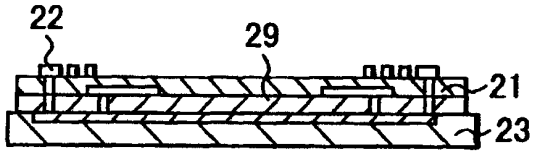


FIG. 13A

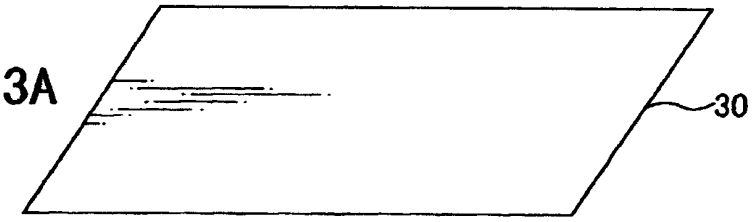


FIG. 13B

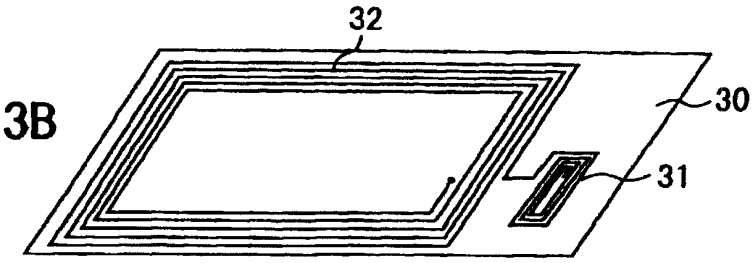
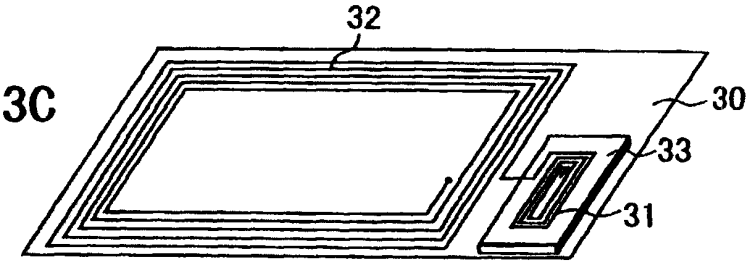


FIG. 13C



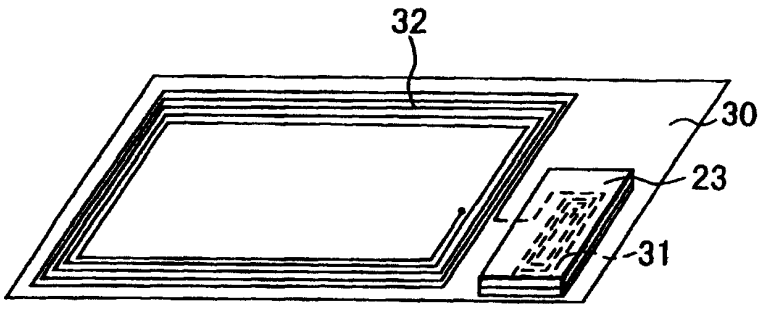


FIG. 13D

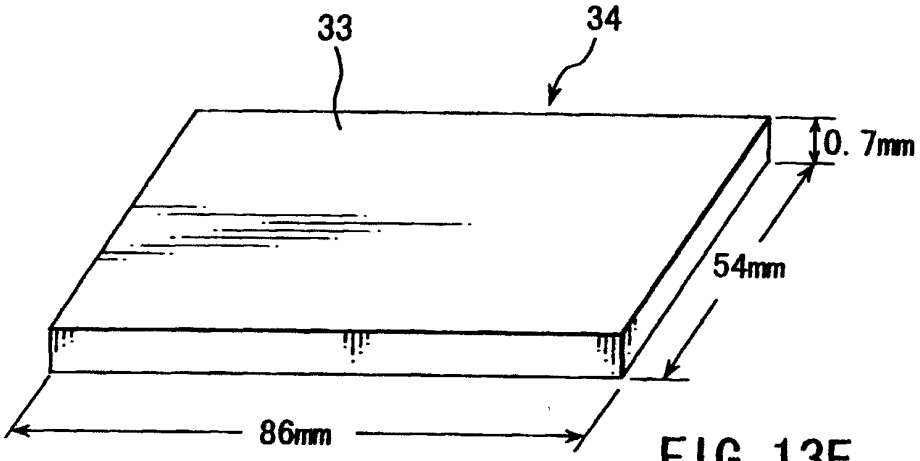


FIG. 13E

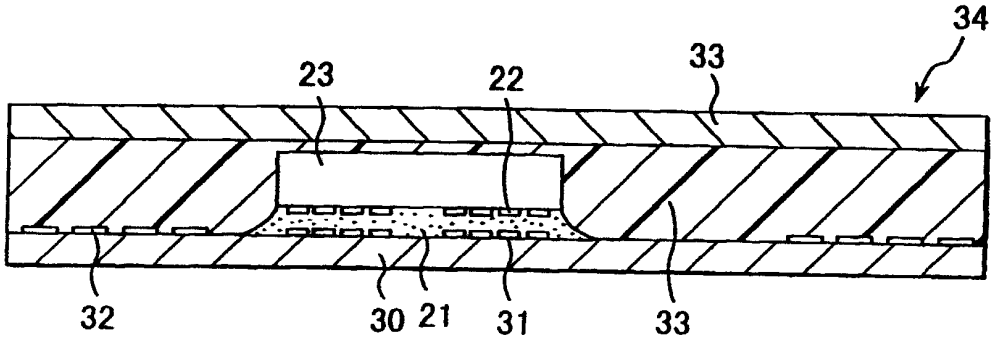


FIG. 14

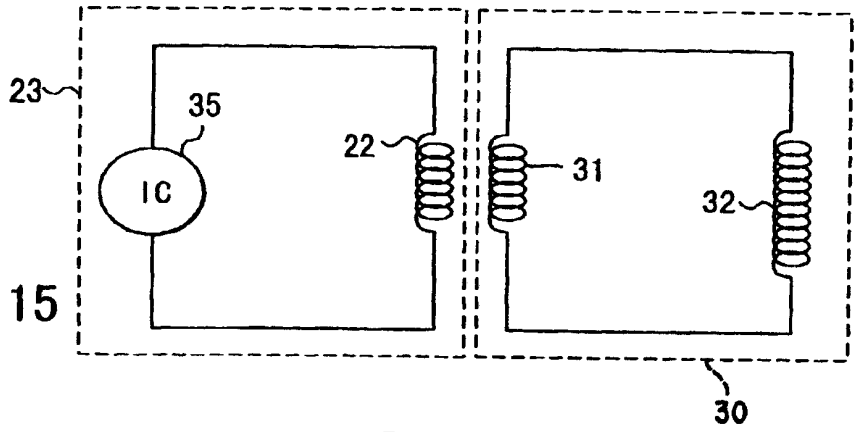


FIG. 15

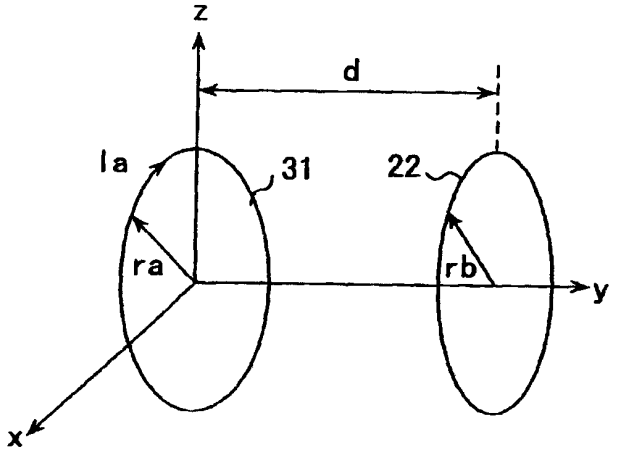


FIG. 16

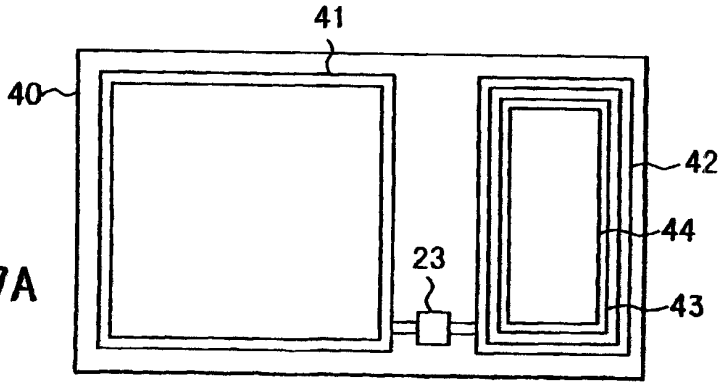


FIG. 17A

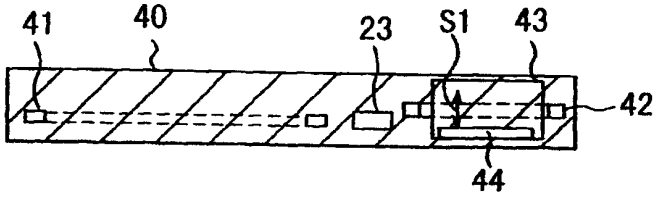


FIG. 17B

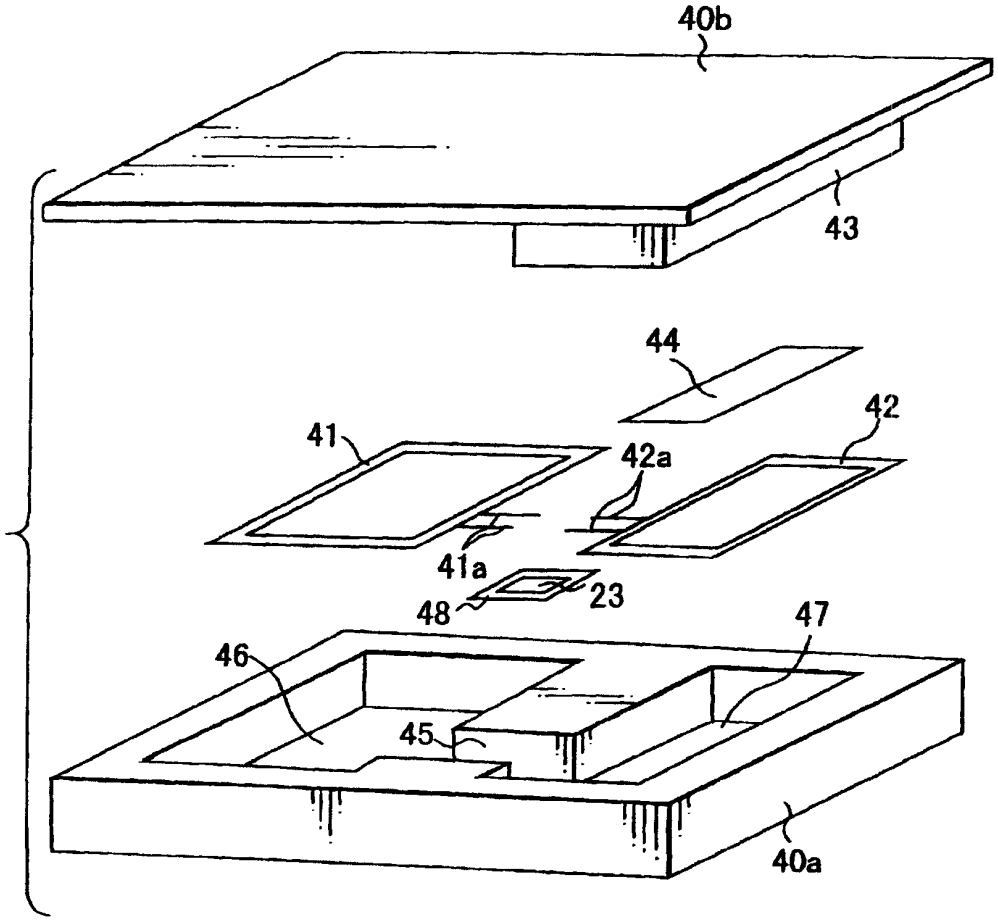


FIG. 18

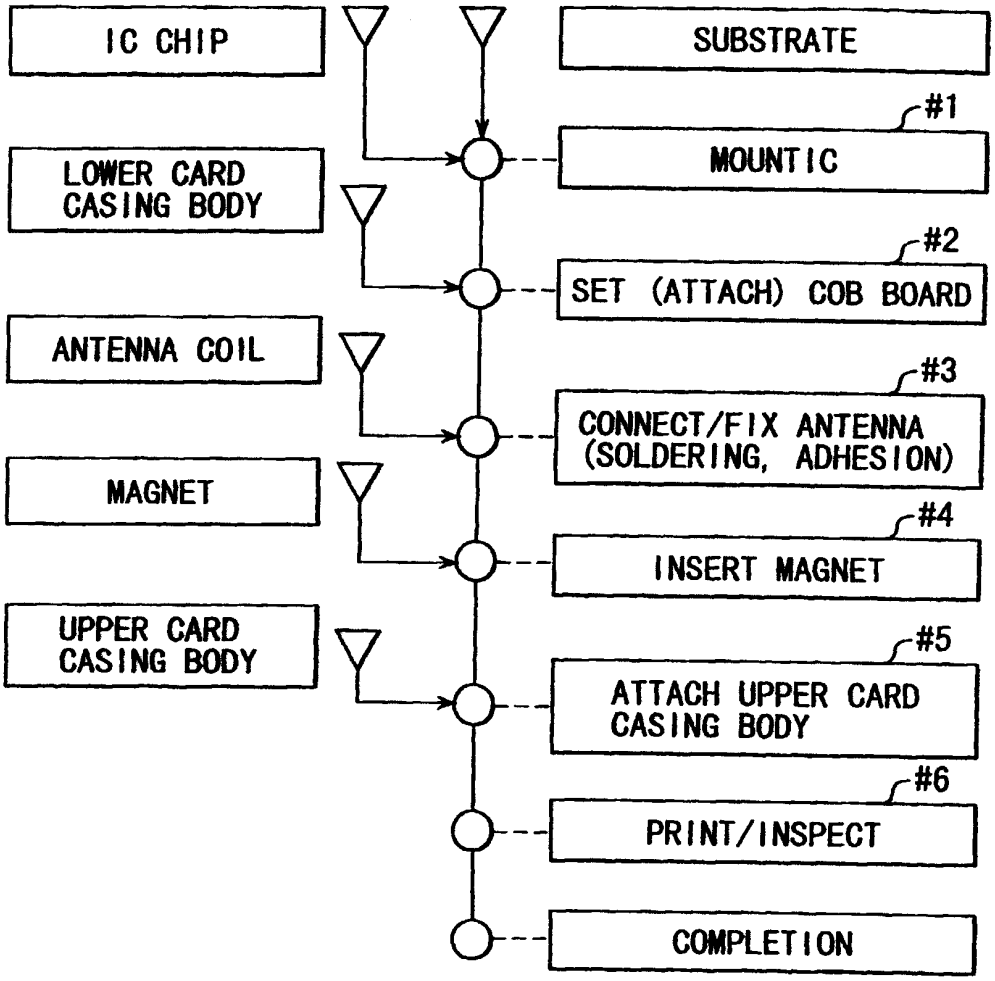

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#1
MOUNT IC
#2
SET (ATTACH) COB BOARD
#3
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#4
INSERT MAGNET
#5
ATTACH UPPER CARD CASING BODY
#6
PRINT/INSPECT
COMPLETION

FIG. 19

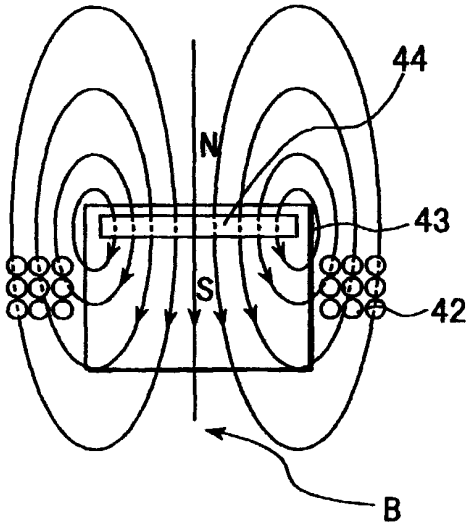


FIG. 20A

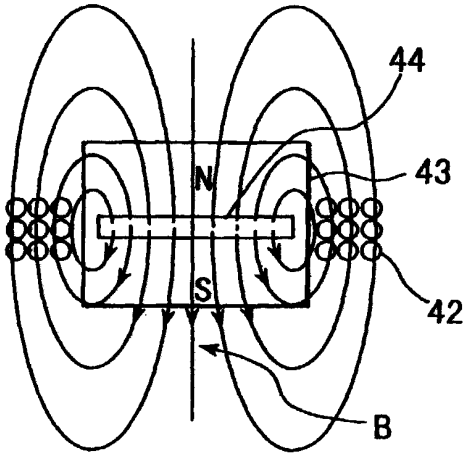


FIG. 20B

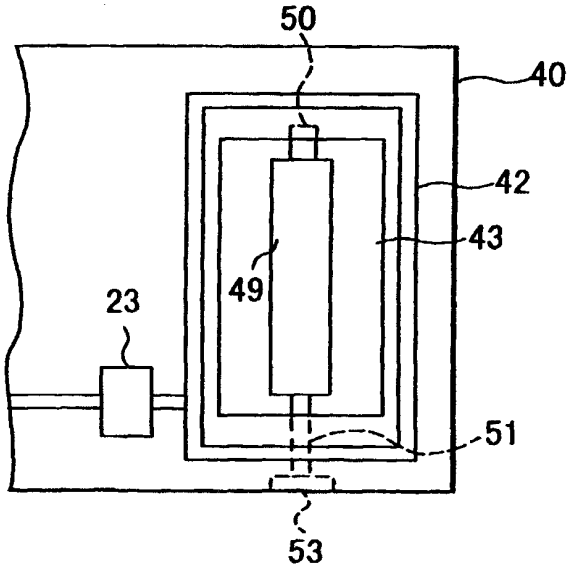


FIG. 21A

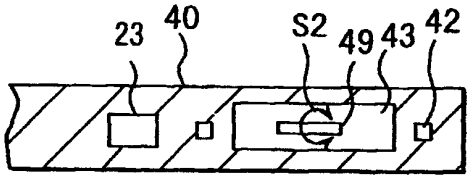


FIG. 21B

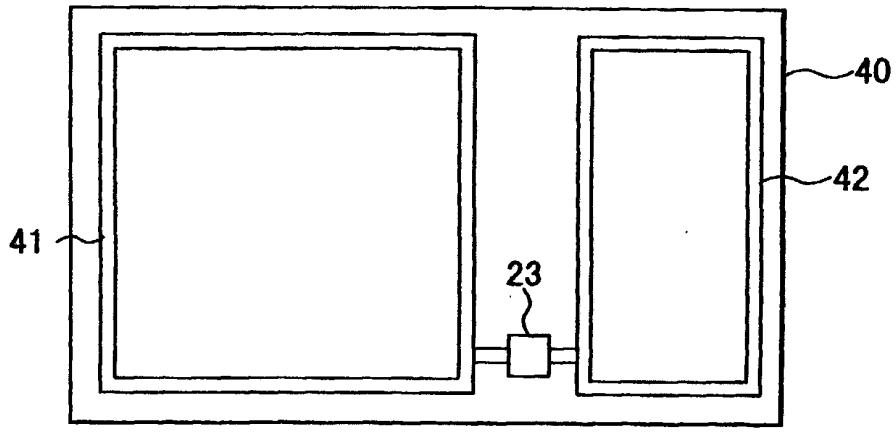


FIG. 22A

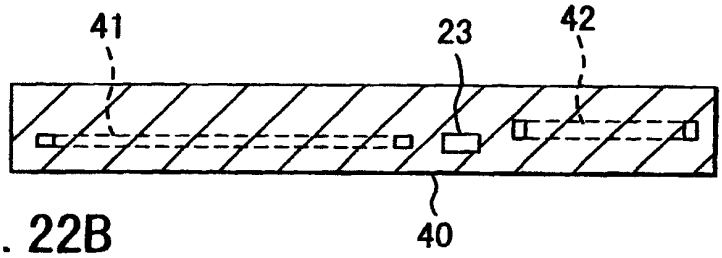


FIG. 22B

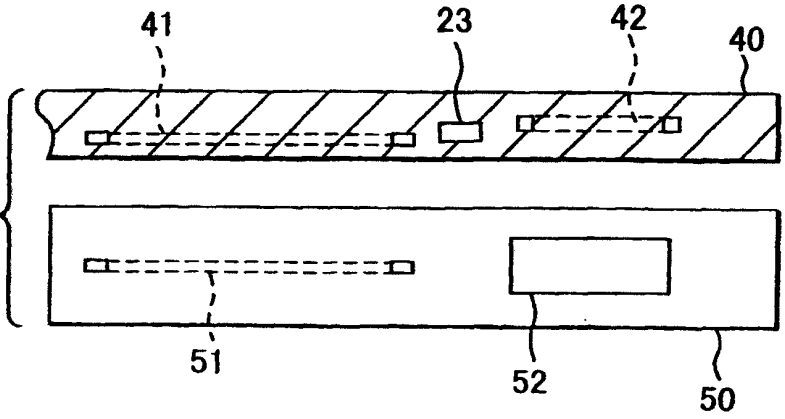


FIG. 23

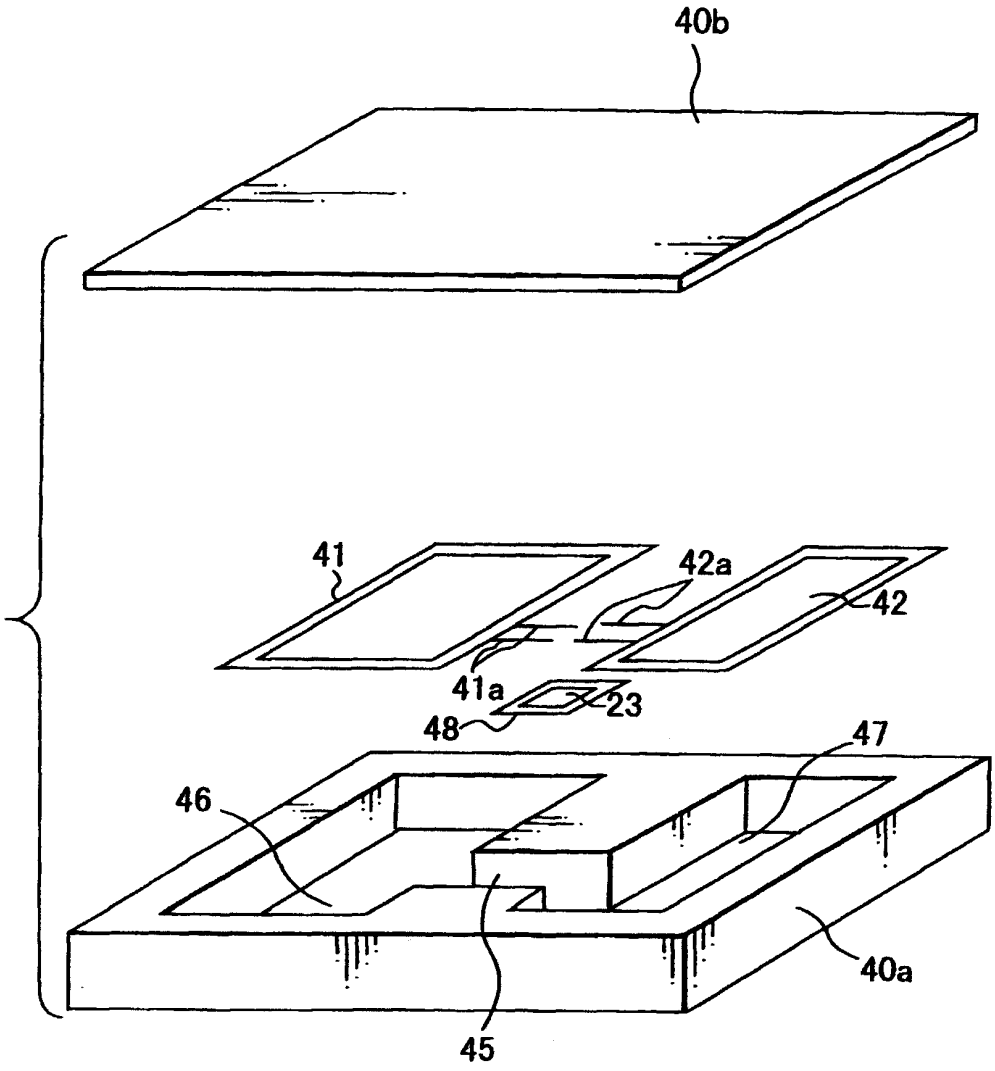


FIG. 24

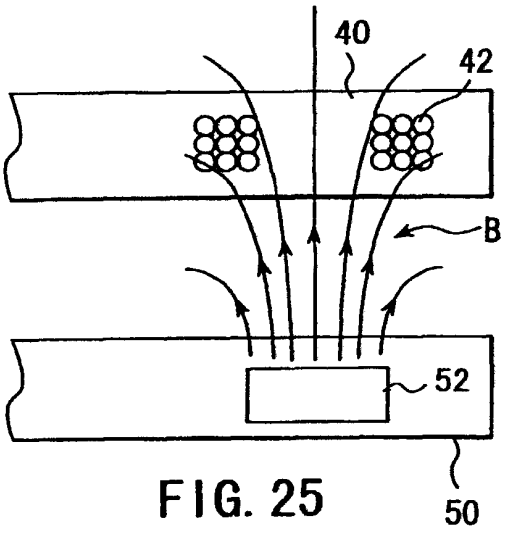


FIG. 25

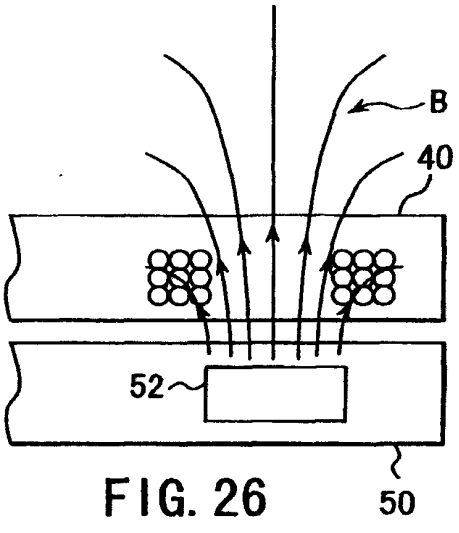


FIG. 26

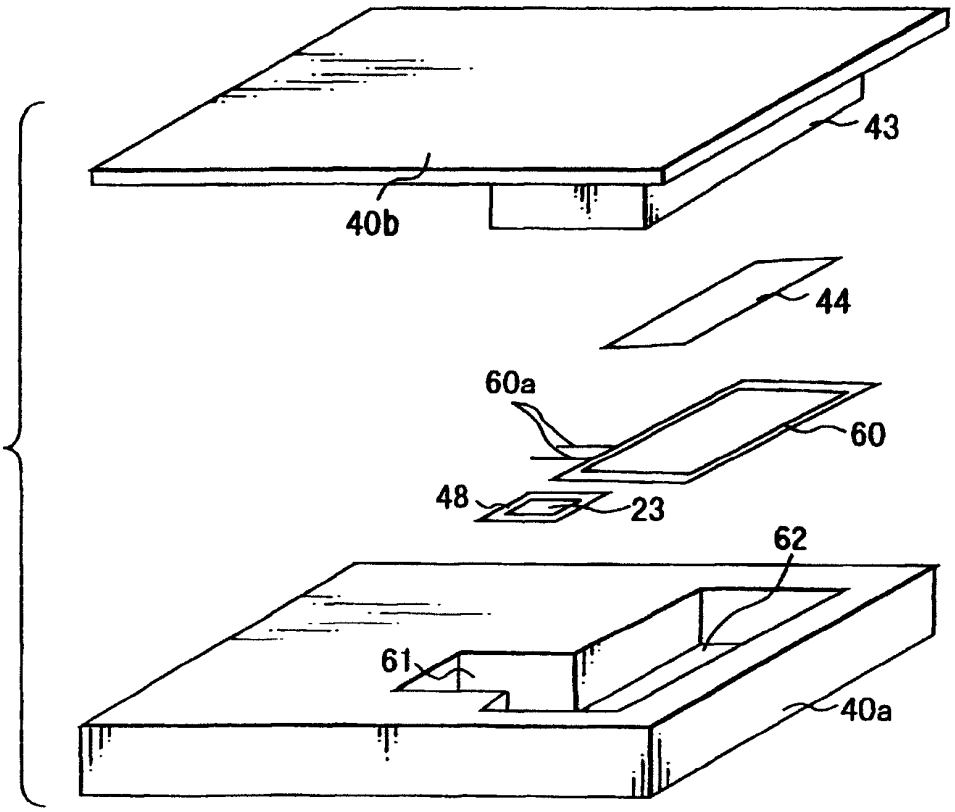


FIG. 27

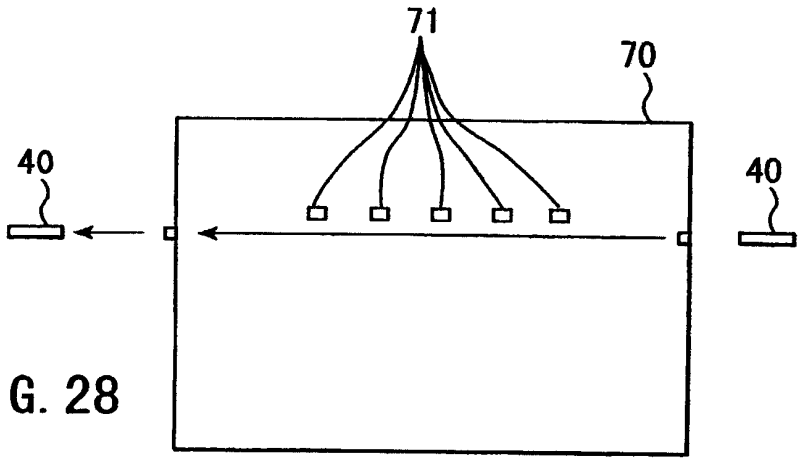


FIG. 28

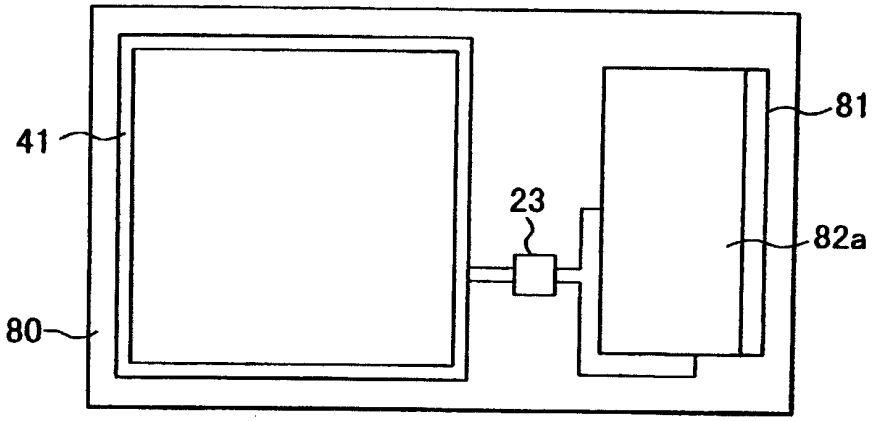


FIG. 29A

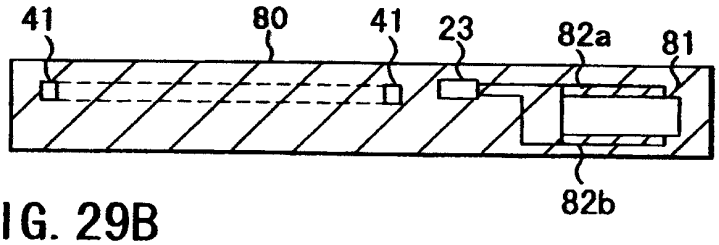


FIG. 29B

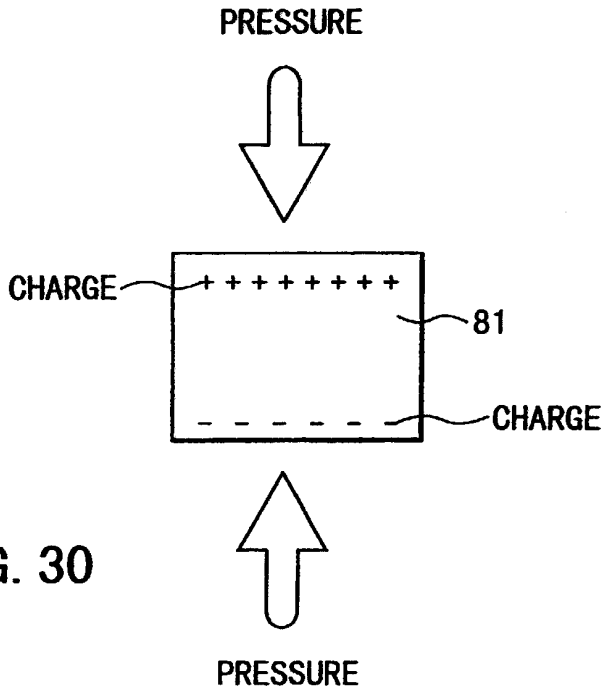


FIG. 30

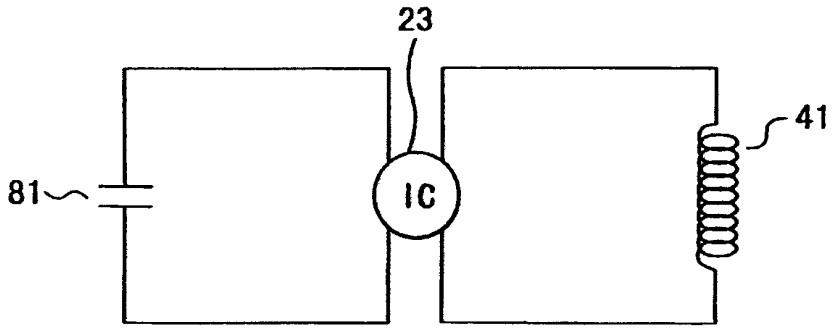


FIG. 31

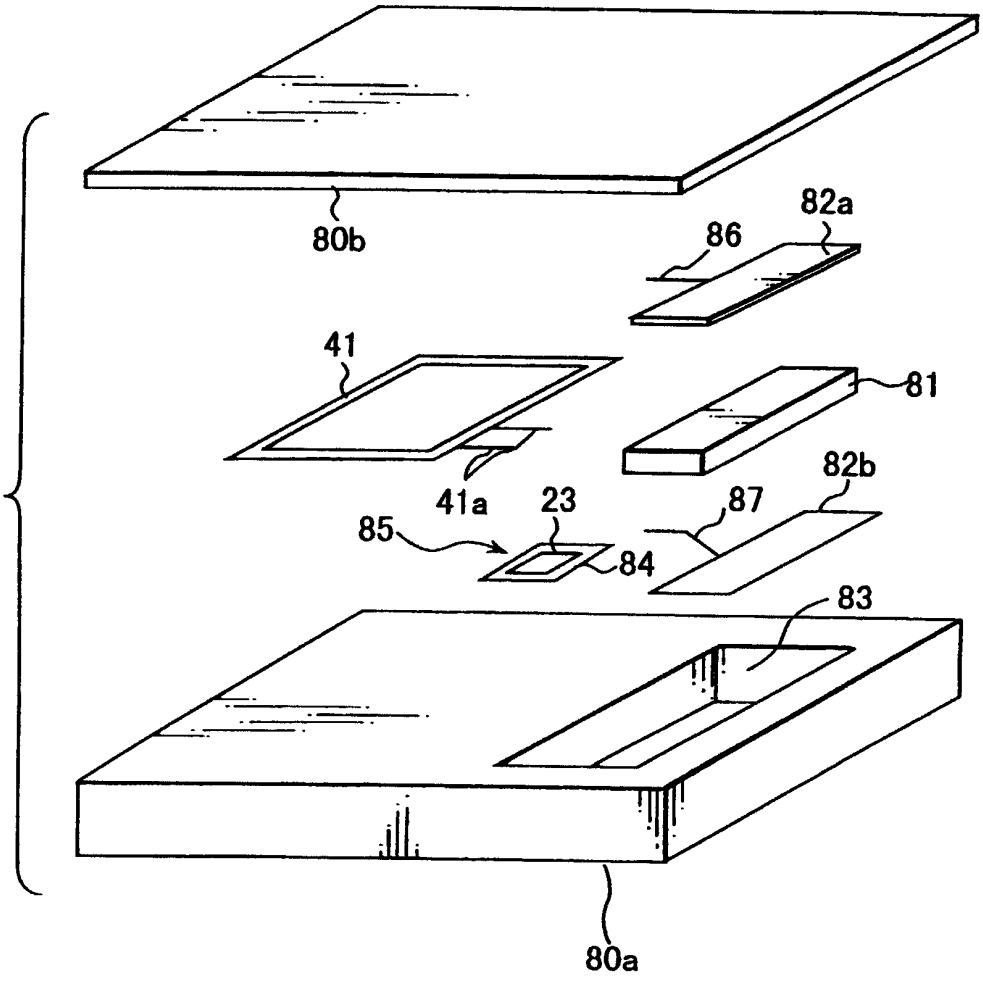


FIG. 32

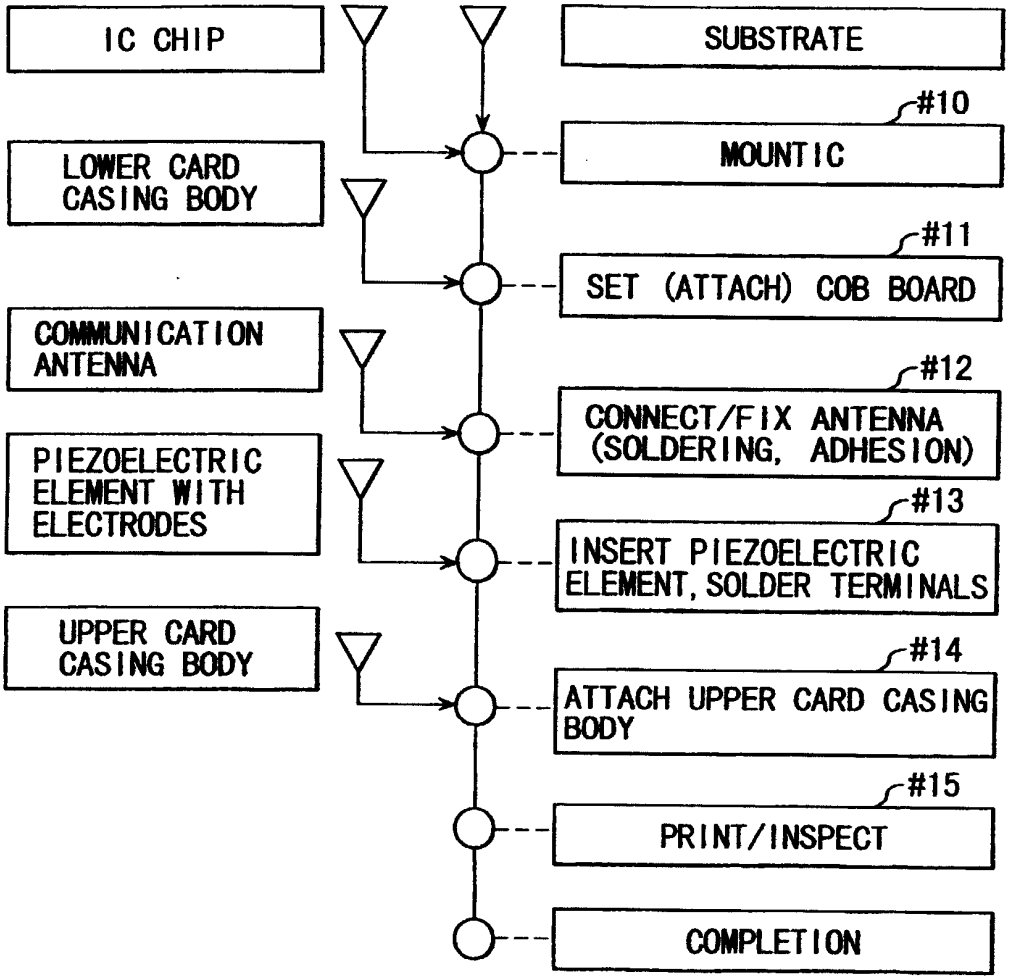

IC CHIP
LOWER CARD CASING BODY
COMMUNICATION ANTENNA
PIEZOELECTRIC ELEMENT WITH ELECTRODES
UPPER CARD CASING BODY
SUBSTRATE
#10
MOUNTIC
#11
SET (ATTACH) COB BOARD
#12
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#13
INSERT PIEZOELECTRIC ELEMENT, SOLDER TERMINALS
#14
ATTACH UPPER CARD CASING BODY
#15
PRINT/INSPECT
COMPLETION

FIG. 33

FIG. 34A

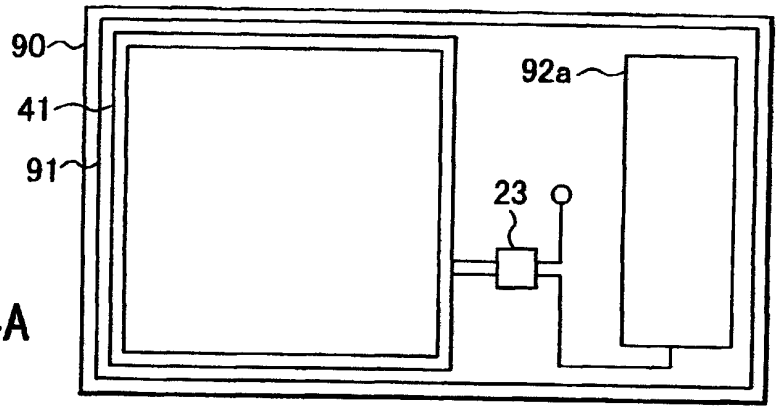


FIG. 34B

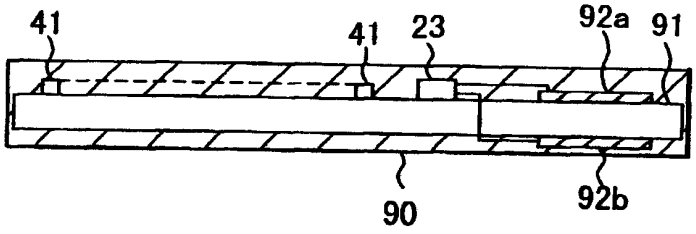
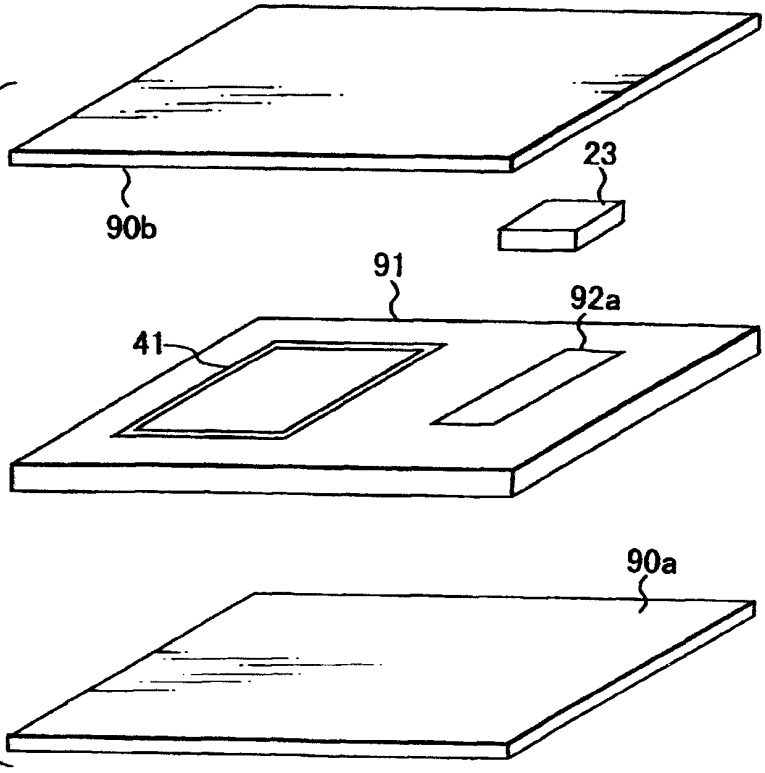


FIG. 35



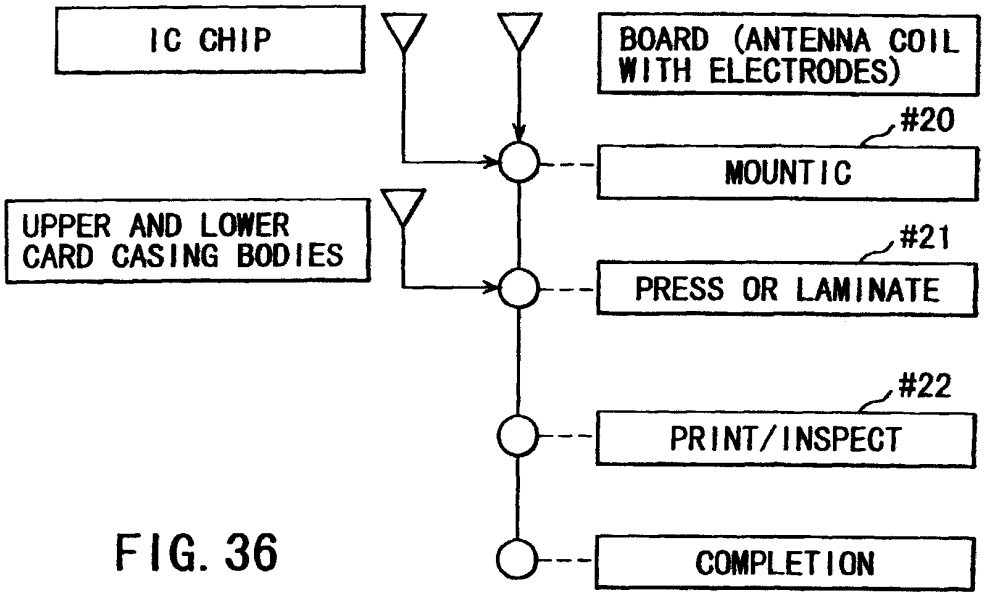


FIG. 36

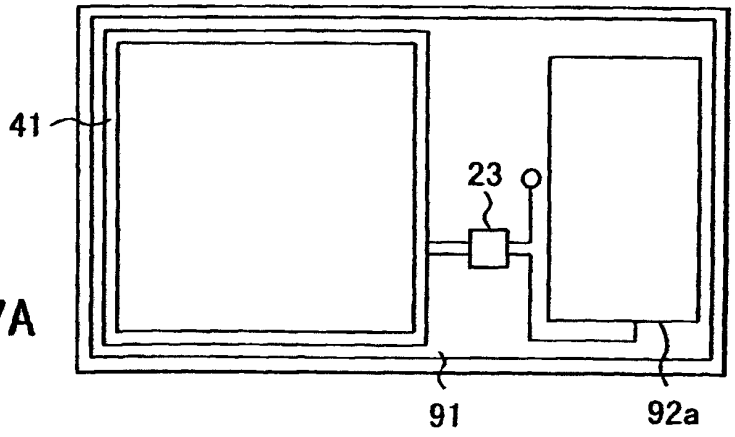


FIG. 37A

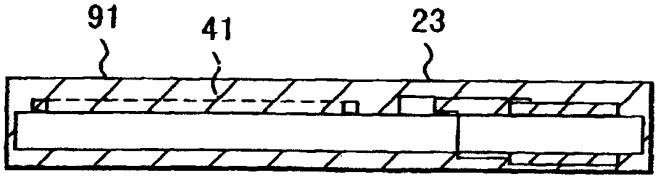


FIG. 37B

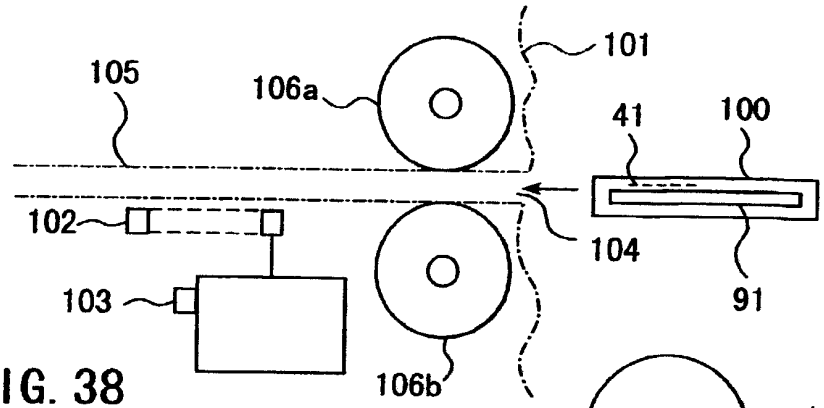


FIG. 38

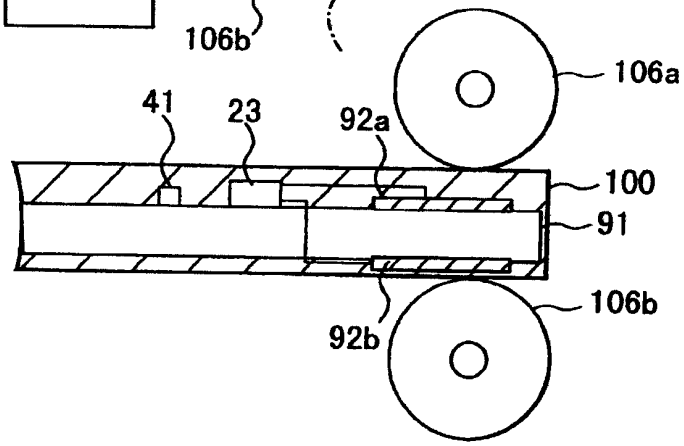


FIG. 39

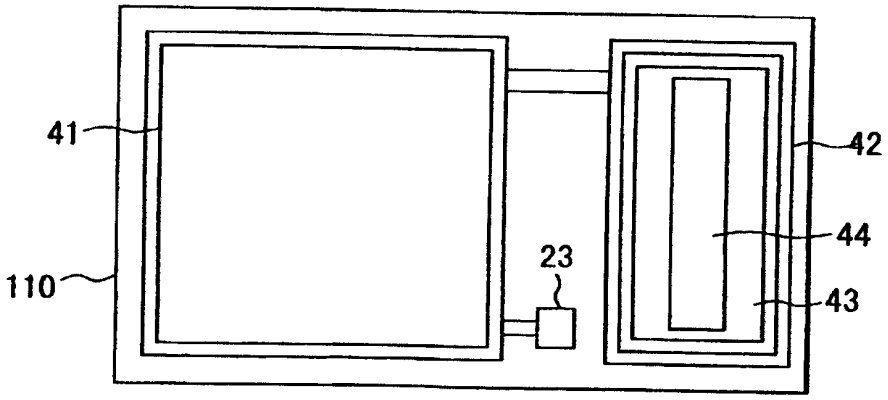


FIG. 40A

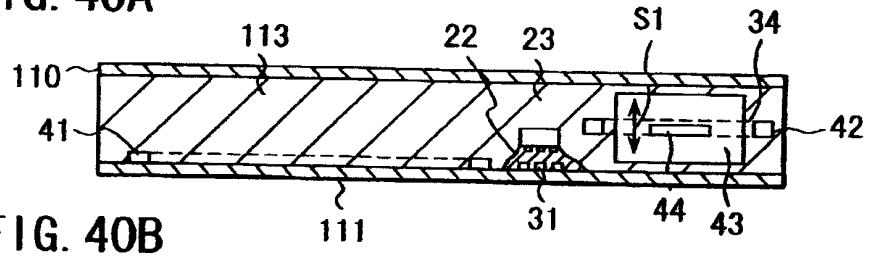


FIG. 40B

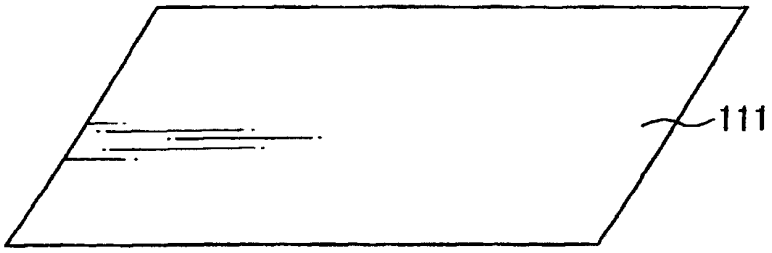


FIG. 41A

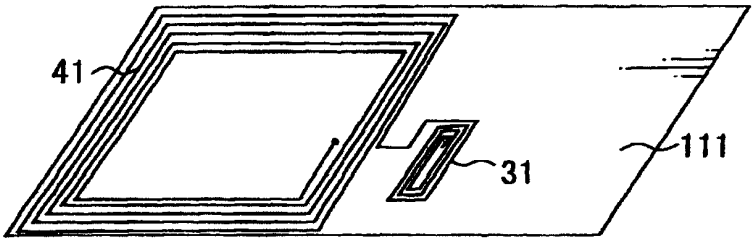


FIG. 41B

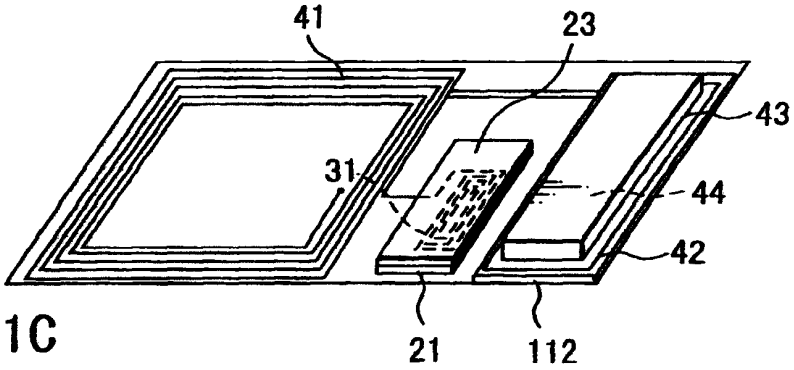


FIG. 41C

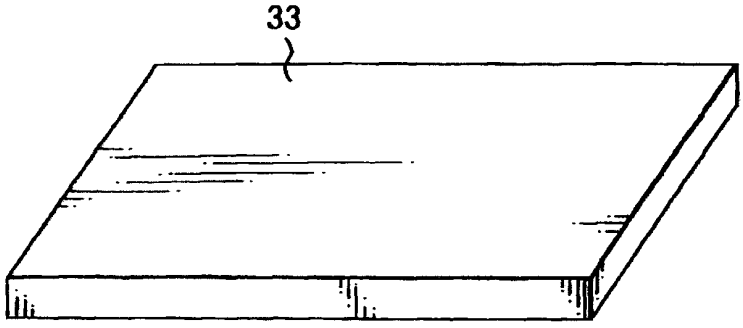
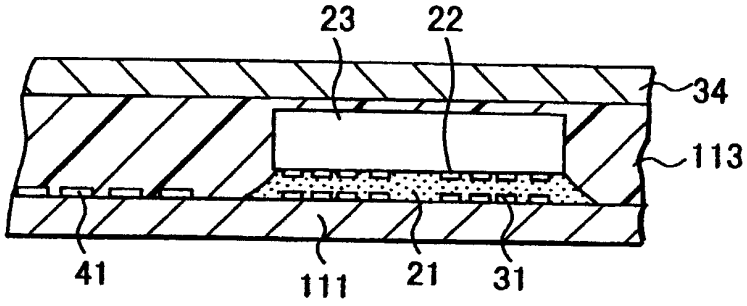


FIG. 41D

FIG. 42


23
22
34
113
41
111
21
31

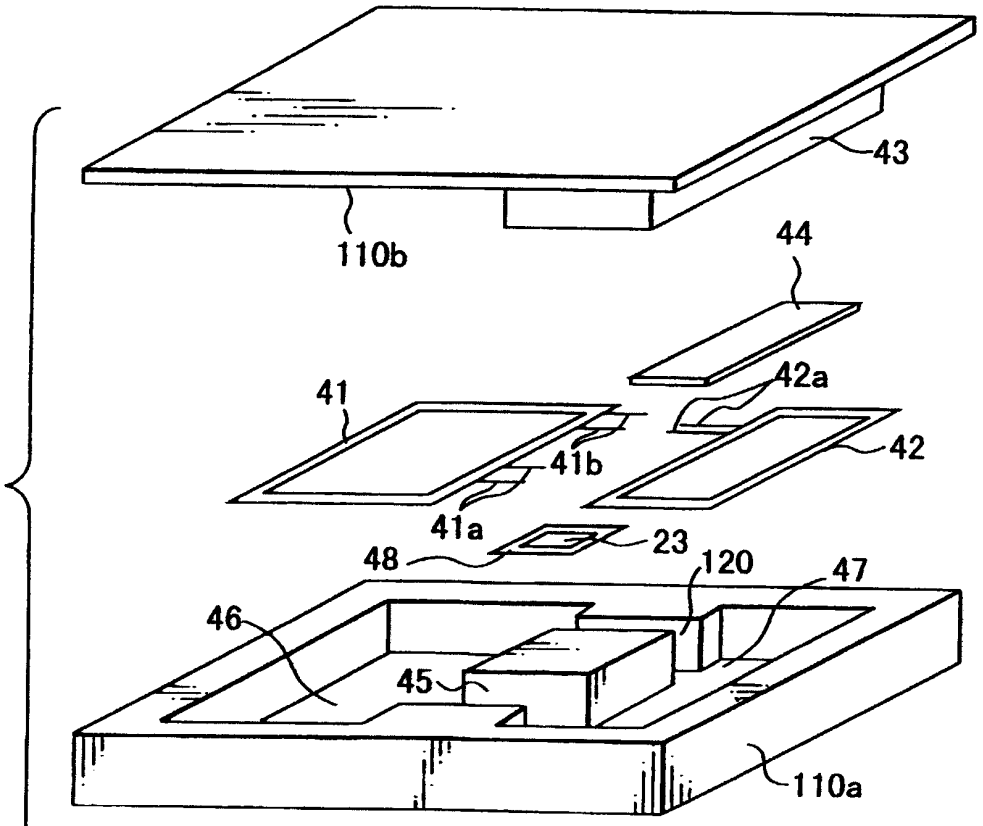

43
110b
44
42a
41
41b
42
41a
48
23
120
47
46
45
110a

FIG. 43

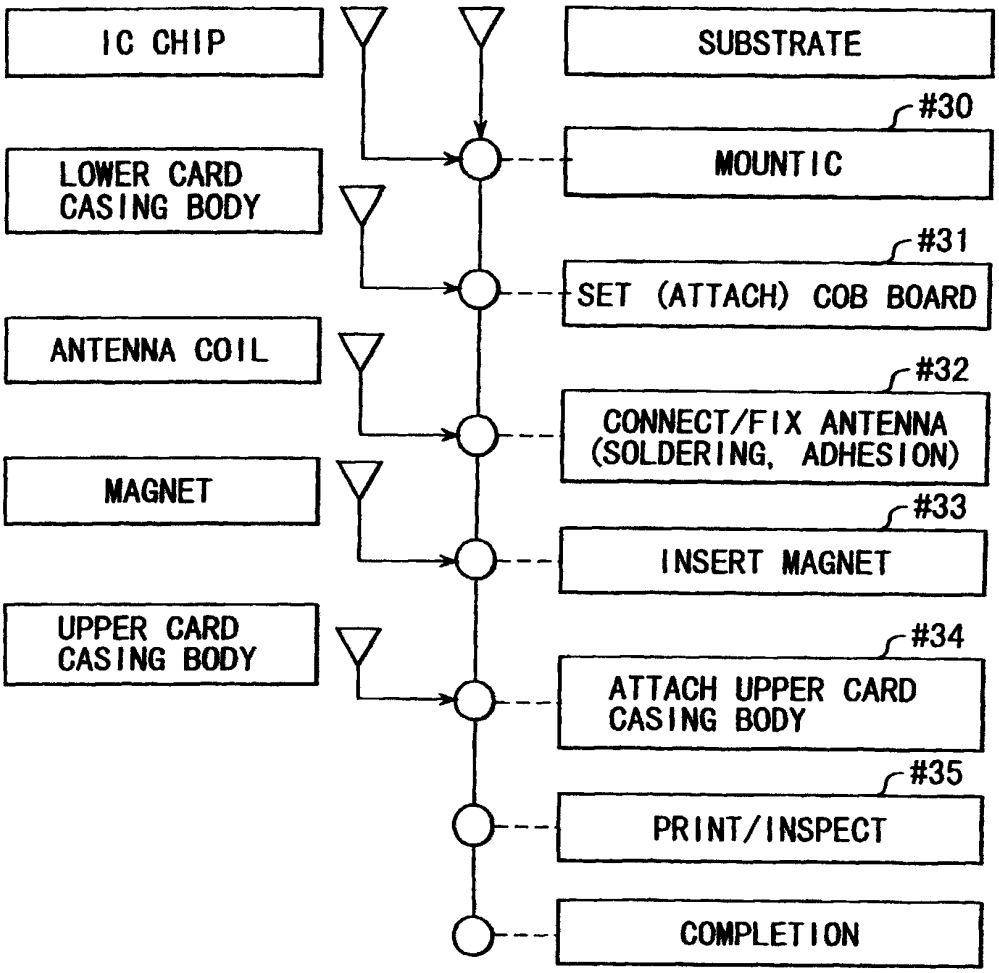

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#30
MOUNTIC
#31
SET (ATTACH) COB BOARD
#32
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#33
INSERT MAGNET
#34
ATTACH UPPER CARD CASING BODY
#35
PRINT/INSPECT
COMPLETION

FIG. 44

Espacenet

Bibliographic data: EP0993999 (A2) — 2000-04-19

Fuel pump immobilization

No documents available for this priority number.

Inventor(s): GILMORE PAUL ROBERT [GB] ± (GILMORE, PAUL ROBERT)

Applicant(s): FORD MOTOR CO [GB] ± (FORD MOTOR COMPANY LIMITED)

Classification: - international: ***B60R25/04; B60R25/042;*** (IPC1-7): B60R25/04
- cooperative: **B60R25/042**

Application number: EP19990305339 19990706

Priority number(s): GB19980022394 19981015

Also published as: EP0993999 (A3) GB2342742 (A)

Abstract of EP0993999 (A2)

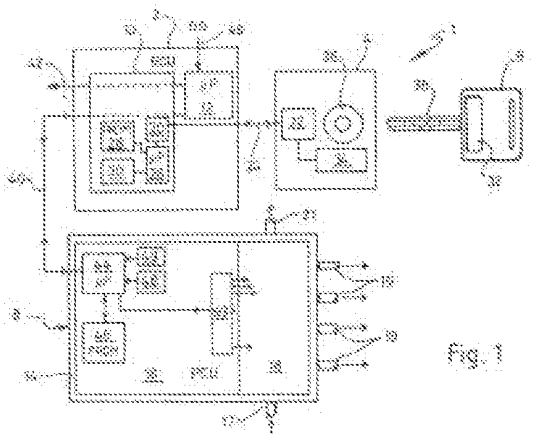


Fig. 1

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).

Last updated: 11.12.2013 Worldwide Database 5.8.15.10; 92p

Electronic Patent Application Fee Transmittal

Application Number:	14028469
Filing Date:	16-Sep-2013
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Francis G. Plati Sr./angelica zepeda
Attorney Docket Number:	116546-6601UT

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	18344924
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	Francis G. Plati Sr./angelica zepeda
Filer Authorized By:	Francis G. Plati Sr.
Attorney Docket Number:	116546-6601UT
Receipt Date:	28-FEB-2014
Filing Date:	16-SEP-2013
Time Stamp:	22:36:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	9985
Deposit Account	502075
Authorized User	ZAPEDA, ANGELEICA

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	Information Disclosure Statement (IDS) Form (SB08)	116546-6601UT_PTOSB08.pdf	614465 3ca07ee715acfb836db3da9ca1c81f0ff3fd266e	no	11
Warnings:					
Information:					
A U.S. Publication 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.					
2	Foreign Reference	116546-6601UT_FP_1.pdf	2661354 4d3fe2c7740c623d7e16d9cd0707d7be022b8b7a	no	90
Warnings:					
Information:					
3	Foreign Reference	116546-6601UT_FP_2.pdf	96959 633fae872b3915a1922213bdd0a6e15a445098e7	no	1
Warnings:					
Information:					
4	Foreign Reference	116546-6601UT_FP_3.pdf	92922 ff0c0d4871e4e32370071aecb74159cc9cf69863	no	2
Warnings:					
Information:					
5	Foreign Reference	116546-6601UT_FP_4.pdf	728847 2f402ff31bcc106e5bc942d30891f6824ba0d7c2	no	11
Warnings:					
Information:					
6	Foreign Reference	116546-6601UT_FP_5.pdf	1668426 0e26bbea9860a3259d94aa1e187167c333fe5f95	no	42
Warnings:					
Information:					
7	Foreign Reference	116546-6601UT_FP_6.pdf	1956578 872706f3cbc884487854893fa7748b6fb7f508f4	no	43
Warnings:					
Information:					

8	Foreign Reference	116546-6601UT_FP_7.pdf	118540 2fdc7f99406fe4c3bb12c5eaf6f90cc3f65849ed	no	2
Warnings:					
Information:					
9	Non Patent Literature	116546-6601UT_NP_1.pdf	580567 53ce71d0c06f4f0ce39cac912083cb85a7f22f69	no	12
Warnings:					
Information:					
10	Non Patent Literature	116546-6601UT_NP_2.pdf	2022834 1cc594f7bfda7ccb6467621485df4076a3eac823	no	7
Warnings:					
Information:					
11	Non Patent Literature	116546-6601UT_NP_3.pdf	126923 8bad07884ec4170845ae3b667e1eaae37da5a392	no	7
Warnings:					
Information:					
12	Non Patent Literature	116546-6601UT_NP_4.pdf	180891 93783ceaf7fbe0f6f613202a4909e5d06cb8a08d	no	1
Warnings:					
Information:					
13	Non Patent Literature	116546-6601UT_NP_22.pdf	317952 bdaf1f9fe98d1cbe7aea6659c31dfeae00fde887	no	7
Warnings:					
Information:					
14	Non Patent Literature	116546-6601UT_NP_23.pdf	1158193 e516fa925df57b99ac32ce08d3110f6d6874ffbc	no	10
Warnings:					
Information:					
15	Non Patent Literature	116546-6601UT_NP_CCR.pdf	11566633 4c46c78ad648a61317bad877ea668393ce13f222	no	5
Warnings:					
Information:					
16	Fee Worksheet (SB06)	fee-info.pdf	30473 0b27c542613bce9b3dbd7810f9bdfc6877d7275c	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	23922557

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/13	Francisco Martinez de Velasco Cortina	116546-6601UT	3712

EXAMINER	
Van Thanh TRIEU	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
February 3, 2014	EFS WEB

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

Commissioner:

In response to the Non-Final Office Action dated December 6, 2013, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following submission, where:

AMENDMENTS TO THE CLAIMS begin on page 2 of this paper; and

REMARKS begin on page 6 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Original) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

2. (Original) The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. (Original) The mobile device of claim 1, wherein the transaction information is credit card transaction information.

4. (Original) The mobile device of claim 1, wherein the transaction information is awards information.

5. (Original) The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. (Original) The mobile device of claim 5, wherein the security block is a cryptographic block.

7. (Currently amended) The mobile device of claim 1, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

8. (Currently amended) The mobile device of claim 7, wherein the RF device is a radio frequency identification (RFID) device.

9. (Original) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory;

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. (Original) The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. (Original) The mobile device of claim 9, wherein the transaction information is credit card transaction information.

12. (Original) The mobile device of claim 9, wherein the transaction information is awards information.

13. (Original) The mobile device of claim 9, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

14. (Original) The mobile device of claim 9, wherein the security block is a cryptographic block.

15. (Currently amended) The mobile device of claim 9, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

16. (Currently amended) The mobile device of claim 15, wherein the RF device is a radio frequency identification (RFID) device.

17. (Original) A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

18. (Original) The mobile device of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. (Original) The mobile device of claim 17, wherein the transaction information is credit card transaction information.

20. (Original) The mobile device of claim 17, wherein the transaction information is awards information.

21. (Original) The mobile device of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. (Original) The mobile device of claim 21, wherein the security block is a cryptographic block.

23. (Currently amended) The mobile device of claim 17, further comprising an RF device configured to communicate the transaction information to an RF reader/writer.

24. (Currently amended) The mobile device of claim 23, wherein the RF device is a radio frequency identification (RFID) device.

REMARKS

Status of the Application

Claims 1-24 are pending in the application and stand rejected. Claims 1, 9, and 17 are the independent claims.

With this Amendment, claims 7, 8, 15, 16, 23, and 24 are amended only to correct grammatical errors. These amendments are editorial in nature and do not implicate an estoppel.

Claim Rejections

Claims 1-3, 5, 6, 9-11, 13, 14, 17-19, 21, and 22 — 35 U.S.C. § 102(b)

Claims 1-3, 5, 6, 9-11, 13, 14, 17-19, 21, and 22 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 7,225,337 to Baessler ("Baessler"). Applicant respectfully traverses this rejection.

Addressing the rejection of independent claim 1, Applicant respectfully submits that Baessler does not disclose or suggest at least a "mobile device, comprising … a biometric reading device configured to read biometric information," as recited in the claim.

In rejecting the claim, the Examiner alleges that Baessler's disclosure of a signature module that generates a fingerprint discloses the claimed "biometric input device." Applicant respectfully submits that the Examiner misconstrues the disclosure of Baessler for at least the following reasons.

Baessler discloses a ***"fingerprint" as a term for a characteristics record of a data object*** created by a hash function: "Conventionally, by means of a hash function, a characteristics record, ***a so-called fingerprint, is obtained from the object data to be signed***" (col. 2, ll. 19-21) (***emphasis added***). Further, "[t]he ***signature module 105 generates first a fingerprint (e.g. a so-called hash) of the object data*** to be signed (e.g. with a SHA1 hash function), and out of that the digital customer signature using the private customer key 102 (col. 6, ll. 4-8) (***emphasis added***).

Thus, as disclosed by Baessler, a fingerprint is a ***hash of a data object, not biometric data*** as recited in the claim. Therefore, Baessler fails to disclose or suggest inputting biometric data and so fails to disclose or suggest at least a "mobile device, comprising … a biometric input device configured to receive biometric data," as recited in independent claim 1.

Accordingly, since Baessler does not disclose or suggest all of the claimed features, Applicant respectfully submits that independent claim 1 is patentable over Baessler.

Independent claims 9 and 17 contain features similar to the features recited in claim 1 and are therefore patentable for similar reasons.

Claims 2, 3, 5, 6, 10, 11, 13, 14, 18, 19, 21, and 22 are patentable at least by virtue of their respective dependencies.

Claims 4, 7, 8, 12, 15, 16, 20, 23, and 24 — 35 U.S.C. § 103(a)

Claims 4, 7, 8, 12, 15, 16, 20, 23, and 24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Baessler in view of U.S. Patent No. 7,980,378 to Jones et al. ("Jones"). Applicant respectfully traverses this rejection.

The combination of Baessler and Jones does not disclose or suggest at least the above-noted features of independent claims 1, 9, and 17 incorporated into claims 4, 7, 8, 12, 15, 16, 20, 23, and 24 by virtue of their respective dependencies. As established above, Baessler does not disclose or suggest at least these features. Jones does not cure the deficiencies of Baessler.

The Examiner relies on Jones to allegedly disclose the claimed features related to the transaction information is awards information, an RF device configured to communicate transaction information, and wherein the RF device is an RFID device, as recited in the dependent claims. Without conceding the disclosure of Jones alleged by the Examiner, Applicant respectfully submits that Jones fails to disclose or suggest at least the features of a "mobile device, comprising … a biometric reading device configured to read biometric information," as incorporated into claims 4, 7, 8, 12, 15, 16, 20, 23, and 24 by virtue of their respective dependencies. Thus, Jones fails to cure the deficiencies of Baessler.

Accordingly, since the combination of Baessler and Jones does not disclose or suggest all of the claimed features, Applicant respectfully submits that independent claims 4, 7, 8, 12, 15, 16, 20, 23, and 24 are patentable over the combined references.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-24 is respectfully requested. If the Examiner believes that a telephone conversation may be useful in advancing prosecution, the Examiner is invited to contact the undersigned at the number listed below.

If necessary, applicant requests to extend the period for filing this reply pursuant to 37 CFR 1.136(a) and authorizes the Director to charge any additional fee(s) or any underpayment of fee(s) or credit any overpayment(s) to Procopio Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: February 3, 2014

/ /
Francis G. Plati, Sr.
Reg. No. 59,153

Customer No. 27189
Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900

Electronic Acknowledgement Receipt

EFS ID:	18101766
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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:	Francis G. Plati Sr./angelica zepeda
Filer Authorized By:	Francis G. Plati Sr.
Attorney Docket Number:	116546-6601UT
Receipt Date:	03-FEB-2014
Filing Date:	16-SEP-2013
Time Stamp:	19:29:16
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		116546-6601UT_Response.pdf	125527 664a438efd02b3f4fd982aaf37f276b403df2283	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Abstract	6	8
Warnings:			
Information:			
	Total Files Size (in bytes):	125527	

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

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

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

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

PTO/SB/06 (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 14/028,469	Filing Date 09/16/2013	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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	02/03/2014	(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))	* 24	Minus	** 24	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 2	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	**0**

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
/SHAUNA ZIMMERMAN/

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-6601UT

CONFIRMATION NO. 3712

PUBLICATION NOTICE

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

OC000000066123879

Title:SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Publication No.US-2014-0019355-A1
Publication Date:01/16/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/028,469	09/16/2013	Francisco Martinez de Velasco Cortina	116546-66001UT	3712

27189 7590 12/06/2013

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
12/06/2013	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. 14/028,469	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner VAN TRIEU	Art Unit 2685	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 *9/16/2013*.

☐ 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) *1-24* 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) *1-24* 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 _____ 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

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-3, 5, 6, 9-11, 13, 14, 17-19, 21, 22 are rejected under 35 U.S.C. 102(b) as being anticipated by **Baessler** [US 7,225,337].

Regarding claim 1, the claimed a mobile device, comprising: Radio Frequency (RF) cellular circuitry (the radio mobile telephone, see Fig. 1, col. 5, line 2);

a memory configured to store biometric authentication information and transaction information (the electronic data store 10, see Fig. 1, col. 5, lines 18-45);

a biometric reading device configured to read biometric information (the signature module 105 generates customer fingerprint, see Fig. 1, col. 6, lines 4-6);

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory (the processor 11 receives all the customer fingerprint, private key, public key and security key for determining of authentication for selected transaction by the authentication module 423, see Figs. 1, 2, col. 8, lines 1-28, col. 9, lines 61-67, col. 10, lines 1-9); and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module (the processor 11 processes to determine if the customer signature of fingerprint/biometric is positively verified/matched or authenticated those of the personal customer attributes 107 are selected by the customer, which are transmitted to the transaction partner with the order, see Figs. 1, 2, col. 5, lines 18-45, col. 9, lines 61-67, col. 10, lines 1-9).

Regarding claim 2, wherein the biometric reading device is a fingerprint reading device (the signature module 105 generates customer fingerprint, see Fig. 1, col. 6, lines 4-6).

Regarding claim 3, wherein the transaction information is credit card transaction information (the credit card, see col. 5, line 39).

Regarding claim 5, further comprising a security block configured to secure the transaction information before it is provided by the transaction module (the signature module 105 comprises cryptographic functions and security module 41 and 42 such as if the customer signature cannot be verified, no signature certificate is generated, see Fig. 1, col. 5, lines 64-67, col. 7, lines 36-67, col. 8, lines 1-6, col. 10, lines 3-4).

Regarding claim 6, wherein the security block is a cryptographic block (the signature module 105 comprises cryptographic functions, see Fig. 1, col. 5, lines 64-67, col. 6,

lines 1-66, col. 10, lines 3-4).

Regarding claim 9, all the claimed subject matters are cited in respect to claim 1 above.

Regarding claim 10, all the claimed subject matters are cited in respect to claims 2 and 9 above.

Regarding claim 11, all the claimed subject matters are cited in respect to claims 3 and 9 above.

Regarding claim 13, all the claimed subject matters are cited in respect to claims 5 and 9 above.

Regarding claim 14, all the claimed subject matters are cited in respect to claims 6 and 9 above.

Regarding claim 17, all the claimed subject matters are cited in respect to claim 1 above.

Regarding claim 18, all the claimed subject matters are cited in respect to claims 2 and 17 above.

Regarding claim 19, all the claimed subject matters are cited in respect to claims 3 and 17 above.

Regarding claim 21, all the claimed subject matters are cited in respect to claims 5 and 17 above.

Regarding claim 22, all the claimed subject matters are cited in respect to claims 6 and 17 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 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.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 4, 7, 8, 12, 15, 16, 20, 23, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Baessler** [US 7,225,337] in view of **Jones et al** [US 7,980,378] Regarding claim 4, **Baessler** fails to disclose the transaction information is awards information. However, **Baessler** discloses the portable communication terminal 2 with a security module 1 processes to provide a transaction selected by a customer's financial technical data such as mode of payment, bank account, credit card number, credit limit or credit worthiness, see Figs. 1, 2, col. 5, lines 30-40). **Jones et al** suggests that the currency processing machines 10 is configured to communicate via an in-store computer system communication link 202, 204 to an interface or receiving device 200 at any one of a plurality of destination locations. The destination locations include, but are not limited to, a service desk 210, a POS station 220a-n, a kiosk 230, and/or a portable electronic device 250. The portable electronic device 250 includes a display and a communication interface for enabling communications via the communication links 202, 204. The communication links 202, 204 may utilize any convention wired or wireless protocol including, but not limited to, Ethernet, 802.11, Bluetooth.TM., USB, cellular (CDMA, GSM, and the like), and so forth. The associated communication interfaces may include wireless transceivers, USB controllers, Ethernet controllers, RFID transceivers, radio microchips, and/or transponders, and the like. The portable electronic device 250 may, in different embodiments, be a digital wallet, a mobile a PDA, a smart card, a token, a fob, and the like. The portable electronic device 250 may comprise, for example, a Nokia 3220 telephone comprising a payment chip or a cellular telephone under development by Nokia and Cingular embedded with a "near

field communication" ("NFC") chip. The store may, for example, give special promotions for those using credit balances off of their preferred accounts by using balances associated with the preferred card. These aspects enable the retailer to reward their most loyal customers and drive customer purchases into their stores (see Figs. 1-20, col. 15, lines 1-37, col. 41, lines 58-67, col. 60, lines 46-67, col. 61, lines 1-26). Therefore, it would have been obvious to one skill in the art at the time the invention was made to implement the portable electronic device with the redemption of coupons, promotional or rewarding functions of **Jones et al** to the portable communication terminal with security transaction module of **Baessler** for advantage in businesses and financials including of advertisements, bonus, coupons, promotions and/or awards and rewards to their good and most loyal customers and drive/motivate customer purchases into their stores, which are available in the free markets.

Regarding claim 7, **Baessler** fails to disclose an RF device configured to communicate the transaction information an RF reader/writer. However, **Baessler** discloses the portable communication terminal 2 is mobile radio telephone, laptop, PDA with a communication module for communication over a mobile radio network, see Fig. 1, col. 5, lines 1-7, col. 7, lines 36-45). **Jones et al** suggests that the currency processing machines 10 is configured to communicate via an in-store computer system communication link 202, 204 to an interface or receiving device 200 at any one of a plurality of destination locations. The destination locations include, but are not limited to, a service desk 210, a POS station 220a-n, a kiosk 230, and/or a portable electronic

device 250. The portable electronic device 250 includes a display and a communication interface for enabling communications via the communication links 202, 204. The communication links 202, 204 may utilize any convention wired or wireless protocol including, but not limited to, Ethernet, 802.11, Bluetooth.TM., USB, cellular (CDMA, GSM, and the like), and so forth. The associated communication interfaces may include wireless transceivers, USB controllers, Ethernet controllers, RFID transceivers, RFID reader such as Mobile 1, radio microchips, and/or transponders, and the like (see Figs. 1-20, col. 15, lines 1-37, col. 41, lines 26-38, col. 60, lines 46-67, col. 61, lines 1-26, col. 63, lines 34-58). Therefore, it would have been obvious to one skill in the art at the time the invention was made to substitute the portable electronic RFID device and RFID reader of **Jones et al** to the portable communication terminal of **Baessler** for quickly identifying and higher secure to prevent of tampering and theft, and the advance of very tiny IC chip device or card.

Regarding claim 8, wherein RF device is a radio frequency identification (RFID) device (as discussed of the RFID reader and RFID device between **Baessler** and **Jones et al** in respect to claim 7 above.

Regarding claim 12, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 4 and 9 above.

Regarding claim 15, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 7 and 9 above.

Regarding claim 16, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 8 and 15 above.

Regarding claim 20, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 4 and 17 above.

Regarding claim 23, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 7 and 17 above.

Regarding claim 24, all the claimed subject matters are discussed between **Baessler** and **Jones et al** in respect to claims 8 and 23 above.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chaum discloses a cryptographic apparatus which may be "personalized" to its owner. The apparatus may be utilized by its owner to identify himself to an external computer system, to perform various financial transactions with an external system, and to provide various kinds of credentials to an external system. The cryptographic device

includes interface circuitry to permit information exchange with the external system, a memory device for storage of data necessary to allow identification of the owner, and control logic for controlling the exchange of data with the external system to identify the owner. Certain data which must be utilized to perform the identification information exchange is stored in the memory device in encrypted form. The decryption of this data requires the entry of a secret ID, known to the owner. [US 4,529,870]

Clark discloses a self-service terminal having a wireless communication port for interacting with a user's portable device. The terminal may be an ATM, and includes a biometric device for capturing biometric data from a user at the terminal. The terminal is operable to receive biometric data from portable devices within the vicinity of the terminal, and compares the received biometric data with data captured by the biometric device to determine which portable device is associated with the user at the terminal. A method of executing a transaction at a self-service terminal having a wireless communications port is also described. [US 6,793,134]

Martinez et al discloses a method and system for verifying and tracking identification information. A system for delivering security solutions is provided that includes at least one of the following: a radio frequency identification device, an identification mechanism e.g., a card, sticker, and an RF reader. [US 7,671,746] and [US 8,004,410]

Beenau et al discloses enabling remote customer service and maintenance using a visual identifier. In response to a user enrolling in a service capability associated with a mobile device, the process utilizes a visual identifier to associate the service capability with the customer account, the service and the mobile device. The system allocates a

visual identifier for each service capability and enables customer service agents to identify the service capability and mobile device, verify the user and retrieve information for the service interaction. [US 8,126,449] and [US 8,401,539]

Bertran et al discloses systems and methods for authorizing financial transactions are described. A request for execution of the financial transaction from a requesting party includes at least one biometric signature of the requesting party and the request is authorized based on identification of the biometric signature in a repository of signatures and a history of prior transactions executed on behalf of the requesting party. The repository may include signatures stored in encrypted form on a smartcard. [US 2010/0094754] and [US 2010/0095130]

4. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner **Van Trieu** whose telephone number is (571) 272-2972. The examiner can normally be reached on Mon-Fri from 8:00 AM to 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Mr. Hai Phan** can be reached on (571) 272-6338

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.

/Van T. Trieu/

Primary Examiner, Art Unit 2685

Date: 12/03/2013

Notice of References Cited	Application/Control No. 14/028,469	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner VAN TRIEU	Art Unit 2685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-4,529,870	07-1985	Chaum, David	235/380
*	B	US-6,793,134	09-2004	Clark, Barrie	235/379
*	C	US-7,225,337	05-2007	Baessler, Felix	713/175
*	D	US-7,671,746	03-2010	Martinez de Velasco Cortina et al.	340/572.4
*	E	US-7,980,378	07-2011	Jones et al.	194/217
*	F	US-8,004,410	08-2011	Martinez de Velasco Cortina et al.	340/572.4
*	G	US-8,126,449	02-2012	Beenau et al.	455/419
*	H	US-8,401,539	03-2013	Beenau et al.	455/419
*	I	US-2010/0094754	04-2010	Bertran et al.	705/44
*	J	US-2010/0095130	04-2010	Bertran et al.	713/189
	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	
	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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10	(("4529870") or ("6793134") or ("7225337") or ("7671746") or ("7980378") or ("8004410") or ("8126449") or ("8401539") or ("20100094754") or ("20100095130")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/12/02 11:03
L2	10	1 and (cellular or phone or telephone)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:04
L3	5	1 and (RFID or smart or tag or transponder)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:05
L4	8	1 and (authentication or authoriz$3 or approv$3) with (biometric or fingerprint or eye)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:07
L5	5	1 and (award$3 or reward$3 or bonus)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:08
L6	6	1 and (cryptic or cryptographic$4)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:09
L7	8	1 and (interrogat$3 or reader)	US-PGPUB; USPAT; USOCR	OR	ON	2013/12/02 11:10

EAST Search History (Interference)

<This search history is empty>

12/2/2013 11:10:40 AM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace.wsp

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
14/028,469	MARTINEZ DE VELASCO CORTINA ET AL.
Examiner	**Art Unit**
VAN TRIEU	2685

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	12/3/13
	1	/
	2	/
	3	/
	4	/
	5	/
	6	/
	7	/
	8	/
	9	/
	10	/
	11	/
	12	/
	13	/
	14	/
	15	/
	16	/
	17	/
	18	/
	19	/
	20	/
	21	/
	22	/
	23	/
	24	/
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14028469	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
340	539.1, 539.11, 539.13, 568.1, 568.7, 572.1, 572.4, 572.7	12/2/13	vt
235	379, 380, 381	12/2/13	vt
455	419	12/2/13	vt
713	175, 189	12/2/13	vt

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

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

MAILED
OCT 15 2013
OFFICE OF PETITIONS

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 14/028,469

1. THE REQUEST FILED September 16, 2013 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 **Michelle R. Eason** at (571) 272-4231. In his/her absence, calls may be directed to Brian W. Brown at (571) 272-5338.

/Michelle R. Eason/
(*Signature*)

Paralegal Specialist, Office of Petitions
(Title)

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
14/028,469	09/16/2013	2876	2220	116546-660001	24	3

CONFIRMATION NO. 3712

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

FILING RECEIPT

OC000000064267429

Date Mailed: 10/10/2013

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)

Francisco Martinez de Velasco Cortina, La Jolla, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/350,665 01/13/2012
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.

If Required, Foreign Filing License Granted: 10/08/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/028,469**
Projected Publication Date: 01/16/2014

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Preliminary Class

235

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/028,469

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))	24 minus 20 =	* 4			OR	x 80 =	320
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 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	1920

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(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($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
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	

AMENDMENT B

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

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

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (03-13)

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), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.
2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.
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. The executed inventor's oath or declaration is filed with the application. (37 CFR 1.63 and 1.64)

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 /Noel C. Gillespie/	Date 2013-09-16
Name (Print/Typed) Noel C. Gillespie	Practitioner Registration Number 47596

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 1 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.

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:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

2. The mobile device of claim 1, wherein the biometric reading device is a fingerprint reading device.

3. The mobile device of claim 1, wherein the transaction information is credit card transaction information.

4. The mobile device of claim 1, wherein the transaction information is awards information.

5. The mobile device of claim 1, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

6. The mobile device of claim 5, wherein the security block is a cryptographic block.

7. The mobile device of claim 1, further comprising an RF device configured to communicate the transaction information an RF reader/writer.

8. The mobile device of claim 7, wherein RF device is a radio frequency identification (RFID) device.

9. A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory;

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module; and

a security block configured to secure the transaction information before it is provided by the transaction module.

10. The mobile device of claim 9, wherein the biometric reading device is a fingerprint reading device.

11. The mobile device of claim 9, wherein the transaction information is credit card transaction information.

12. The mobile device of claim 9, wherein the transaction information is awards information.

13. The mobile device of claim 9, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

14. The mobile device of claim 9, wherein the security block is a cryptographic block.

15. The mobile device of claim 9, further comprising an RF device configured to communicate the transaction information an RF reader/writer.

16. The mobile device of claim 15, wherein RF device is a radio frequency identification (RFID) device.

17. A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

a memory configured to store biometric authentication information and transaction information;

a biometric reading device configured to read biometric information;

an authentication module configure to authenticate the biometric information read by the biometric reading device based at least in part on the biometric authentication information stored in the memory; and

a transaction module configured to provide the transaction information for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module.

18. The mobile device of claim 17, wherein the biometric reading device is a fingerprint reading device.

19. The mobile device of claim 17, wherein the transaction information is credit card transaction information.

20. The mobile device of claim 17, wherein the transaction information is awards information.

21. The mobile device of claim 18, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

22. The mobile device of claim 21, wherein the security block is a cryptographic block.

23. The mobile device of claim 17, further comprising an RF device configured to communicate the transaction information an RF reader/writer.

24. The mobile device of claim 23, wherein RF device is 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.

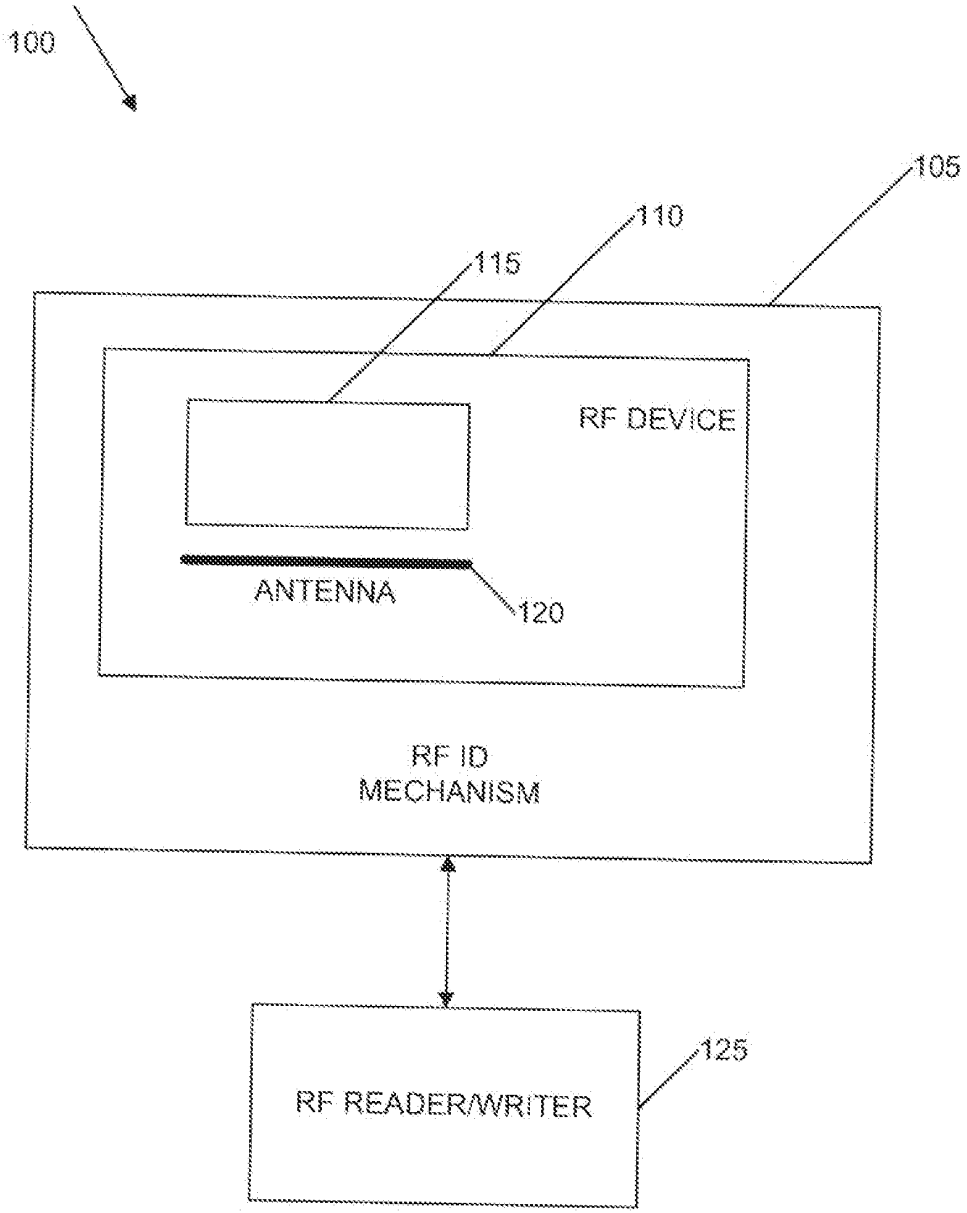

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

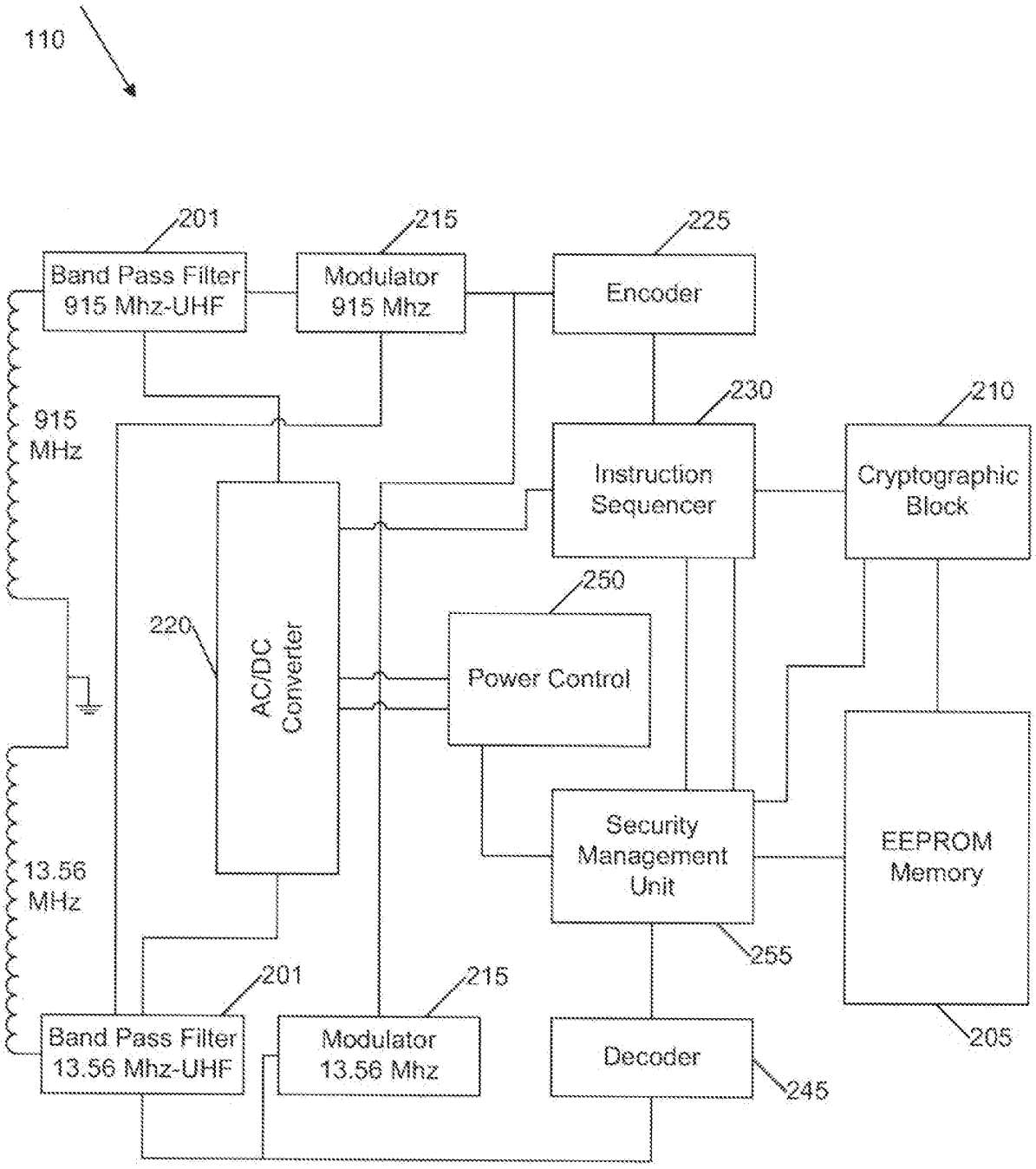

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
13.56
MHz
Security
Management
Unit
EEPROM
Memory
255
201
215
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
245
205

FIG. 2

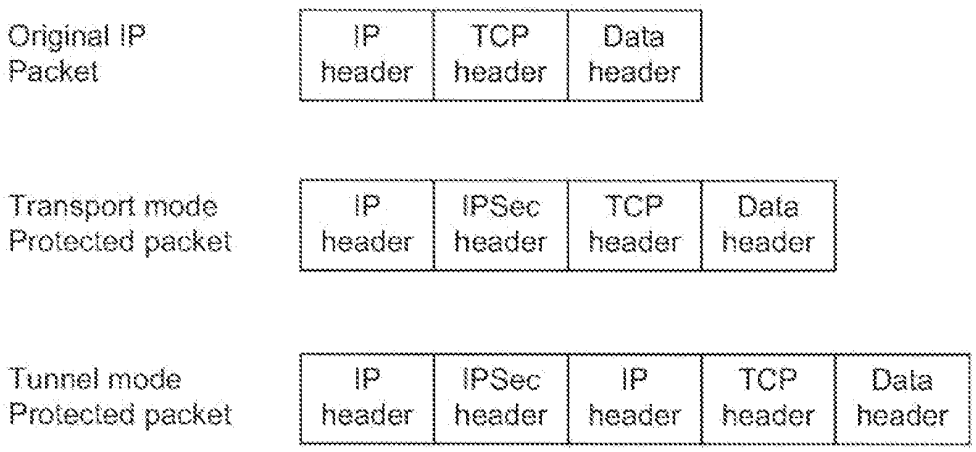

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

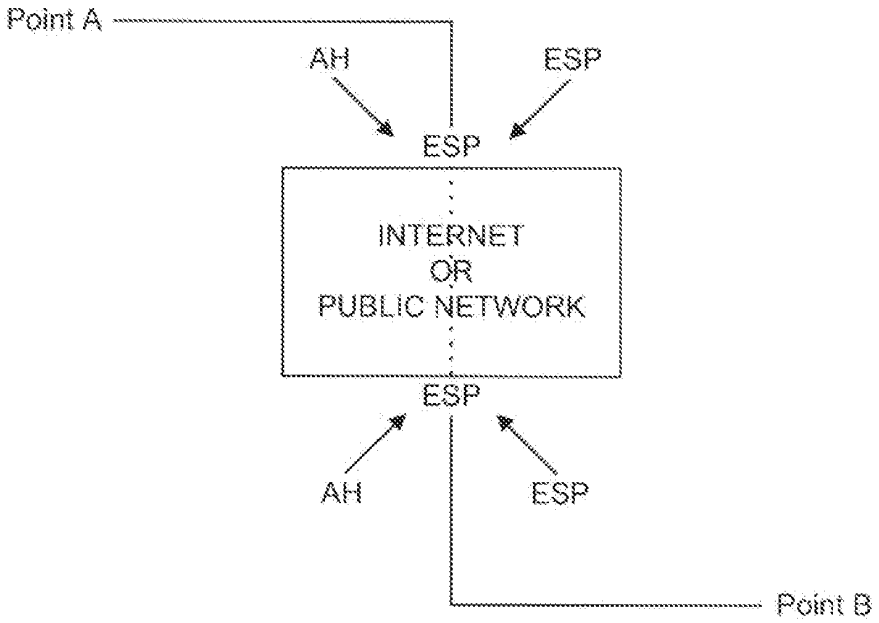

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

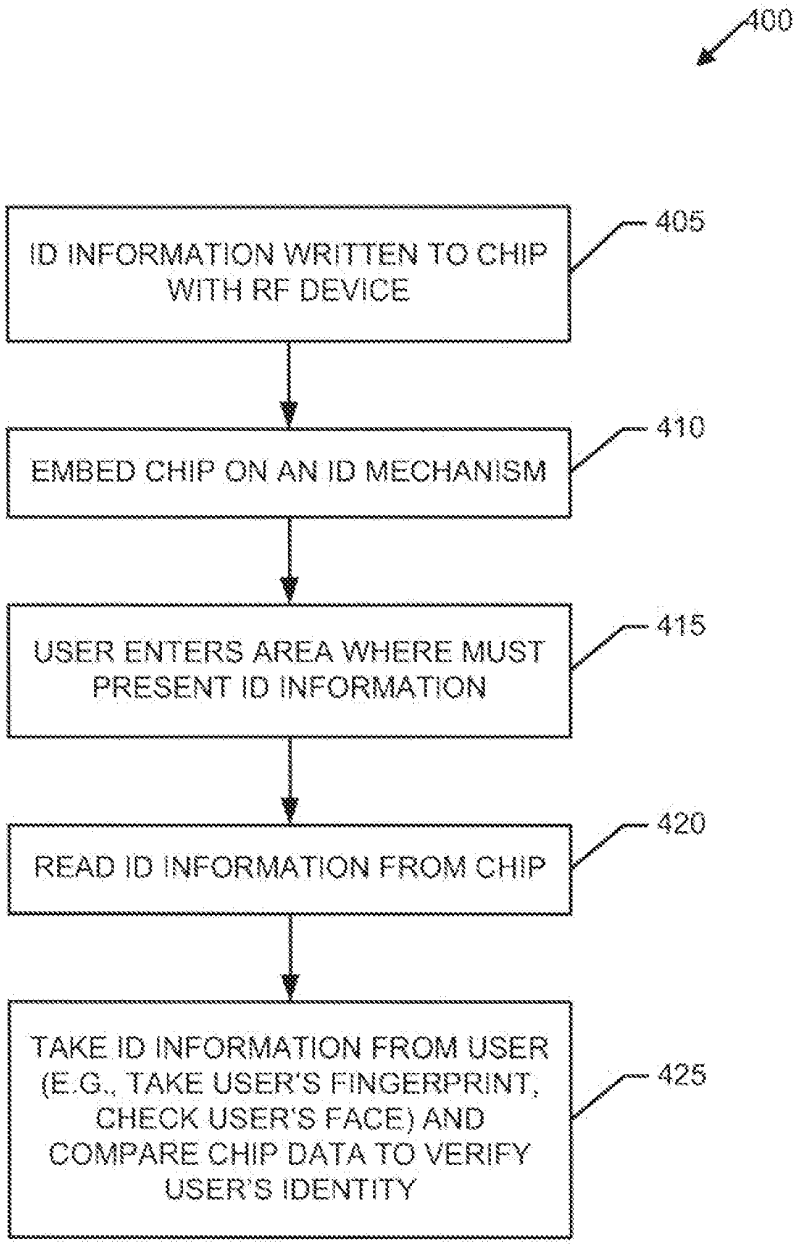

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY
425

FIG. 4

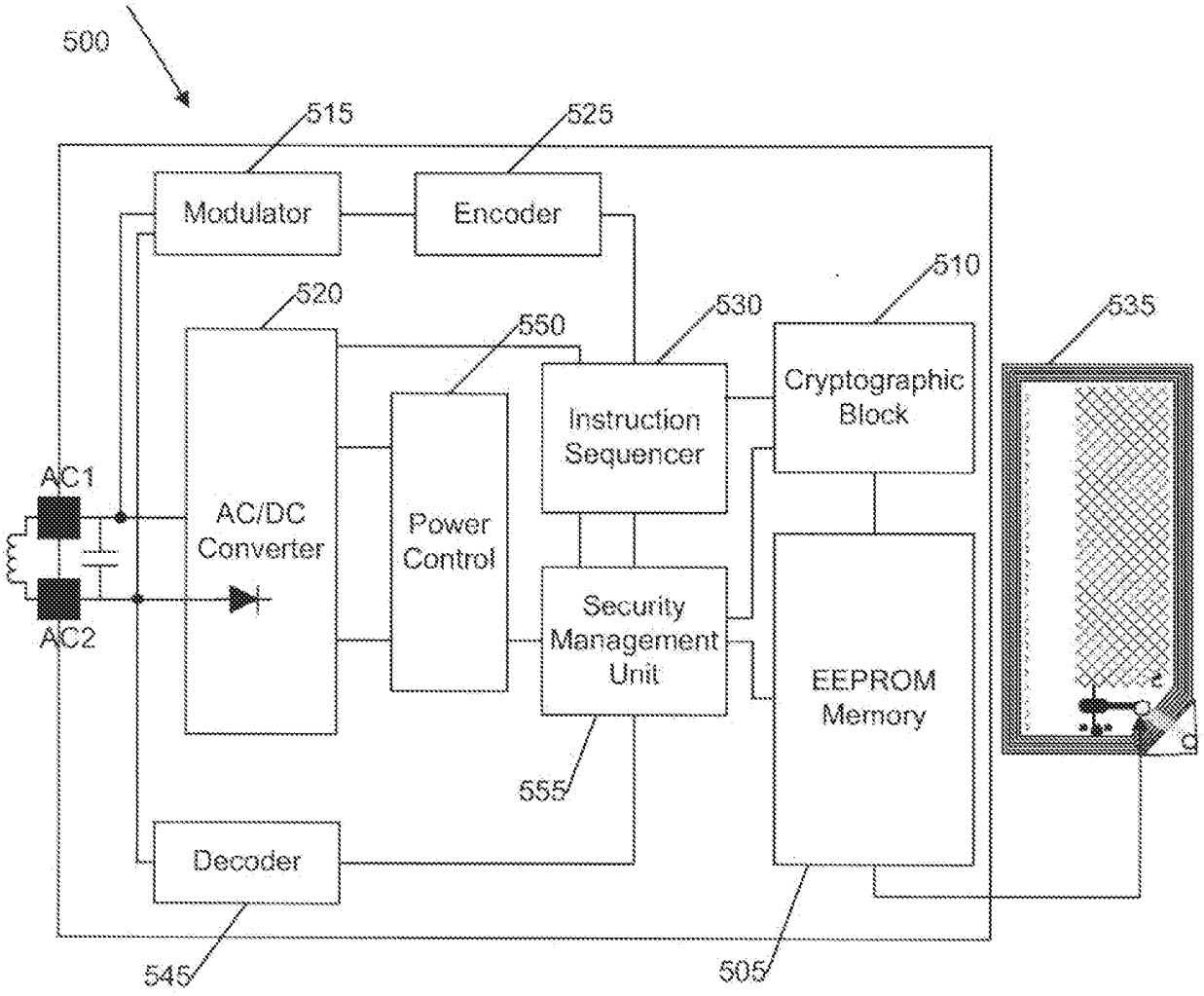

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

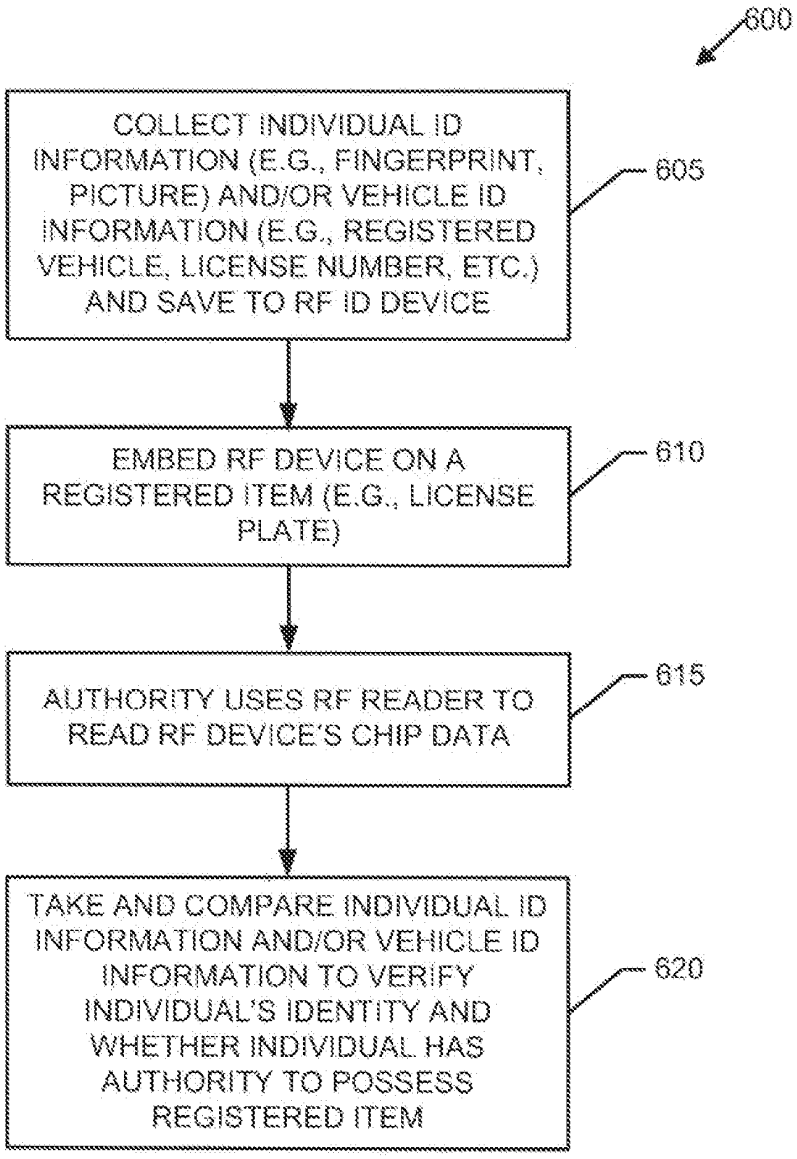

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

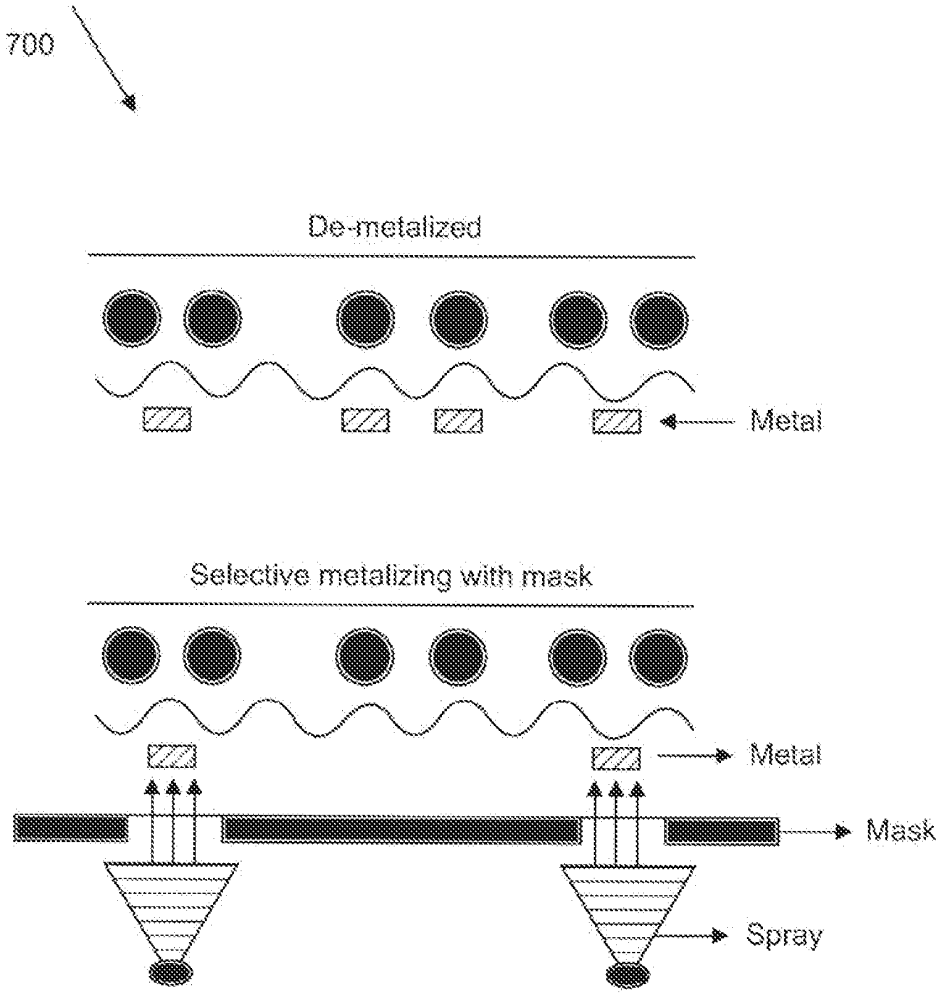

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

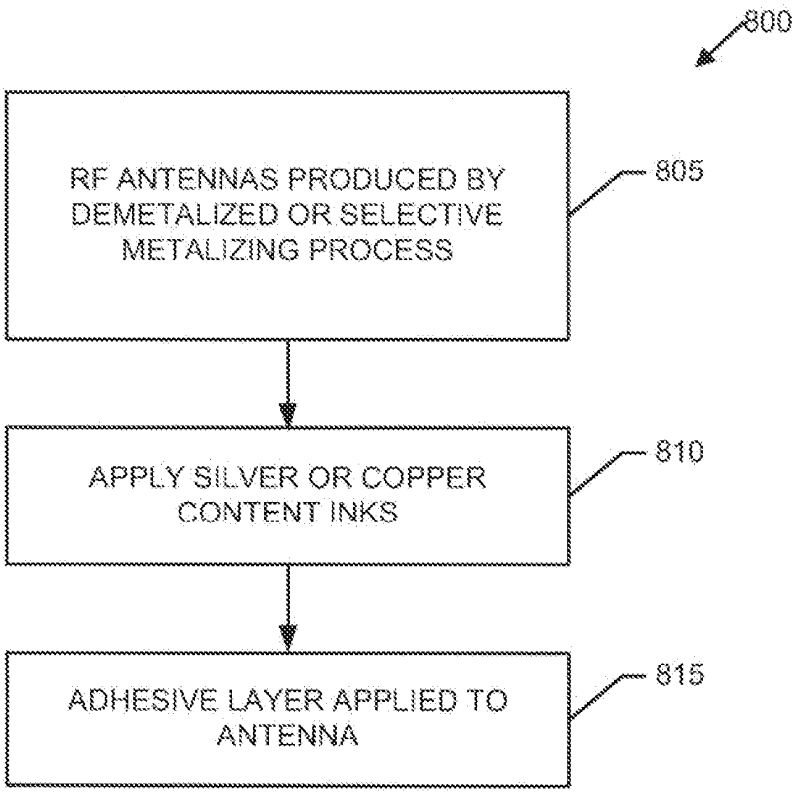

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

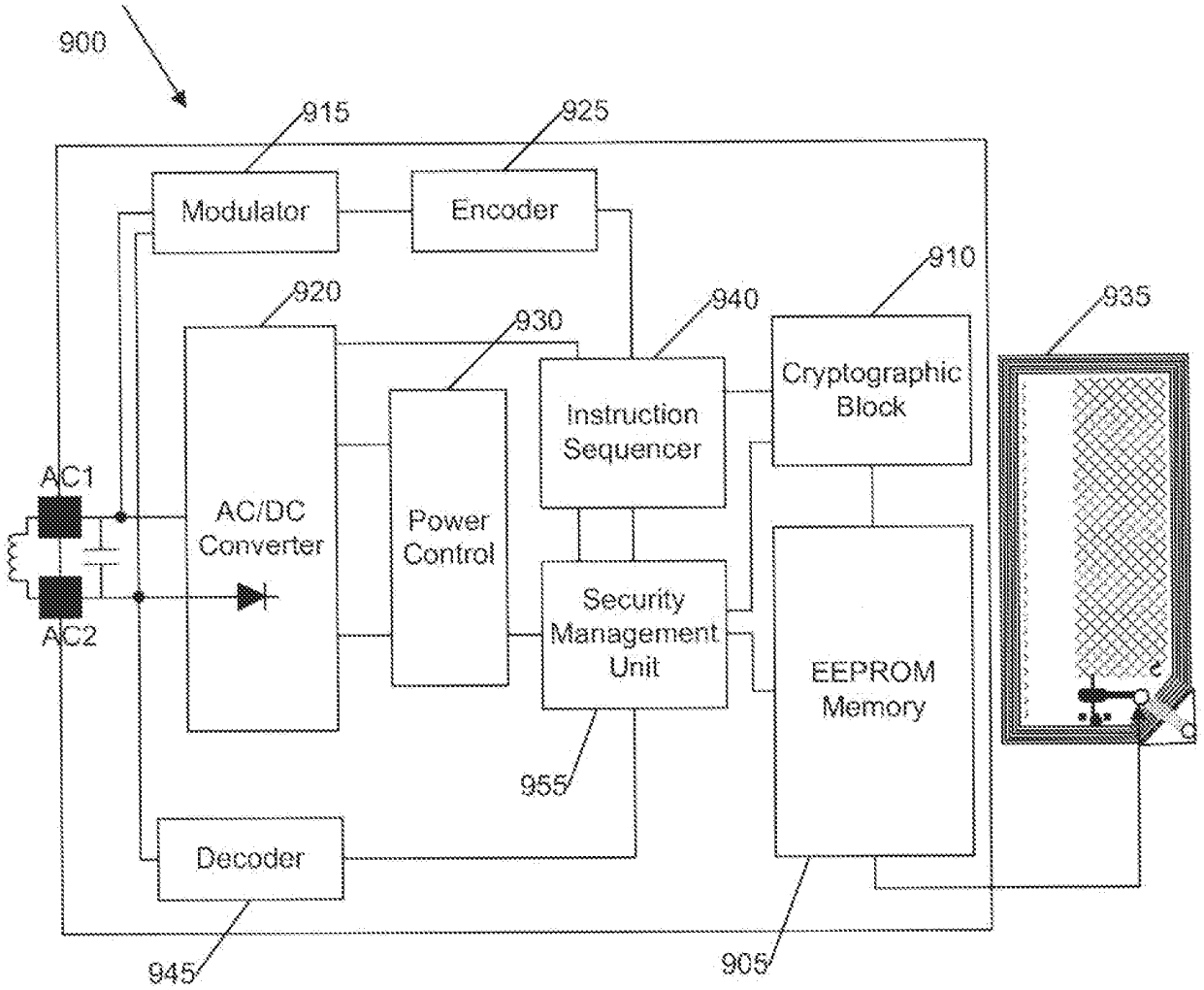

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

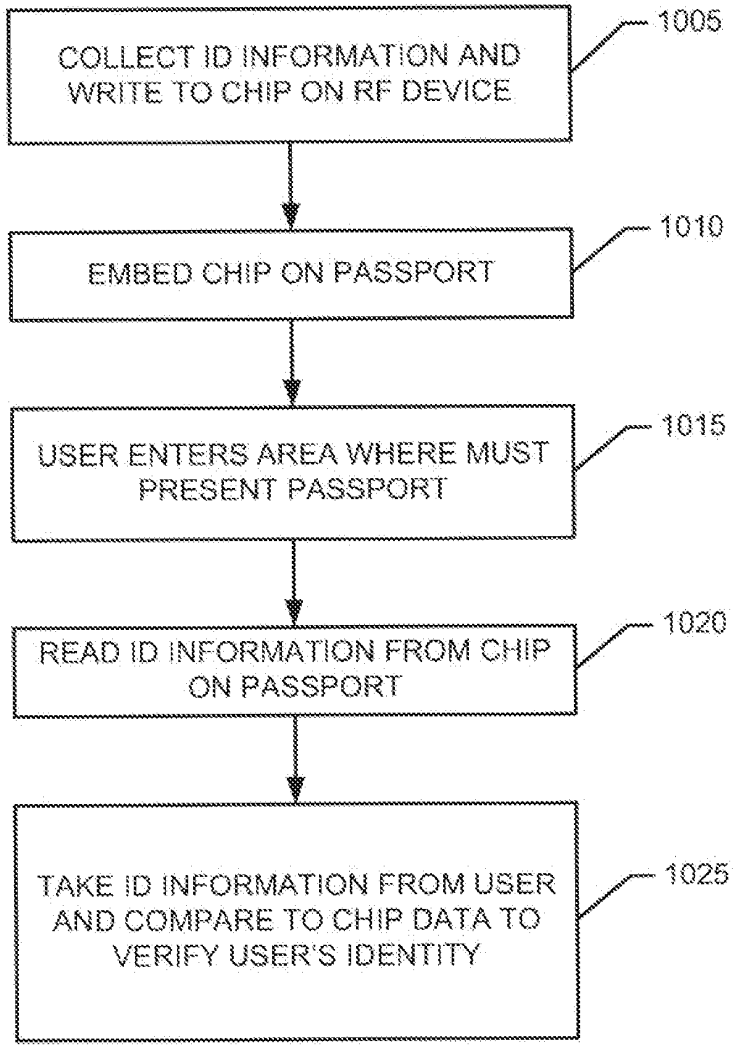

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

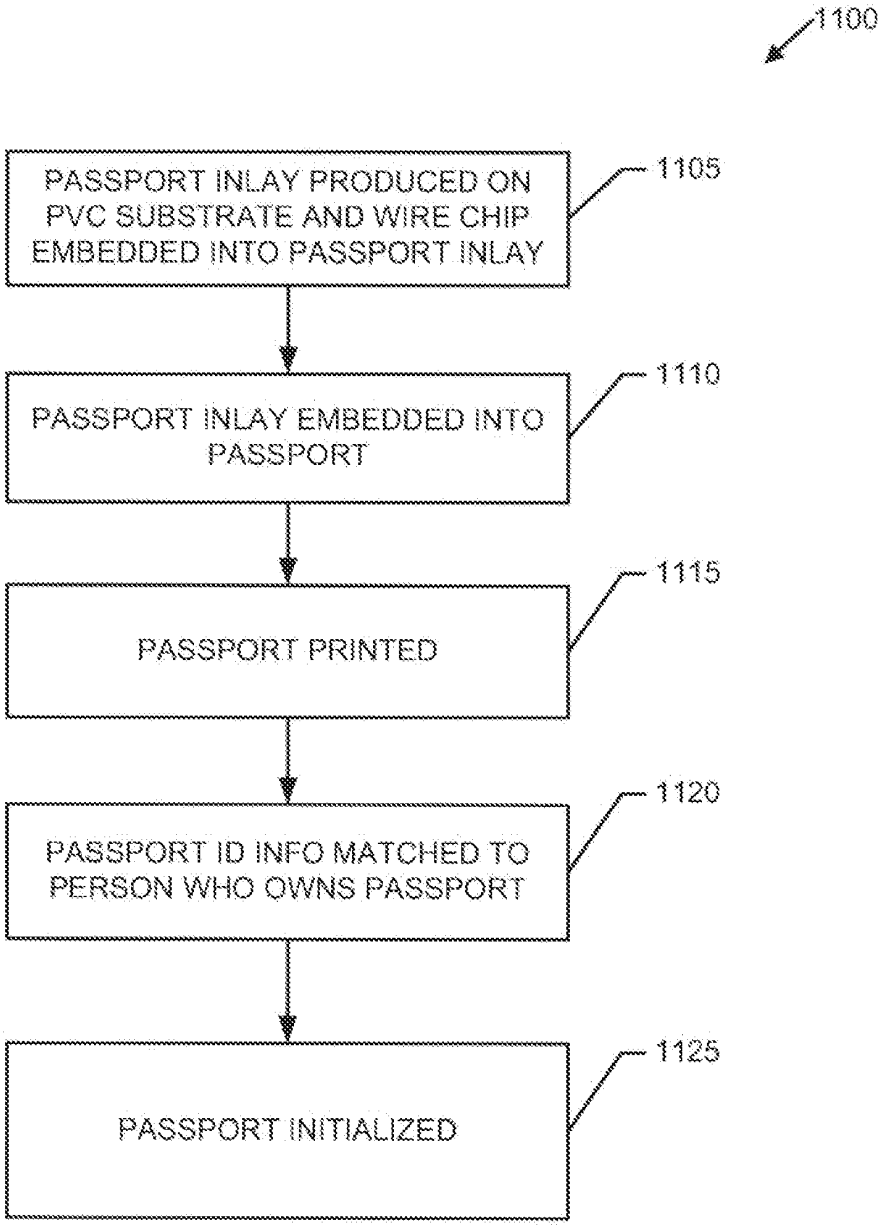

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

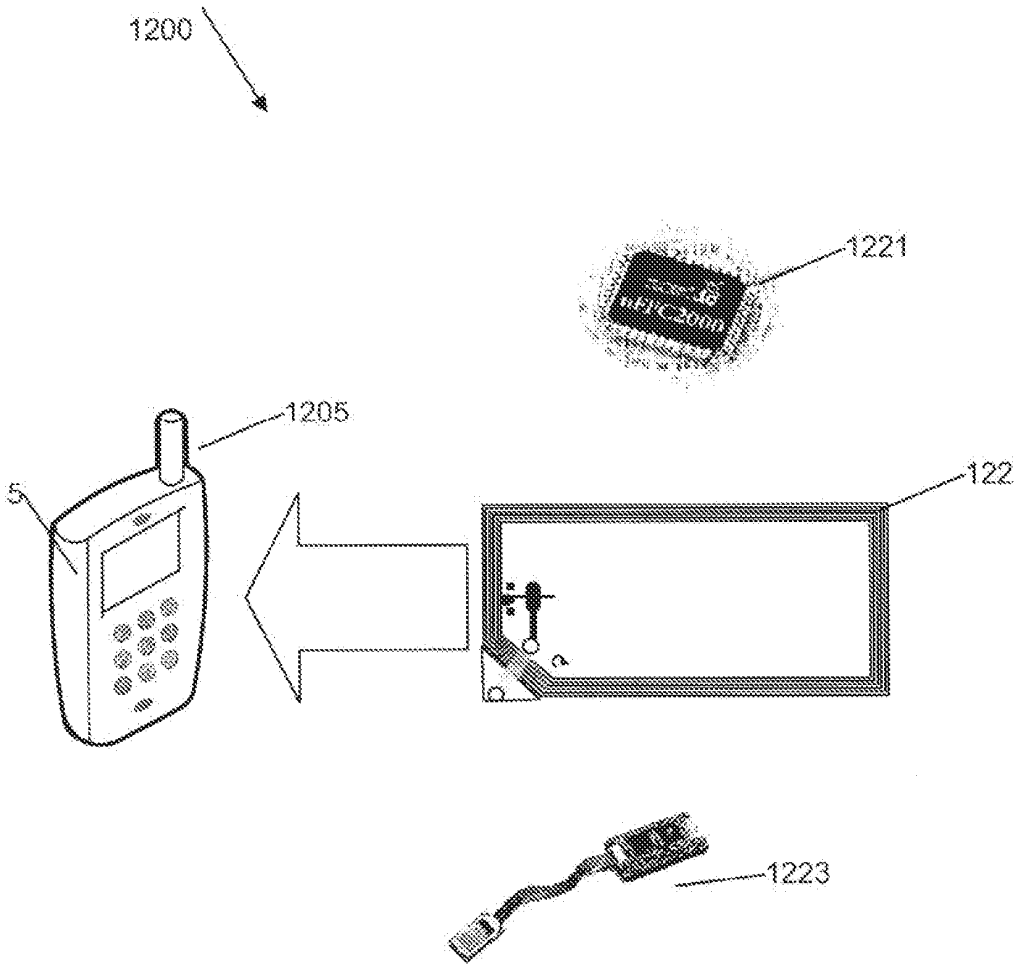


FIG. 12

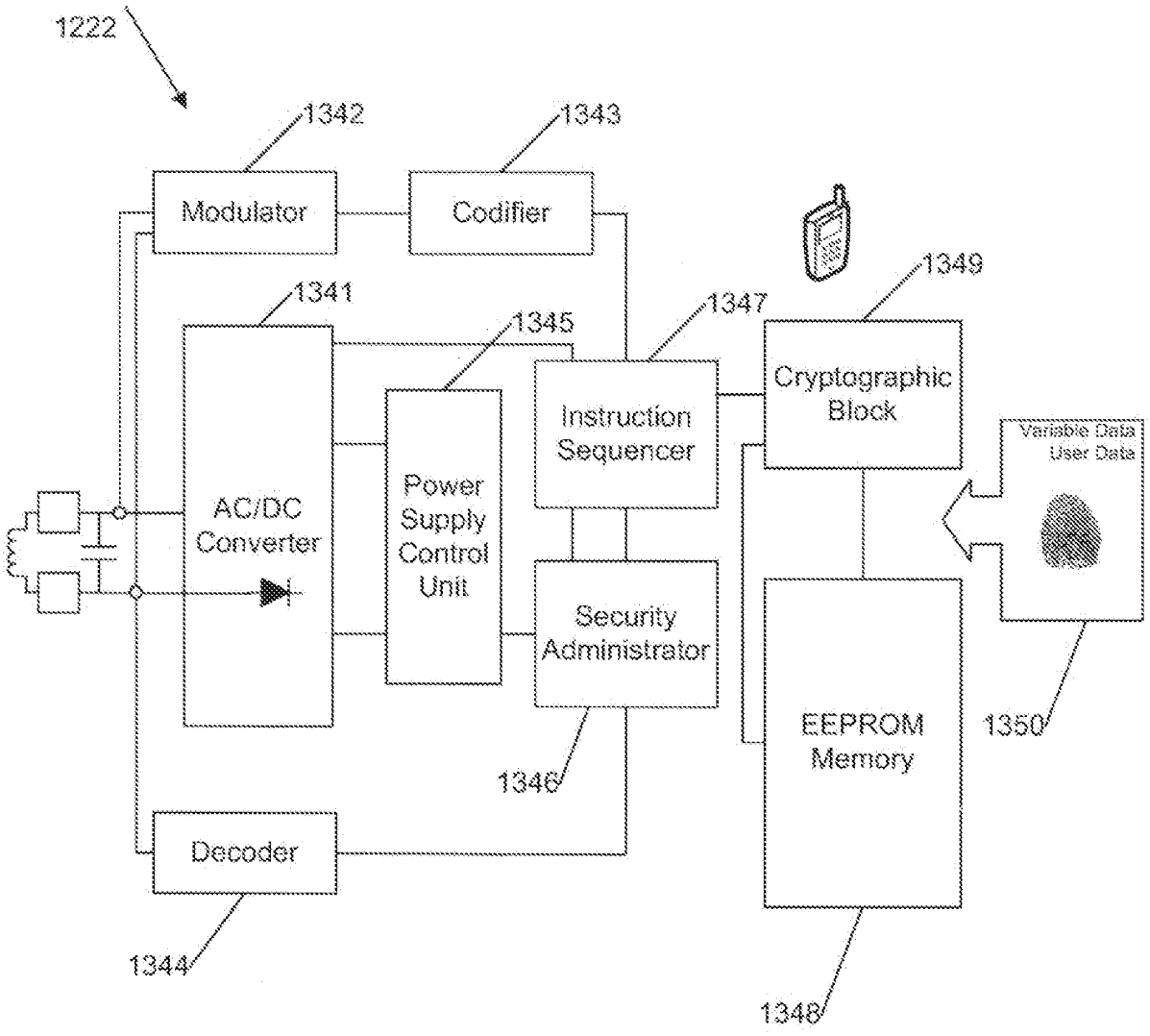

1222
1342
1343
Modulator
Codifier
1341
1345
1347
1349
AC/DC Converter
Power Supply Control Unit
Instruction Sequencer
Cryptographic Block
Variable Data
User Data
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

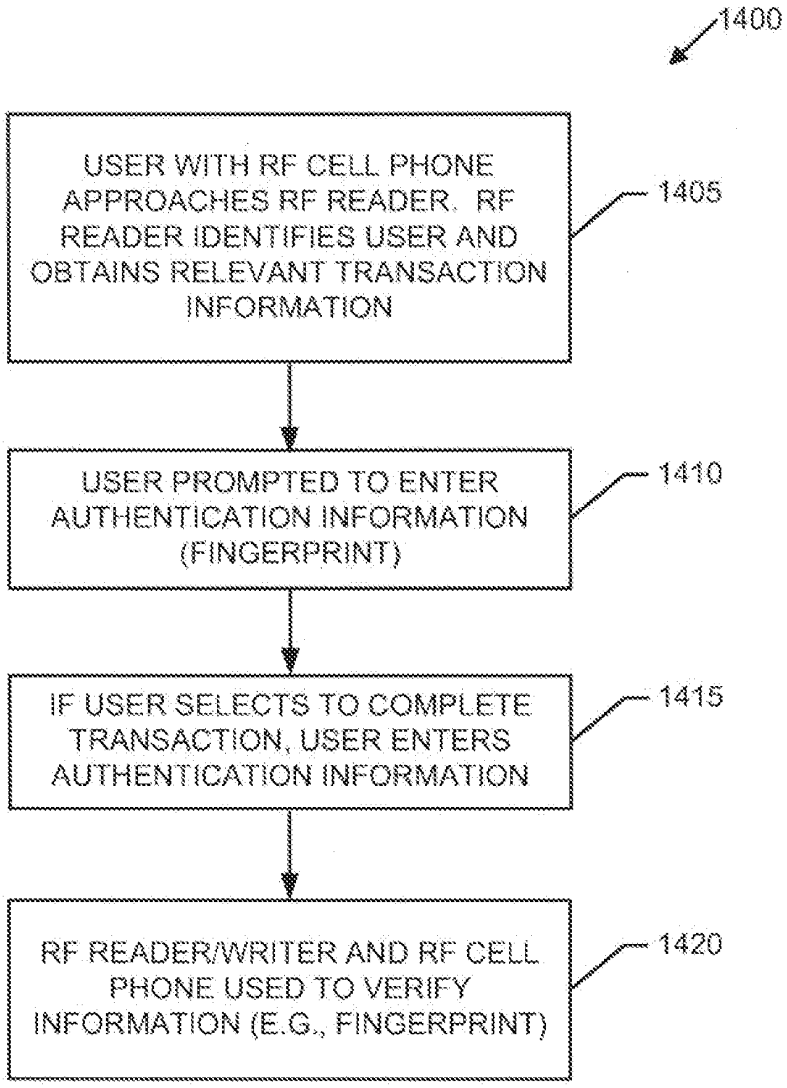

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

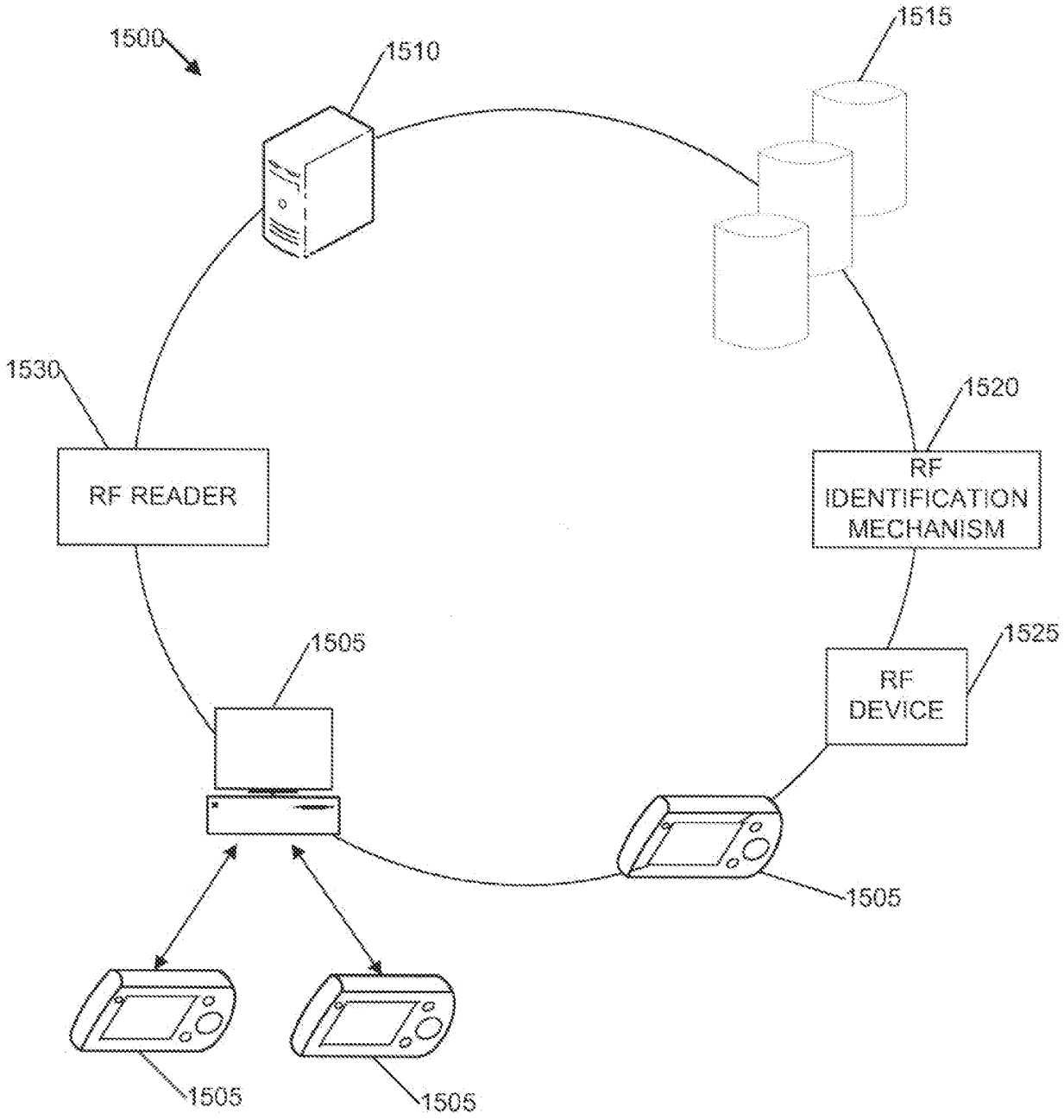

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

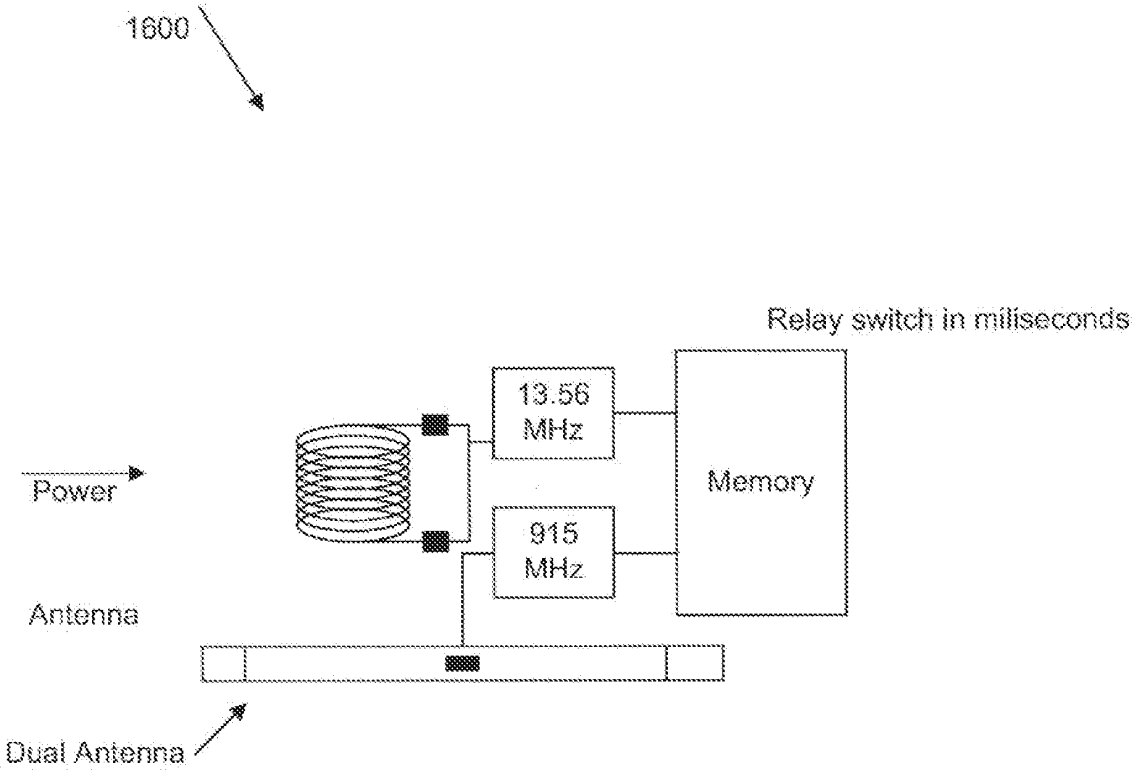

1600
Relay switch in milliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

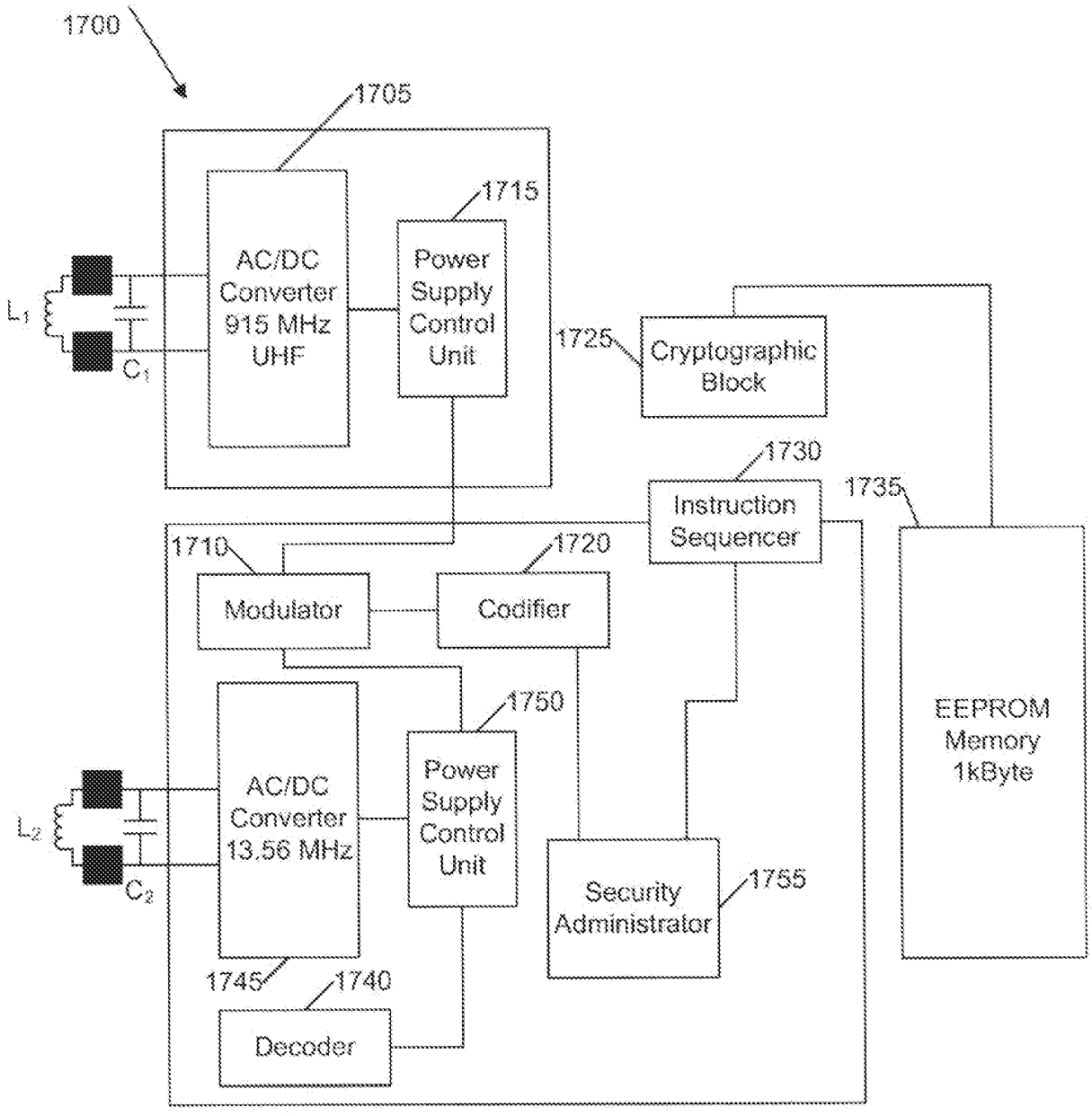

1700
1705
1715
AC/DC
Converter
915 MHz
UHF
Power
Supply
Control
Unit
L1
C1
1725
Cryptographic
Block
1730
Instruction
Sequencer
1735
1710
1720
Modulator
Codifier
EEPROM
Memory
1kByte
1750
AC/DC
Converter
13.56 MHz
Power
Supply
Control
Unit
L2
C2
Security
Administrator
1755
1745
1740
Decoder

FIG. 17

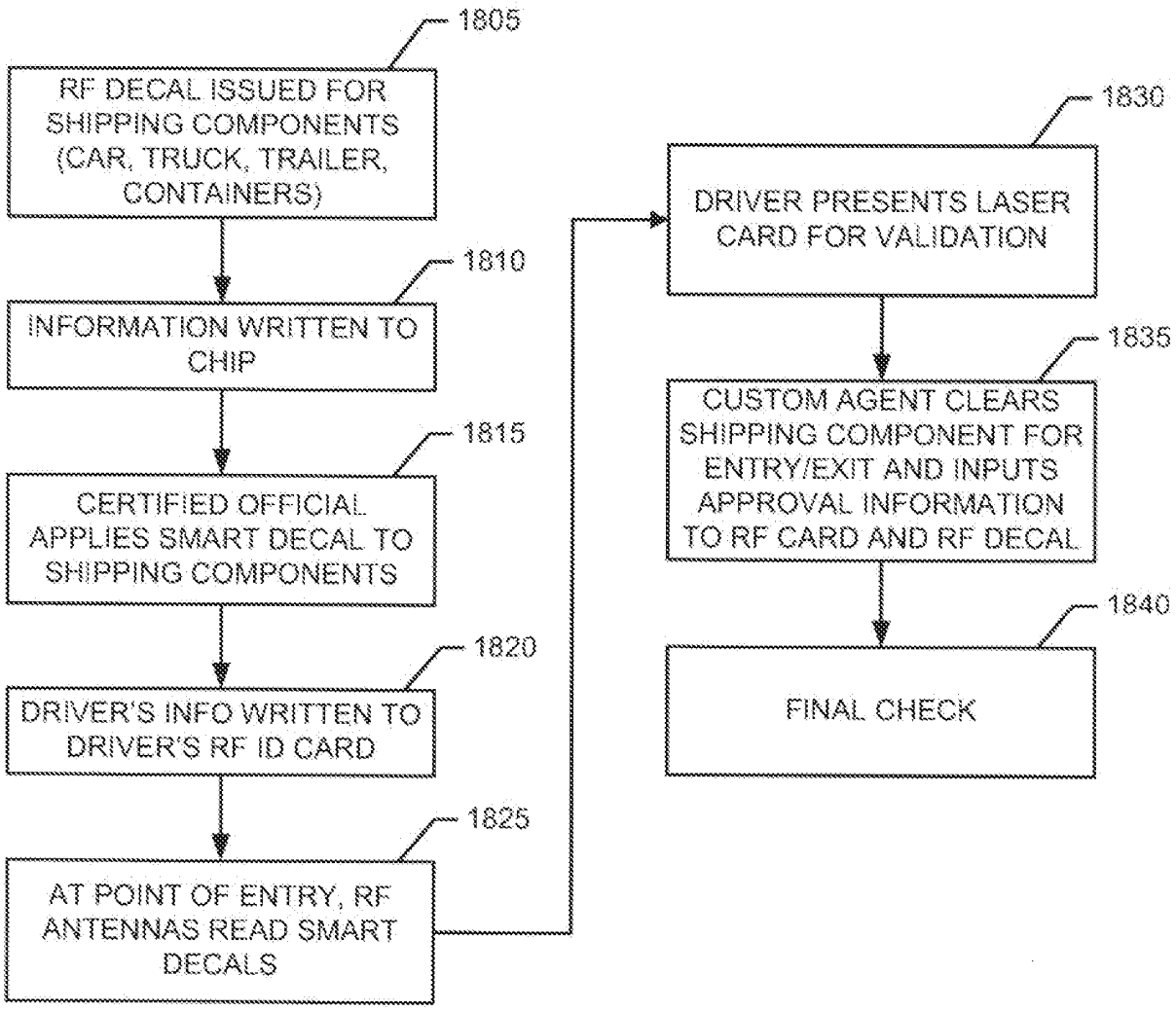

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS 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

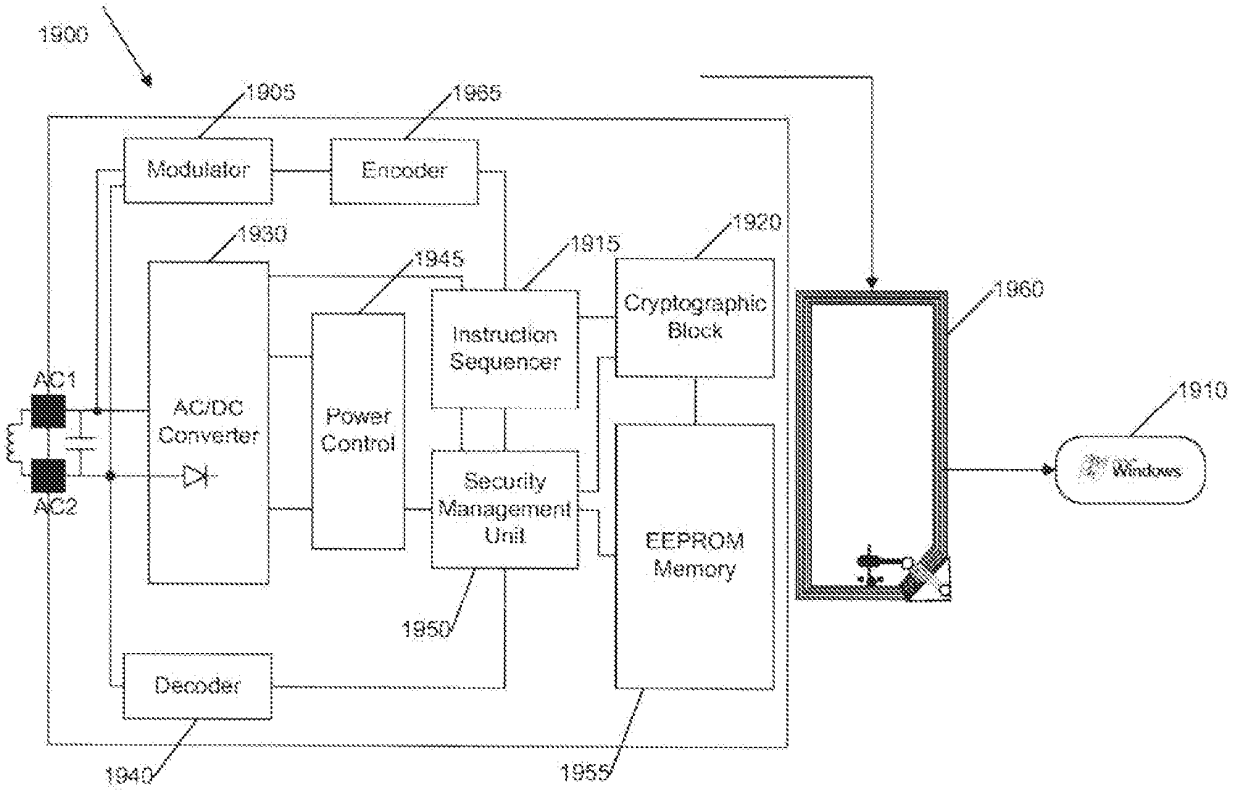

1900
1905
1955
Modulator
Encoder
1930
1945
1915
1920
1960
Cryptographic Block
Instruction Sequencer
AC1
AC2
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
1910
Windows
1950
Decoder
1940
1955

FIG. 19

116946.0102/4144967v1

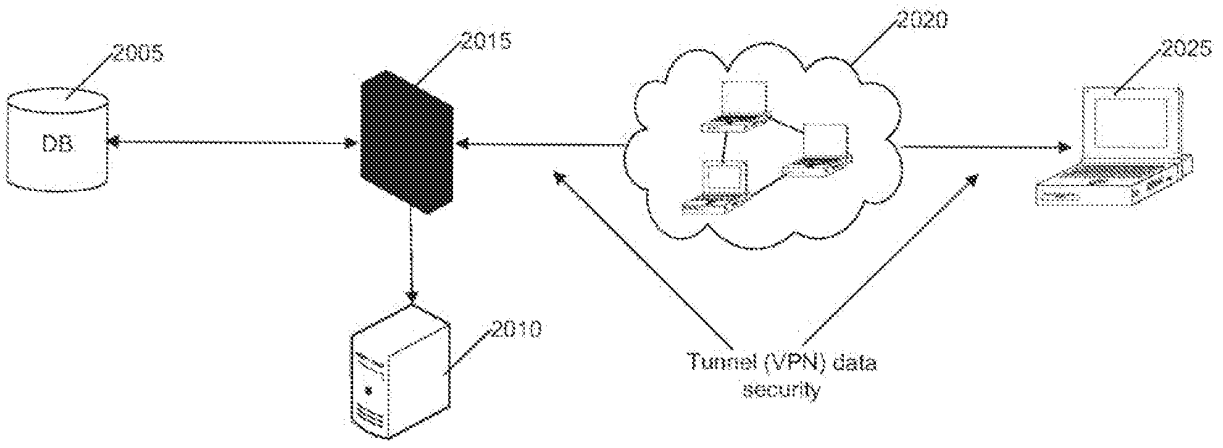


FIG. 20

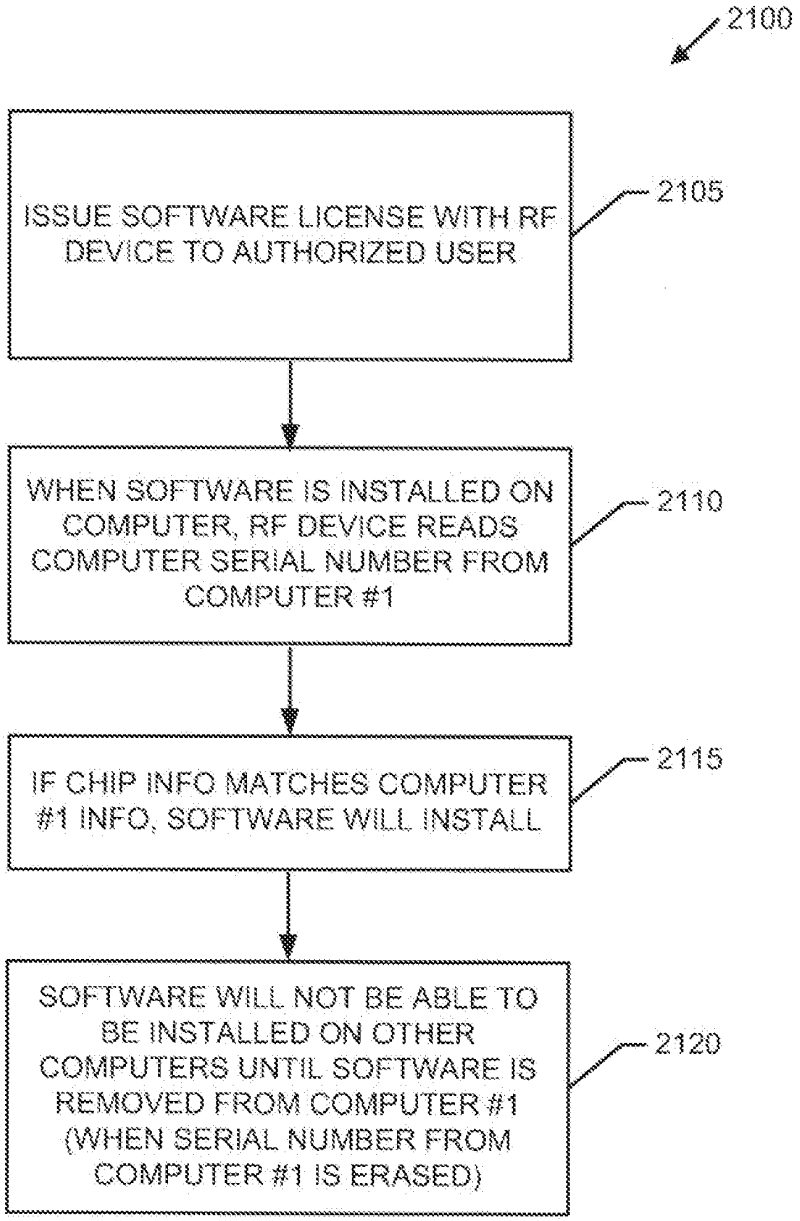

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL SOFTWARE IS REMOVED FROM COMPUTER #1 (WHEN SERIAL NUMBER FROM COMPUTER #1 IS ERASED)
2120

FIG. 21

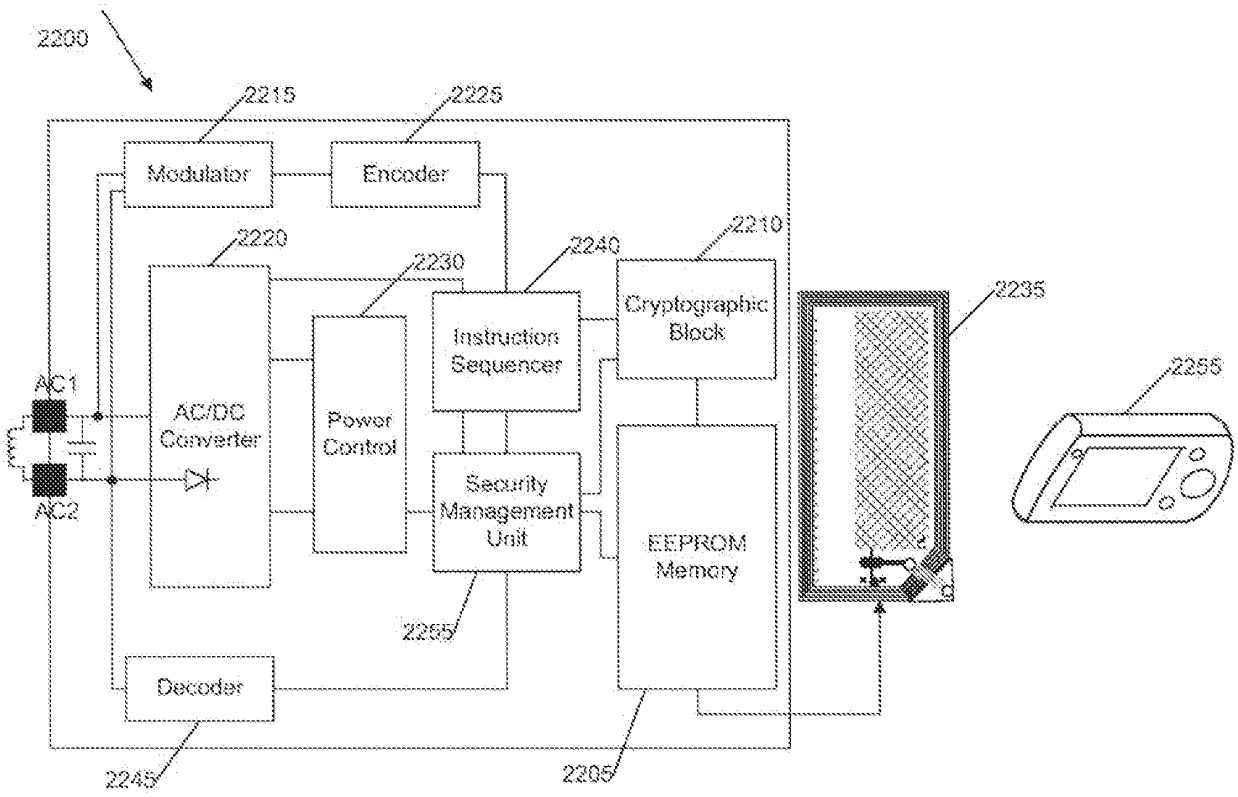


FIG. 22

Page 23/24

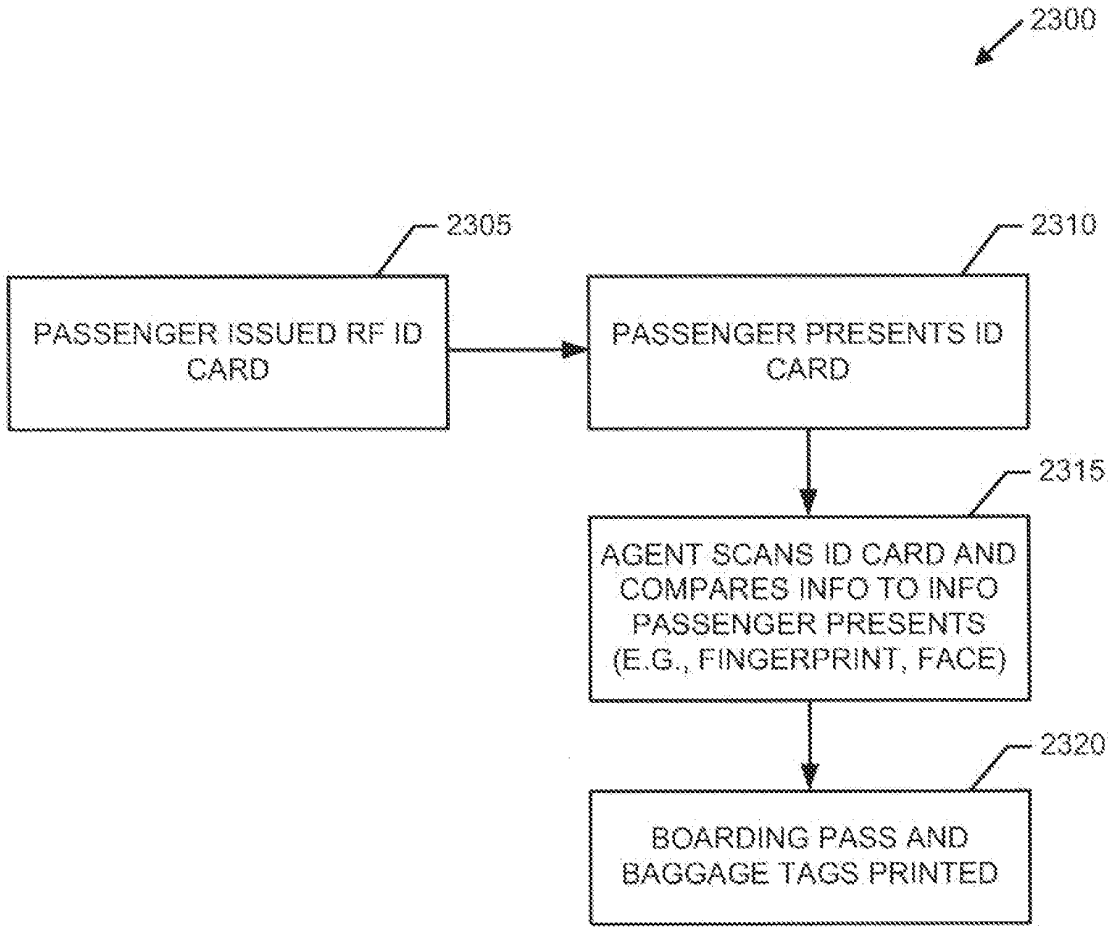

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	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., Suite A		
Address 2			
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 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	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	116546-660001	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	24	**Suggested Figure for Publication (if any)**	

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		

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.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13350665	2012-01-13
Prior Application Status	Patented		Remove

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

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	non provisional of	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:

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

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

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

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.

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

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. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
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

PTO/AIA/14 (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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660001
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1	
Address 2	

City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional 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	/Noel C. Gillespie/			Date (YYYY-MM-DD)	2013-09-16
First Name	Noel C.	Last Name	Gillespie	Registration Number	47596

Additional Signature may be generated within this form by selecting the Add button. Add

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.

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:	Noel C. Gillespie/angelica zepeda
Attorney Docket Number:	116546-660001
Filed as Large Entity	

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

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:				
Claims in Excess of 20	1202	4	80	320
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300
OTHER PUBLICATION PROCESSING FEE	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**6350**

Electronic Acknowledgement Receipt

EFS ID:	16869308
Application Number:	14028469
International Application Number:	
Confirmation Number:	3712
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/angelica zepeda
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-660001
Receipt Date:	16-SEP-2013
Filing Date:	
Time Stamp:	21:28:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$6350
RAM confirmation Number	8510
Deposit Account	502075
Authorized User	

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

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	116546-66001_Declarations.pdf	806807 c833f9f92ab9bebb39e9aade10ff5f891c04b499	no	4
Warnings:					
Information:					
2	TrackOne Request	116546-660001_Track_1_Request.pdf	153015 549e7a972a9228b374fcdd0f3638c35f77d3439f	no	2
Warnings:					
Information:					
3		116546-660001_Application.pdf	262720 7c5cb7c2e93818023a222e17c7cdbd4a9b264fae	yes	39

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	35
Claims	36	38
Abstract	39	39

Warnings:					
Information:					
4	Drawings-only black and white line drawings	116546-660001_drawings.pdf	9209850 ac08dec422183da2daf60c12a4be7e0fb10602ab	no	24
Warnings:					
Information:					
5	Application Data Sheet	116546-660001_ADS.pdf	1505720 c41c4ead669a53cc4c56c7e97e9f1f2791f8658d	no	7
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	41574 1bd1ca59cab7e9193e9d1560bbbe17f944c67e73	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	11979686		

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/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 _____ filed on _____

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 Rietzler Date (Optional): _____

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.

HC

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.

4C

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:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

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): _____

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.

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.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 10/07/2013

ASAHLE SALE #00000001 Mailroom Dt: 09/16/2013 502075 14028469
01 FC : 1830 140.00 DA

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 10/07/2013

ASAHLE ADJ #00000001 Mailroom Dt: 09/16/2013
Seq No: 8510 Sales Acctg Dt: 09/17/2013 502075 14028469
07 FC : 1808 130.00 CR